Measuring Software Security

Defining Security Metrics

Dr. Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: May 1, 2015 at 08:15

Why Is CyberSecurity Hard?

Why is cybersecurity any harder than any other technological problem? *Or is it?*

Partial answer: Most technological problems are concerned with ensuring that something good happens.
Security is all about ensuring that *bad things never happen*.

What Bad Things?

If security is all about ensuring that *bad things never happen*, that means we have to know what those bad things are.

The hardest thing about security is convincing yourself that you've thought of all possible attack scenarios, before the attacker thinks of them.

"A good attack is one that the engineers never thought of." –Bruce Schneier

Cyber Defense is Asymmetric

The defender has to find and eliminate *all* exploitable vulnerabilities; the attacker only needs to find *one*!

In cybersecurity, you have to defeat an *actively malicious adversary*.

Principle of Easiest Penetration: an intruder will use any available means to subvert the security of a system.

You Can't Defend Everything

Modern information management systems are a complex, "target-rich" environment comprising: hardware, software, storage media, peripheral devices, data, and people.

He who defends everything defends nothing. –old military adage

Security Isn't the Point

Security is often treated as an afterthought. *No-one builds a digital system for the purpose of being secure.* They build digital systems to do something useful.

Security mechanisms may be viewed as a nuisance to be subverted, bypassed, or disabled.

It's often hard to convince management to allocate extra resources to prevent attacks that may never occur.

The More Things Change ...

"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it." –Robert H. Morris (mid 1980's), former chief scientist of the National Computer Security Center

"Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground." –Prof. Fred Chang (2009), former director of research at NSA

Perfect Security: It Ain't Happening

Perfect security is unachievable in any useful system.

We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.

Security is Risk Management

Viega and McGraw, *Building Secure Software* assert that software and system security is "all about managing risk."

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. The assessment of risk must take into account the consequences of an exploit.

Risk management is a process for an organization to identify and address the risks in their environment.

Current IT Security Metrics

"If you can't measure something, you can't understand it. If you can't understand it, you can't control it. If you can't control it, you can't improve it." H. James Harrington

Some Popular IT Security Metrics:

- Security risk assessment matrices
- Security vulnerabilities and incident statistics
- Annualized loss expectancy (ALE)
- Return on investment (ROI)
- Total cost of ownership (TCO)

Current Metrics are Flawed

Typical Security Risk Assessment:

		Likelihood of Event		
		High	Medium	Low
Severity of Impact	High	"We're Doomed!"	Bad	Outlier
	Medium	Bad	Not Good	Error
	Low	Annoyance	Typical	"Whatever..."

Problem: This doesn't measure security risk; it measures human judgments about risk. *That can be useful, assuming you understand what you're getting.*

Counting Vulnerabilities or Incidents

The number of vulnerabilities discovered or security-related "incidents" are often used as general indicators of the level of security.

But these depend critically on:

- How thorough are your scans?
- How many systems are scanned?
- What severity is assigned to what vulnerabilities/incidents?
- How many applications are deployed?
- How does your number compare with peers?

Annualized Loss Expectancy

ALE is a common tool for risk assessment. Given potential threats, where do you put your security dollars?

Risks in a large bank:

Loss type	**Amount**	**Incidence**	**ALE**
SWIFT fraud	$50,000,000	0.005	$250,000
ATM fraud (large)	$250,000	0.2	$100,000
ATM fraud (small)	$20,000	0.5	$10,000
Teller theft	$3,240	200.0	$648,000

But this is really nothing more than expected value! Is that the right way to compute risk?

Is ALE the Right Model?

Consider the following two scenarios:

1. I give you a dollar.
2. We flip a coin. Heads: I give you $1000. Tails: you give me $998.

The expected values are exactly the same, but the risks seem quite different.

Often ALE deals in opinions and expectations because IT security does not have data to define actual probabilities.

ROI and TCO

Return on Investment (ROI) attempts to calculate how much benefit will be gained from an investment.

- How do current security expenditures affect future losses? This is very hard to estimate.
- Traditionally, ROI (in a financial setting) involves profit or rate of return. These don't apply well for a security investment.

Total Cost of Ownership (TCO) seeks to quantify the cost over the entire lifecycle of the investment.

- Only really applies to security purchases, not to measurement of the IT security process.
- Data for adequate comparison is lacking.

Lessons from Other Industries

We typically don't have very good data for estimating IT security risk!

Other industries—insurance, manufacturing, design—have a long history of dealing with risk.

Some lessons:

1. Metrics and process will improve as the ability to collect, analyze and understand data improves.
2. *Security is a business process.* You must measure the business process to measure security.
3. *Security results from human activities.* You must understand people as well as technology.

Choosing Good Metrics

One approach: The Goal-Question-Metric (GQM) method borrowed from software engineering.

Goal: *What do I need to accomplish in my security program?* Goals should be specific, limited, meaningful, contextual, well-documented.

Questions: *What specifically must I learn for that goal to be realized?*

Metrics: *What data must I collect to answer the questions raised by the goals?*

GQM provides a structured process for thinking about security, translating thoughts into requirements, and developing the data to meet those requirements.

Example: GQM for Security-Related Downtime

Goal Statement: *Understand security impact on system availability by reviewing security-related downtime as a percentage of total downtime.*

Question 1: How often is the system down due to failure?

Metrics: Time between failures
Failure duration
Mean system availability

Example: GQM for Security-Related Downtime

Question 2: How often is the system down due to maintenance?

Metrics: Time between maintenance events
Maintenance duration
Mean system availability

Question 3: How often is downtime the result of a security event?

Metrics: Number of security events in time period
Duration of event remediation

Are Goals Appropriate? Cisco Example:

The security goals must align with the mission of the enterprise.

Operating System Count & Urgent Vulnerabilities

	# Hosts	# Vuln.	# Hosts w/ Vuln.	% Hosts w/ Vuln.
Windows	4212	593	347	8.2
Linux	8026	62	41	< 1
Solaris	2733	216	143	5.2
Cisco	4626	6	6	< 1

Presented with these findings, Cisco management responded that since Linux and Cisco OS teams "had less than 1 percent of their hosts with high severity vulnerabilities, those teams must be spending too much time, effort and resources patching their hosts." (Hayden, *IT Security Metrics*, p. 84)

Conclusions

- Cyber security is important, but hard.
- Perfect security is impossible, so treat it as risk management.
- Must measure security to improve security.
- Some popular metrics are weak, largely because the underlying data is weak.
- Systematic approaches exist to build successful IT security metrics programs.
- Treat security as another business process.

CS361C: Information Assurance and Security

It's a Dangerous (Cyber) World

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Last updated: January 26, 2015 at 14:28

What I'd Like to Discuss

- The scope of the problem
- Why cyber security is hard
- Are we at (Cyber) war?
- What responses are legal and feasible

From the Headlines

Silent War, Vanity Fair, July 2013

On the hidden battlefields of history's first known cyber-war, the casualties are piling up. In the U.S., many banks have been hit, and the telecommunications industry seriously damaged, likely in retaliation for several major attacks on Iran.

Washington and Tehran are ramping up their cyber-arsenals, built on a black-market digital arms bazaar, enmeshing such high-tech giants as Microsoft, Google, and Apple.

From the Headlines

Iran's supreme leader tells students to prepare for cyber war, rt.com, 2/13/14

Ayatollah Ali Khamenei has delivered a sabre-rattling speech to Iran's 'Revolutionary foster children' (in other words, university students) to prepare for cyber war. The supreme leader has urged his country's students whom he called "cyber war agents" — to prepare for battle.

Israel, Tehran's main adversary in regional politics, has voiced similar statements recently; Major General Aviv Kochavi said that cyber warfare will change the nature of conflict. "Cyber, in my modest opinion, will soon be revealed to be the biggest revolution in warfare, more than gunpowder and the utilization of air power in the last century."

From the Headlines

House Intel Chair Mike Rogers Calls Chinese Cyber Attacks 'Unprecedented', ABC News, 2/24/13

House Intelligence Committee Chair Mike Rogers, R-Mich., said it was "beyond a shadow of a doubt" that the Chinese government and military is behind growing cyber attacks against the United States, saying "we are losing" the war to prevent the attacks.

"It is unprecedented," Rogers added. "This has never happened in the history of the world, where one nation steals the intellectual property to re-purpose it—to illegally compete against the country ... and I'll tell you, It is as bad as I've ever seen it and exponentially getting worse. Why? There's no consequence for it."

From the Headlines

Pentagon accuses China of trying to hack US defence networks, The Guardian, 5/7/13

China is using espionage to acquire technology to fuel its military modernisation, the Pentagon has said, for the first time accusing the Chinese of trying to break into US defense computer networks and prompting a firm denial from Beijing.

From the Headlines

Cyber security in 2013: How vulnerable to attack is US now?, Christian Science Monitor, 1/9/13

The phalanx of cyberthreats aimed squarely at Americans' livelihood became startlingly clear in 2012 and appears poised to proliferate in 2013 and beyond.

That prediction came true:
2013 was the most historic year ever for cyber attacks. The industry saw several mega attacks that included sophisticated DDoS attack methods. (IT Business Edge, 12/16/13)

Do you think that 2014 was even worse? What's your evidence of that?

From the Headlines

U.S. Not Ready for Cyberwar Hostile Attackers Could Launch, The Daily Beast, 2/21/13

The Chinese reportedly have been hacking into U.S. infrastructure, and Leon Panetta says future attacks could plunge the U.S. into chaos.

If we are plunged into chaos and suffer more physical destruction than 50 monster hurricanes and economic damage that dwarfs the Great Depression ... Then we will wonder why we failed to guard against what outgoing Defense Secretary Leon Panetta has termed a "cyber-Pearl Harbor."

The U.S. at Risk?

Experts believe that U.S. is perhaps particularly vulnerable to cyberattack compared to many other countries.

- The U.S. is probably more dependent on technology than any other society on earth.
- Sophisticated attack tools are readily available to anyone on the Internet.
- The openness of U.S. society means critical information and vulnerabilities are accessible.

The U.S. at Risk?

More reasons we're vulnerable:

- Much of the U.S. critical infrastructure is accessible on-line.
- Other nation states have much more control over their national communication infrastructure.
- The defense establishment is drowning in data.
- Technology advances rapidly but remains riddled with vulnerabilities.

How Bad Is It?

Cyberwarfare greater threat to US than terrorism, say security experts, Al Jazeera America, 1/7/14

Cyberwarfare is the greatest threat facing the United States — outstripping even terrorism — according to defense, military, and national security leaders in a Defense News poll, a sign that hawkish warning about an imminent 'cyber Pearl Harbor' have been absorbed in defense circles.

45 percent of the 352 industry leaders polled said cyberwarfare is the gravest danger to the U.S., underlining the government's shift in priority—and resources—toward the burgeoning digital arena of warfare.

The U.S. Government Takes this Seriously

"The Pentagon has concluded that computer sabotage coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force." (Wall Street Journal, 5/31/11)

"The Pentagon plans to triple its cybersecurity staff by 2016, U.S. Secretary of Defense Chuck Hagel announced recently. A few days later, FBI Supervisory Special Agent Charles Gilgen said at a conference on cybercrime that his agency's cyber division plans to hire 1,000 agents and 1,000 analysts in the coming year. Just those two agencies are looking for 6,000 people with cybersecurity skills in the next two years." (Bloomberg Business, 4/15/14)

Current Concern

The Obama administration has placed an emphasis on protection of critical infrastructure from cyber attack.

On 2/12/13, the administration released an executive order *Improving Critical Infrastructure Cybersecurity* and Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience*

> *The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure including assets, networks, and systems that are vital to public confidence and the Nation's safety, prosperity, and well-being.*

But Are We Already at (Cyber) War?

Cyber warfare involves "actions by a nation-state to penetrate another nation's computers or networks for the purpose of causing damage or disruption." –Clarke and Knape.

This definition raises as many questions as it addresses:

- Can't a non-state entity engage in warfare?
- Which computers or networks matter?
- Which actions should qualify as acts of war?
  - Is "warfare" even a useful term in this context?
  - Why not just make our computers and networks impervious to such attacks?

Why Are We At Risk?

Arguably, the only way that another nation-state can "penetrate [our] computers or networks for the purpose of causing damage or disruption" is

1. if they have insider access; or
2. there are exploitable vulnerabilities that allow them to gain remote access.

So, why not just "harden" our computers and networks to remove the vulnerabilities?

Why Security is Hard: Target Rich Environment

From the DoD 2010 *Quadrennial Defense Review*:

"On any given day there are as many as 7 million DoD computers and telecommunication tools in use in 88 countries using war-fighting and support applications. The number of potential vulnerabilities, therefore, is staggering."

That means that there are *lots* of insiders, in addition to the possible vulnerabilities in the software and hardware.

Is Cyber Security Particularly Hard?

But why is cybersecurity any harder than any other technological problem? Or is it?

Partial answer: Most technological problems are concerned with ensuring that something good happens. Security is all about ensuring that *bad things never happen*.

In cybersecurity, you have to defeat an *actively malicious adversary*. Security Guru Ross Anderson characterizes this as *"Programming Satan's Computer."*

Cyber Defense is Asymmetric

The defender has to find and eliminate *all* exploitable vulnerabilities; the attacker only needs to find *one*!

Not only do you have to find "bugs" that make the system behave differently than expected, you have to identify any features of the system that are susceptible to misuse and abuse, *even if your programs behave exactly as you expect them to.*

Cyber Security is Tough

Perfect security is unachievable in any useful system. We trade-off security with other important goals: functionality, usability, efficiency, time-to-market, and simplicity.

© Scott Adams, Inc./Dist. by UFS, Inc.

Is It Getting Better?

"The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it." –Robert H. Morris (mid 1980's), former chief scientist of the National Computer Security Center

"Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement and bury it 100 feet below the ground." –Prof. Fred Chang (2009), former director of research at NSA

Some Sobering Facts

- It is *undecidable* whether a given piece of software contains malicious functionality.
- Once PCs are infected they tend to stay infected. The median length of infection is 300 days.

- "More than 5.5 billion attempted attacks were identified in 2011, an increase of 81 percent over 2010, with an unprecedented 403 million unique malware variants that year, a 41 percent leap." (Symantec Internet Security Threat Report, 2012)

The Cost of Data Breaches

The Privacy Right's Clearinghouse's *Chronology of Data Breaches* (January, 2012) estimates that more than half a billion sensitive records have been breached since 2005. This is actually a very "conservative estimate."

The Ponemon Institute estimates that the approximate current cost per record compromised is around $318.

"A billion here, a billion there, and pretty soon you're talking real money" (attributed to Sen. Everett Dirksen)

Security is About Managing Risk

In *Building Secure Software*, Viega and McGraw assert that software and system security is "all about managing risk." This can be done through:

Risk acceptance: some risks are simply tolerated by the organization.

Risk avoidance: not performing an activity that would incur risk.

Risk mitigation: taking actions to reduce the losses due to a risk.

Risk transfer: shift the risk to someone else.

There is generally much more money in a bank than in a convenience store; but which is more likely to be robbed? Why?

But is it War?

- How real is the threat?
- Is the warfare metaphor a help or a hinderance?
- Are cyberattacks best viewed as crimes, "armed attacks," both, or something else entirely?
- Is this issue about semantics or substance?
- Does it really matter?

Why Does it Matter?

Many experts believe that cyber attacks are a serious risk to U.S. national interests today.

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008

But others argue the threat is overrated and is largely hype by the security establishment.

Is it really warfare or is it just crime, that should be dealt with by the criminal justice establishment?

Warfare: Cyber and Otherwise

In modern parlance, a shooting war is called *kinetic warfare*, where "kinetics" is concerned with the relationship between the motion of bodies and its causes.

Recall Clarke's definition of cyber warfare: "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."

Can activity in cyberspace have kinetic consequences such as property damage and loss of lives? *Does it have to have such consequences to qualify as an act of war?*

The Pentagon View

Cyber Combat: Act of War, Wall Street Journal, 5/31/11

"The Pentagon has concluded that computer sabatoge coming from another country can constitute an act of war, a finding that for the first time opens the door for the U.S. to respond using traditional military force. ...

One idea gaining momentum at the Pentagon in the notion of 'equivalence.' If a cyber attack produces the death, damage, destruction, or high level disruption that a traditional military attack could cause, it would be a candidate for a 'use of force' consideration."

Notable Cyber Campaigns

First Persian Gulf War (1991): Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

Estonia (2007): Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

Georgia (2008): Russia attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

What Might an Attack Look Like: Stuxnet

Stuxnet is a Windows computer worm discovered in July 2010 that targets Siemens SCADA (Supervisory Control and Data Acquisition) systems.

In interviews over the past three months in the United States and Europe, experts who have picked apart the computer worm describe it as far more complex and ingenious than anything they had imagined when it began circulating around the world, unexplained, in mid-2009. –New York Times, 1/16/11

Stuxnet Characteristics

Stuxnet is the new face of 21st-century warfare: invisible, anonymous, and devastating. ... Stuxnet was the first literal cyber-weapon. America's own critical infrastructure is a sitting target for attacks like this.
(Vanity Fair, April 2011)

- Stuxnet was the first (known) malware that subverts specific industrial systems.
- Believed to have involved years of effort by skilled hackers to develop and deploy.
- Narrowly targeted, quite possibly at Iran's nuclear centrifuges.
- Widely believed to have been developed by Israel and the U.S.

Stuxnet Worm

Kaspersky Lab Provides Its Insights on Stuxnet Worm, Kaspersky.com, 9/24/10

"I think that this is the turning point, this is the time when we got to a really new world, because in the past there were just cyber-criminals, now I am afraid it is the time of cyber-terrorism, cyber-weapons and cyber-wars."

Children of Stuxnet

The successors of Stuxnet may be even more sophisticated:

DuQu: (Sept. 2011) looks for information that could be useful in attacking industrial control systems.

Flame: (May 2012) designed for cyber-espionage, targeted government organizations and educational institutions in Iran and elsewhere.

Gauss: (Aug. 2012) complex cyber-espionage toolkit designed to steal sensitive data.

Unlike conventional munitions, could be repurposed and redirected at the sender.

Cyber Attacks on the U.S.

The U.S. has already been "attacked" in the sense of cyber espionage.

Moonlight Maze: coordinated attacks on U.S. computer systems in 1999, traced to a computer in Moscow. Hackers obtained large stores of data possibly including classified naval codes and information on missile guidance systems.

Titan Rain: series of coordinated attacks on U.S. computer systems since 2003. Probably Chinese in origin and probably gathering intelligence; *an estimated 10-20 terabytes of data may have been downloaded.*

There are undoubtedly others that we don't yet know about.

Does This Go Beyond Espionage?

Some security experts warn that a successful possible widespread attack on U.S. computing infrastructure *could largely shut down the U.S. economy for up to 6 months.*

It is estimated that the destruction from a single wave of cyber attacks on U.S. critical infrastructures could exceed $700 billion USD—the equivalent of 50 major hurricanes hitting U.S. soil at once. (Source: US Cyber Consequences Unit, July 2007)

CyberAttacks: An Existential Threat?

Cyberattacks an 'Existential Threat' to U.S., FBI Says, Computerworld, 3/24/10

A top FBI official warned today that many cyber-adversaries of the U.S. have the ability to access virtually any computer system, posing a risk that's so great it could "challenge our country's very existence."

According to Steven Chabinsky, deputy assistant director of the FBI's cyber division: "The cyber threat can be an existential threat—meaning it can challenge our country's very existence, or significantly alter our nation's potential."

Not Everyone Agrees

Howard Schmidt, the new cybersecurity czar for the Obama administration, has a short answer for the drumbeat of rhetoric claiming the United States is caught up in a cyberwar that it is losing. "There is no cyberwar. I think that is a terrible metaphor and I think that is a terrible concept," Schmidt said. "There are no winners in that environment." (Wired, 3/4/10)

Does Mr. Schmidt think there is no problem? Or just that we're calling it by the wrong name?

Not Everyone Agrees

The cyberwar rhetoric is dangerous. Its practitioners are artists of exaggeration, who seem to think spinning tall tales is the only way to make bureaucracies move in the right direction. ... Not only does it promote unnecessary fear, it feeds the forces of parochial nationalism and militarism undermining a communications system that has arguably done more to connect the world's citizens than the last 50 years of diplomacy. (Ryan Singel review of Clarke and Knape in Wired, 4/22/10)

Is a Cyber Attack an Act of War?

There are some serious questions that deserve national and international dialogue.

- How serious would a cyber attack have to be considered an "act of war"?
- What if it were an act by *non-state* actors?
- Would it require *certainty* about who initiated it?
- What degree of control would the offending nation have to exert over such actors?
- Must the response be electronic or could it be a "kinetic"?

An Act of War?

According to the McAfee *2009 Virtual Criminology Report*:

"When determining whether a cyber attack is an act of cyber war, experts evaluate four key attack attributes:

- **Source:** Was the attack carried out or supported by a nation-state?
- **Consequence:** Did the attack cause harm?
- **Motivation:** Was the attack politically motivated?
- **Sophistication:** Did the attack require customized methods and/or complex planning?"

What do you think of these criteria? Are they precise enough to be useful?

Cyber Attacks as Armed Attacks

Various international conventions allow a self-defense or "anticipatory self-defense" response to an *armed attack*. But they don't define "armed attack."

So, when is a cyber attack "equivalent" to an armed attack?

At least three different analytic frameworks have been proposed:

Instrument-based: the damage is such that it previously could only have been caused by a kinetic attack.

Effects-based: what are the overall effects of the attack on the victim state.

Strict liability: attacks against critical infrastructure qualify because of the potential serious consequences.

Which of these analytic frameworks do you find most reasonable?

Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

Selecting Targets

In traditional warfare, the targets tend to be *military*, or industrial sites with military value. Maybe it's too obvious, but why is that?

1. Military and industrial targets allow the enemy to counterattack, so have high value.
2. Military assets are likely to be on the defensive perimeter.
3. Certain principles (are supposed to) regulate the conduct of states during warfare.

Selecting Targets

States are supposed to adhere to certain criteria in selecting targets:

- **Distinction:** requires distinguishing combatants from non-combatants and directing actions against military objectives
- **Necessity:** limits force to that "necessary to accomplish a valid military objective"
- **Humanity:** prohibits weapons designed "to cause unnecessary suffering"
- **Proportionality:** protects civilians and property against excessive uses of force

Do these apply to cyberattacks? To responses to cyberattacks?

Targets

There are good reasons to believe that the choice of targets might be different in cyber vs. kinetic warfare.

- Non-state actors may not feel bound by the conventional laws of war.
- The actors may be in an asymmetric power relationship.
- Non-state actors may be looking for "soft" high-value targets.
- Cyber attacks offer the ability to "skip the battlefield."

Systems that people rely upon, from banks to air defense radars, are accessible from cyberspace and can be quickly taken over or knocked out without first defeating a country's traditional defenses. –*Clarke and Knape, 31*

Targets

In a cyberattack, targets could be: *military, civil or private sector.*

If a major cyber conflict between nation-states were to erupt, it is very likely that the private sector would get caught in the crossfire. Most experts agree that critical infrastructure systems—such as the electrical grid, banking and finance, and oil and gas sectors—are vulnerable in many countries. Some nation-states are actively doing reconnaissance to identify specific vulnerabilities. –McAfee report, 3

Targets

If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet. –McAfee report, 16

Protecting Critical Infrastructure

The government takes protection of infrastructure very seriously. Presidential Decision Directive (PDD-63) of 1998 states:

- Civilian systems are "essential to the minimum operations of the economy and government"
- Examples: telecommunications, energy, banking, transportation and emergency services

Surely such systems are not vulnerable to cyberattack. Nobody would be dumb enough to make such critical functionality accessible remotely. Would they?

How Vulnerable is Our Infrastructure?

Surely our critical infrastructure is not vulnerable to cyberattack. Nobody would be dumb enough to make such critical functionality accessible remotely. *Would they?*

"I have yet to meet anyone who thinks SCADA systems should be connected to the Internet. But the reality is that SCADA systems need regular updates from a central control, and it is cheaper to do this through an existing Internet connection than to manually move data or build a separate network." –Greg Day, Principal Security Analyst at McAfee

Non-State Actors

Should a nation-state act against another nation-state in response to actions by a non-state actor?

Did the Afghan government (Taliban) attack the World Trade Center and Pentagon on September 11, 2001?

Did Russia actively organize, encourage and facilitate private hackers participating in the cyber attacks on Georgia and Estonia?

Herb Lin, Senior Scientist of the National Academy of Sciences, said that cyberattacks against the U.S. *go up* during exam periods in China. *What do you think that's about?*

Active vs. Passive Defenses

Defenses against cyber attack can be:

Passive: taking steps to prevent an attack or to mitigate the damage should an attack occur (access control, secure system design, security administration).

Active: electronic measures designed to strike attacking computer systems and shut down an attack midstream (destructive viruses, packet flooding)

Most effective approach is probably a *layered* defense or *"defense in depth"* incorporating both approaches.

But victim states often worry that active defenses may violate the laws of war.

The Attribution Problem

Often it is extremely difficult to determine the source of a cyber attack.

"States find themselves in a 'response crisis' during a cyber attack, forced to decide between effective but arguably illegal, active defenses, and the less effective, but legal, passive defenses and criminal laws." –Carr, *Inside Cyber Warfare*, 47

The Law of War

How do the laws of war apply to cyber attacks?

Laws of war arose in a conventional context in which:

- it is easy to assess the damage following an attack, and
- it is typically easy to identify the attacker.

"Current international law is not adequate for addressing cyber war. Analogies to environmental law, law of the sea and kinetic war all break down at some point. Answering the question of when to use force in response to a cyber attack needs its own framework." –Eneken Tikk, legal advisor for the Cooperative Cyber Defence Centre of Excellence in Estonia

The Prevailing View

According to Lt. Cmd Matt Sklerov (quoted in Carr, 47):

"The prevailing view of states and legal scholars is that states must treat cyber attacks as a criminal matter

1. out of uncertainty over whether a cyberattack can even qualify as an armed attack, and
2. because the law of war requires states to attribute an armed attack to a foreign government or its agents before responding with force."

The Crime-Based Approach

If you treat cyber attacks as a criminal matter, with deterrence from criminal laws and penalties, *how do you force states to comply with international criminal laws?*

- "Several major states, such as China and Russia, allow their attackers to operate with impunity when their attacks target rival states." (Carr, 47)
- "International legal acts regulating relations arising in the process of combating cyber crimes and cyber terrorism must not contain norms violating such immutable principles of international law as non-interference in the internal affairs of other states, and the sovereignty of the latter." (Moscow Military Thought, 3/31/97)

U.N. Charter

The U.N. Charter preserves the right of states to engage in "individual or collective self-defense" in response to an "armed attack." (Article 51).

However, that begs the question of when a cyber attack should be considered an "armed attack."

The Law of War

States have a long-standing duty to prevent non-state actors from using their territory to commit cross-border attacks, including the requirement for states to act against groups generally known to carry out illegal attacks.

Sklerov suggests that duty "should be interpreted to require states to enact and enforce criminal laws to deter cross-border cyber attacks."

A state which fails to do so could be labeled a *sanctuary state* and sanctioned by the international community.

The Laws of War

In the cases relating to war crimes in the former Yugoslavia, it was allowed:

> *to impute host-state responsibility for the actions of groups of non-state actors when a state exercised "overall control" of the group, even though the state may not have directed the particular act in question.* (*Prosecutor vs. Tadic*)

International Agreements

Most directly relevant is the European Convention on Cybercrime, which recognizes the need of states to criminalize cyber attacks and the duty of states to prevent non-state actors on their territory from launching them.

- requires states to establish domestic criminal offenses for most types of cyber attacks
- recognizes the importance of prosecuting attackers
- requires extending jurisdiction to cover a state's territory and actions of citizens regardless of their location.

The Convention has been signed by 26 countries including the U.S.

Conclusions

- Cyber attacks are a serious threat to the U.S. and other states.
- Cyber warfare may not be a helpful metaphor.
- The nature of the Internet makes cyber attacks powerful, difficult to counter, and difficult to attribute.
- No technical solutions are on the horizon.
  - Treaties and legal frameworks have not kept pace with the threat.
  - Promising theories and approaches are developing to help the international community cope.

CS361C: Information Assurance and Security

Introduction to IA

Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: February 2, 2015 at 06:38

Some Sources

- Andrew Blyth and Gerald L. Kovacich, *Information Assurance: Surviving in the Information Environment*: Springer, 2001.
- Debra S. Herrmann, *Complete Guide to Security and Privacy Metrics*: Auerbach, 2007.
- Douglas J. Landoll, *The Security Risk Assessment Handbook*: Auerbach, 2006.
- Michael E. Whitman and Herbert J. Mattord, *Principles of Information Security*: Thomson, 2009.
- Bel G. Raggad, *Information Security Management: Concepts and Practice*: CRC Press, 2010.

Thought Experiment

Suppose you visit an e-commerce website such as your bank, stock broker, etc.

Before you type in highly sensitive information, you'd like to have some assurance that your information will be protected. Do you (have such assurance)? How can you know?

What security-relevant things do you want to happen, or not happen when you use such a website?

Thought Experiment

You might want:

- Privacy of your data
- Protection against phishing
- Integrity of your data
- Authentication
- Authorization
- Confidentiality
- Non-repudiation
- Availability
- What else?

Which of these do you think fall under Information Assurance?

System Quality

According to ISO/IEC Standard 9126-1 (Software Engineering—Product Quality), the following are all aspects of system quality:

- functionality
  - adequacy
  - interoperability
  - correctness
  - security
- reliability
- usability
- efficiency
- maintainability
- portability

Which of these do you think apply to IA?

What is Information?

This class is about *Information Assurance*; so what is "information"? How does information differ from data?

What is Information?

This class is about *Information Assurance*; so what is "information"? How does information differ from data?

"Information is data endowed with relevance and purpose. Converting data into information thus requires knowledge. Knowledge by definition is specialized." *(Blyth and Kovacich, p. 17)*

And what characteristics should information possess to be useful?

It should be: accurate, timely, complete, verifiable, consistent, available.

What is Information?

According to Raggad (pp. 14ff), the following are all distinct conceptual resources:

Noise: raw facts with an unknown coding system

Data: raw facts with a known coding system

Information: processed data

Knowledge: accepted facts, principles, or rules of thumb that are useful for specific domains. Knowledge can be the result of inferences and implications produced from simple information facts.

What is Information Assurance?

What about "assurance"? What does that mean? Assurance from what or to do what? Is it context-dependent?

What is Information Assurance?

What about "assurance"? What does that mean? Assurance from what or to do what? Is it context-dependent?

According to the U.S. Department of Defense, IA involves:

> *Actions taken that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities.*

Information Assurance (IA) is the study of how to protect your information assets from destruction, degradation, manipulation and exploitation. But also, how to recover should any of those happen. *Notice that it is both proactive and reactive.*

What is IA? (cont)

According to the DoD definition, these are some aspects of information needing protection:

Availability: timely, reliable access to data and information services for authorized users;

Integrity: protection against unauthorized modification or destruction of information;

Confidentiality: assurance that information is not disclosed to unauthorized persons;

Authentication: security measures to establish the validity of a transmission, message, or originator.

Non-repudiation: assurance that the sender is provided with proof of a data delivery and recipient is provided with proof of the sender's identity, so that neither can later deny having processed the data.

Is this specifically a military view? Which of these are the most important? How would you decide?

What is IA?

Information Assurance is such a broad field that there is no universally accepted definition. Researchers often give their own spin to IA, usually reflecting their own concerns.

In these slides, are several different views of IA, including the DoD view (above), Herrmann's view (below), and Blyth and Kovacich's view (below). Be able to compare and contrast these views.

A Different View of IA

According to Debra Herrmann (*Complete Guide to Security and Privacy Metrics*), IA should be viewed as spanning four security engineering domains:

- physical security
- personnel security
- IT security
- operational security

> *The simple truth is that IT security cannot be accomplished in a vacuum, because there are a multitude of dependencies and interactions among all four security engineering domains.* *(Herrmann, p. 10)*

So threats/risks to IA should be considered along these dimensions as well.

A Different View of IA

According to Debra Herrmann, IA has four major categories:

- physical security
- personnel security
- IT security
- operational security

Into which of these would you put the following?

- enforcing hard-to-guess passwords
- encrypting your hard drive
- locking sensitive documents in a safe
- stationing a marine guard outside an embassy
- assigning security clearances to staffers
- using SSL for data transfers
- having off-site backup of documents

Four Security Domains

Quotes from Debra Herrmann, *Complete Guide to Security and Privacy Metrics*:

"*Physical security* refers to the protection of hardware, software, and data against physical threats to reduce or prevent disruptions to operations and services and loss of assets."

"*Personnel security* is a variety of ongoing measures taken to reduce the likelihood and severity of accidental and intentional alteration, destruction, misappropriation, misuse, misconfiguration, unauthorized distribution, and unavailability of an organization's logical and physical assets, as the result of action or inaction by insiders and known outsiders, such as business partners."

Four Security Domains

"*IT security* is the inherent technical features and functions that collectively contribute to an IT infrastructure achieving and sustaining confidentiality, integrity, availability, accountability, authenticity, and reliability."

"*Operational security* involves the implementation of standard operational security procedures that define the nature and frequency of the interaction between users, systems, and system resources, the purpose of which is to

1. achieve and sustain a known secure system state at all times, and
2. prevent accidental or intentional theft, release, destruction, alteration, misuse, or sabotage of system resources."

Are these domains purely defensive, or might they be offensive? Compare and contrast Herrmann's view of IA with the government view outlined before.

Yet Another Perspective

According to Raggad's taxonomy of information security, a computing environment is made up of five continuously interacting components:

- activities,
- people,
- data,
- technology,
- networks.

A comprehensive security plan must take all of these into account. How do these map onto the previous scheme?

Does protecting a computing environment merely mean protecting these five components?

Yet Another View: Components of IA

IA includes computer and information security, but more besides. According to Blyth and Kovacich, IA can be thought of as protecting information at three distinct levels:

- **physical:** data and data processing activities in physical space;
- **information infrastructure:** information and data manipulation abilities in cyberspace;
- **perceptual:** knowledge and understanding in human decision space.

IA Levels: the Physical

The lowest level focus of IA is the physical level: computers, physical networks, telecommunications and supporting systems such as power, facilities and environmental controls. Also at this level are the people who manage the systems.

Desired Effects: to affect the technical performance and the capability of physical systems, to disrupt the capabilities of the defender.

Attacker's Operations: physical attack and destruction, including: electromagnetic attack, visual spying, intrusion, scavenging and removal, wiretapping, interference, and eavesdropping.

Defender's Operations: physical security, OPSEC, TEMPEST.

IA Levels: Infrastructure

The second level focus of IA is the information structure level. This covers information and data manipulation ability maintained in cyberspace, including: data structures, processes and programs, protocols, data content and databases.

Desired Effects: to influence the effectiveness and performance of information functions supporting perception, decision making, and control of physical processes.

Attacker's Operations: impersonation, piggybacking, spoofing, network attacks, malware, authorization attacks, active misuse, and denial of service attacks.

Defender's Operations: information security technical measures such as: encryption and key management, intrusion detection, anti-virus software, auditing, redundancy, firewalls, policies and standards.

IA Levels: Perceptual

The third level focus of IA is the perceptual level, also called *social engineering*. This is abstract and concerned with the management of perceptions of the target, particularly those persons making security decisions.

Desired Effects: to influence decisions and behaviors.

Attacker's Operations: psychological operations such as: deception, blackmail, bribery and corruption, social engineering, trademark and copyright infringement, defamation, diplomacy, creating distrust.

Defender's Operations: personnel security including psychological testing, education, and screening such as biometrics, watermarks, keys, passwords.

IA Overview

Thus, IA includes aspects of:

- COMPSEC: computer security;
- COMSEC: communications and network security;
- ITSEC: (which includes both COMPSEC and COMSEC);
- OPSEC: operations security.

Compare Blyth and Kovacich's view of IA with the government view and Herrmann's views described previously.

IA Overview

If you entrench yourself behind strong fortifications, you compel the enemy to seek a solution elsewhere. –Carl von Clausewitz

A recent headline in the AAS read: "The Biggest Threat to Computer Security? Carelessness"

Principle of Easiest Penetration: An attacker on any information system will use the simplest means of subverting system security.

Many IA Failures Don't Involve Technology

In 1996, news of possible signs of life in a Martian meteorite called ALH84001 leaked out ahead of a press conference that had been scheduled by NASA.

This was partly because a high-ranking White House official told a prostitute about the meteorite, who then sold the information to a tabloid.

NASA had to scramble to reschedule its press conference to an earlier date to satisfy the growing demand for information from the press and the public.

The Information Warfare Spin on IA

The flip side of Information Assurance is Information Warfare (IW). In fact, one can think of the offensive part of IW as "information operations," and the defensive part as information assurance.

- *Type I* involves managing an opponent's perception through deception and psychological operations. In military circles, this is called *Truth Projection*.
- *Type II* involves denying, destroying, degrading, or distorting the opponent's information flows to disrupt their ability to carry out or co-ordinate operations.
- *Type III* gathers intelligence by exploiting the opponent's use of information systems.

IW can be carried out against individuals, corporations, or nations. Is hacking IW?

Nature of the Threat

Necessary for IW, as for any related activity, are *motive*, *means*, and *opportunity*.

In general, the offensive players in the world of IW come in six types:

- **Insiders:** consists of employees, former employees and contractors.
- **Hackers:** one who gains unauthorized access to or breaks into information systems for thrills, challenge, power, or profit.
- **Criminals:** target information that may be of value to them: bank accounts, credit card information, intellectual property, etc.

Nature of the Threat (cont.)

Corporations: actively seek intelligence about competitors or steal trade secrets.

Governments and agencies: seek the military, diplomatic, and economic secrets of foreign governments, foreign corporations, and adversaries. May also target domestic adversaries.

Terrorists: usually politically motivated and may seek to cause maximal damage to information infrastructure as well as endanger lives and property.

Is there overlap among these categories of actors? Which do you think is the biggest threat? Does it depend on the target?

Why Does it Matter?

It's a dangerous world out there.

> *While experts may disagree on the definition of cyber war, there is significant evidence that nations around the world are developing, testing and in some cases using or encouraging cyber means as a method of obtaining political advantage.* –*McAfee Virtual Criminology Report 2009*

> *A plausible worst-case worm could cause $50 billion or more in direct economic damage by attacking widely used services in Microsoft Windows and carrying a highly destructive payload."* –*Nicholas Weaver and Vern Paxson, 6/14/04*

Why Does it Matter?

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –*CSIS report on Securing Cyberspace for the 44th Presidency, Dec. 2008*

IA Functional Components

Note that IA is both proactive and reactive involving: *protection, detection, capability restoration, and response.*

- *IA environment protection pillars:* "ensure the availability, integrity, authenticity, confidentiality, and non-repudiation of information"
- *Attack detection:* "timely attack detection and reporting is key to initiating the restoration and response processes."

IA Functional Components (2)

- *Capability restoration:*
  - "relies on established procedures and mechanisms for prioritizing restoration of essential functions. Capability restoration may rely on backup or redundant links, information system components, or alternative means of information transfer."
  - "A post-attack analysis should be conducted to determine the command vulnerabilities and recommended security improvements."
- *Attack response:* "involves determining actors and their motives, establishing cause and complicity, and may involve appropriate action against perpetrators... contributes ... by removing threats and enhancing deterrence."

IA Applies to Info Infrastructure

If adversaries intended to attack nations in cyber space, they would select targets which would cause the largest impacts and losses to their opponents with the least effort. It is therefore a very reasonable assumption that adversaries would attack critical infrastructure systems via the Internet. –McAfee Virtual Criminology Report 2009, p. 16

- *Global Information Infrastructure:* "worldwide interconnection of communication networks, computers, databases, and consumer electronics that make vast amounts of information available to users."
- *National Information Infrastructure:* those within or serving the U.S., for government, commerce and research.
- *Defense Information Infrastructure:* those within or serving the DoD (e.g. nodes on SIPRNET and NIPRNET).

Critical Infrastructure Protection

Presidential Decision Directive (PDD-63) of 1998

- Civilian systems are "essential to the minimum operations of the economy and government"
- Examples: telecommunications, energy, banking, transportation and emergency services

Increased vulnerability as:

- information systems have become automated and interlinked;
- information systems are using COTS technology, subject to viruses, worms, etc.

Every federal department CIO is responsible for information assurance.

Federal Orgs Defining IA

Committee on National Security Systems (CNSS)

- Designation of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), chaired by DoD.
- Establishes federal policy directives on network security.
- Sanctions universities to offer security certification.

National Security Agency (NSA)

- Lead cryptographic organization
- Builds and tests secure systems for classified applications
- Coordinates with industry on security development

National Institute of Standards and Technology (NIST)

- Formerly National Bureau of Standards (NBS)
- Leverages NSA's experience in standardizing cryptosystems for civilian use. E.g. DES, SHA, AES.

IA Relationship to Computer Security

- IA includes considerations for non-security threats to information systems, such as acts of nature and the process of recovery from incidents.
- IA *emphasizes management, process, and human involvement*, and not merely technology.
- IA deployments may involve multiple disciplines of security:
  - COMPUSEC (Computer security)
  - COMSEC (Communications security), SIGSEC (Signals security) and TRANSEC (transmission security)
  - EMSEC (Emanations security) denying access to informatoin from unintended emanations such as radio and electrical signals
  - OPSEC (Operations security) the processes involved in protecting information

Some Basic IA Terms

A complete IA glossary can be found at: *National Information Assurance Glossary*, `www.cnss.gov/Assets/pdf/cnssi_4009.pdf`.

Assets

An *asset* is the resource being protected, including:

- **physical assets**: devices, computers, people;
- **logical assets**: information, data (in transmission, storage, or processing), and intellectual property;
- **system assets**: any software, hardware, data, administrative, physical, communications, or personnel resource within an information system.

Assets have value so are worth protecting.

Subjects and Objects

Often a security solution/policy is phrased in terms of the following three categories:

- **Objects:** the items being protected by the system (documents, files, directories, databases, transactions, etc.)
- **Subjects:** entities (users, processes, etc.) that execute activities and request access to objects.
- **Actions:** operations, primitive or complex, that can operate on objects and must be controlled.

For example, in the Unix operating system, processes (subjects) may have permission to perform read, write or execute (actions) on files (objects). In addition, processes can create other processes, create and delete files, etc. Certain processes (running with `root` permission) can do almost anything. That is one approach to the security problem.

Can an entity be both a subject and an object?

Attributes

Both subjects and objects have associated *attributes*. The security mechanisms may operate in terms on the attributes and manipulation of the attributes can be used to subvert security.

What are some attributes associated with subjects? With objects? How are attributes established/changed?

Critical Aspects

Information assets (objects) may have critical aspects:

- **availability:** authorized users are able to access it;
- **accuracy:** the information is free of error and has the value expected;
- **authenticity:** the information is genuine;
- **confidentiality:** the information has not been disclosed to unauthorized parties;
- **integrity:** the information is whole, complete and uncorrupted;
- **utility:** the information has value for the intended purpose;
- **possession:** the data is under authorized ownership and control.

Terms: Threat and Threat Actors

A *threat* is a *category* of entities, or a circumstance, that poses a potential danger to an asset (through unauthorized access, destruction, disclosure, modification or denial of service).

- Threats can be categorized by intent: accidental or purposeful (error, fraud, hostile intelligence);
- Threats can be categorized by the kind of entity involved: human (hackers, someone flipping a switch), processing (malicious code, sniffers), natural (flood, earthquake);
- Threats can be categorized by impact: type of asset, consequences.

A *threat actor* is a specific instance of a threat, e.g. a specific hacker, a particular storm, etc.

Examples of Threats

Interruption: an asset becomes unusable, unavailable, or lost.

Interception: an unauthorized party gains access to an information asset.

Modification: an unauthorized party tampers with an asset.

Fabrication: an asset has been counterfeit.

Give examples of each of these.

Examples of Threats

Interruption: an asset becomes unusable, unavailable, or lost.

Interception: an unauthorized party gains access to an information asset.

Modification: an unauthorized party tampers with an asset.

Fabrication: an asset has been counterfeit.

Give examples of each of these.

Examples:

Interruption: a denial of service attack on a website

Interception: compromise of confidential data, e.g., but packet sniffing

Modification: hacking to deface a website

Fabrication: spoofing attacks in a network

Terms: Environments, Enclaves

A *hostile environment* for assets is one that has known threats. Example: locating an asset in a war zone or a flood zone, or placing an unprotected machine on the Internet.

A *benign environment* is a nonhostile environment that may be protected from external hostile elements by physical, personnel, and procedural countermeasures.

An *enclave* is a collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security.

Describe a local enclave here at UT?

Terms: Vulnerabilities and Exploits

A *vulnerability* is a weakness or fault in a system that exposes information to attack.

- A bug in a computer program is a very common vulnerability in computer security (e.g. buffer overflow situation).
- A procedural failing can subvert technology controls (e.g. a core dump of secure information upon a failure).
- A lack of controls can result in vulnerabilities, if controls are subverted (e.g. Enron financials).

An *exploit* is a method for taking advantage of a known vulnerability.

What's the difference between an exploit and an attack?

Terms: Vulnerabilities and Exploits

A *dangling vulnerability* is one for which there is no known threat (vulnerability is there but not exploitable).

A *dangling threat* is one that does not pose a danger as there is no vulnerability to exploit (threat is there, but can't do damage).

Can you give examples of these or situations in which they might occur?

Terms: Attacks, etc.

An *attack* is an attempt to gain access, cause damage to or otherwise compromise information and/or systems that support it.

Passive attack: an attack in which the attacker observes interaction with the system.

Active attack: at attack in which the attacker directly interacts with the system.

Unintentional attack: an attack where there is not a deliberate goal of misuse

Terms: Attacks, etc. (2)

Attacks have a subject and object.

Attack subject: the active entity, usually a threat actor, that interacts with the system.

Attack object: the targeted information system asset.

The *attack surface* of an organization/entity is the set of ways in which an adversary can enter the system and potentially cause damage. For example:

> *The attack surface of a software environment is the code within a computer system that can be run by unauthenticated users. This includes, but is not limited to: user input fields, protocols, interfaces, and services. (Wikipedia)*

Mention some ways in which the attack surface can be reduced.

Terms: Exposure, Compromise

Exposure is an instance when the system is vulnerable to attack.

A *compromise* is a situation in which the attacker has succeeded.

An *indicator* is a recognized action—specific, generalized or theoretical—that an adversary (threat actor) might be expected to take in preparation for an attack.

Give an example of an indicator.

Terms: Consequences

A *consequence* is the outcome of an attack. In a purposeful threat, the threat actor has typically chosen a desired consequence for the attack, and selects the IA objective to target to achieve this.

Disruption: targets availability

Corruption: targets integrity

Exploitation: targets confidentiality

A consequence may cause the information system to lose effectiveness, and may have other costs.

Inadvertant disclosure is a type of consequence, involving accidental exposure of information to an agent not authorized access.

Terms: Countermeasures

Controls, *safeguards* and *countermeasures* are any actions, devices, procedures, techniques and other measures that reduce the vulnerability of an information system. There are many kinds:

- technical
- policy, procedures and practices
- education, training and awareness
- cover and deception (camouflage)
- human intelligence (HUMINT), e.g. disinformation
- monitoring of data and transmissions
- surveillance countermeasures that detect or neutralize sensors, e.g. TEMPEST
- assessments and inspections.

A *security posture* or security profile is the implementation (policy, procedures, technology) of the security effort within an organization.

Terms: Risk

Viega and McGraw, *Building Secure Software* assert that software and system security is "all about managing risk." Do you agree? Why or why not?

Risk is the possibility that a particular threat will adversely impact an information system by exploiting a particular vulnerability. The assessment of risk must take into account the consequences of an exploit.

Risk management is a process for an organization to identify and address the risks in their environment. There are several *risk management frameworks*, and each defines a procedure for an organization to follow.

Risk Management Framework

One particular risk management procedure (from Viega and McGraw) consists of six steps:

1. Assess assets
2. Assess threats
3. Assess vulnerabilities
4. Assess risks
5. Prioritize countermeasure options
6. Make risk management decisions

Thought experiment: try to follow this procedure to manage risks to your material possessions stored at your home or apartment.

Risk Treatments

Once the risk has been identified and assessed, managing the risk can be done through one of four techniques:

Risk acceptance: risks not avoided or transferred are retained by the organization. E.g. sometimes the cost of insurance is greater than the potential loss. Sometimes the loss is improbable, though catastrophic.

Risk avoidance: not performing an activity that would incur risk. E.g. disallow remote login.

Risk mitigation: taking actions to reduce the losses due to a risk; many technical countermeasures fall into this category.

Risk transfer: shift the risk to someone else. E.g. most insurance contracts, home security systems.

Risk Management

The risk treatments—acceptance, avoidance, mitigation, transfer—are with respect to a *specific risk for a specific pary.*

E.g., buying insurance is risk transfer for you, not for the insurance company. For the insurance company, it's risk acceptance. But they may require you to take measures to avoid or mitigate their risk.

There is generally more money in a bank than in a convenience store; but which is more likely to be robbed? Why? Of which risk management technique(s) is this an instance?

Mitigation versus Avoidance

There is often a confusion about the difference between *risk avoidance* and *risk mitigation*.

Risk avoidance is about preventing the risk from being actualized. E.g., not parking in a high crime area.

Risk mitigation is about limiting the damage should the risk be actualized. E.g., having a LoJack or cheap car stereo.

Note the risk in this case is that your car will be broken into.

Terms: Trust and Assurance

Trust is a generic term that implies a mechanism in place to provide a basis for confidence in the reliability/security of the system. Failure of the mechanism may destroy the basis for trust.

Trust mechanisms are the security features of a system that provide enforcement of a security policy.

The *trusted computing base* (TCB) is a collection of all the trust mechanisms of a computer system which collectively enforce the policy.

Assurance is a measure of confidence that the security features, practices, procedures, and architecture of a system accurately mediates and enforces the security policy.

Trust Management

The concept of *trust management* provides a unified approach to conceptualizing (parts of) IA. That is, a big part of IA is about controlling interactions among:

- actions
- principals
- policies
- credentials

Various policy management systems have been built with the goal of formalizing and describing these relationships: KeyNote (1999) and Extensible Access Control Markup Language (XACML) (2009).

These provide formal mechanisms for defining policy languages.

Why do you think that trust is a vital component of IA?

Lifecycle

A *lifecycle* is the process by which an asset is managed from its arrival or creation to its termination or destruction.

Software engineering defines several lifecycle models for the development or acquisition of computer software. in a *waterfall model*, the process is divided into stages performed sequentially:

- Requirements
- Design
- Coding
- Testing
- Deployment
- Production
- Decommission

Security Systems Lifecycle Management

Security systems lifecycle management is a process by which the project managers for a system will ensure that appropriate information assurance safeguards are incorporated into a system.

The stages leading to acquisition by the government of a secured system might be:

1. evaluation of sensitivity of the application based on risk analysis
2. determination of security specifications
3. design review and perform system tests to ensure safeguards are adequate, through testing and validation that the product meets specifications
4. system certification and accreditation, issuance of a certificate that the system meets the need and can be procured.

Assurance Requirements

Some indication of various types of lifecycle concerns appear in the Common Criteria "Assurance requirements", including:

Class APE, ASE: *System Evaluation*.

Class ACM: *Configuration Management*, includes CM automation, capabilities, and scope.

Class ADO: *Delivery and Operations*, includes delivery and installation, and generation and set-up.

Class ADV: *Development*, includes functional specification, low-level design, implementation representation, TSF internals, high-level design, representation correspondence, and security policy modeling.

Assurance Requirements (2)

Class AGC: *Guidance Documentation*, includes administrator guidance, and user guidance.

Class ALC: *Life Cycle*, includes development security, flaw remediation, tools and techniques, and life cycle definition.

Class ATE: *Tests*, includes test coverage, test depth, functional tests, and independent testing.

Class AVA: *Vulnerability Assessment*, includes covert channel analysis, misuses, strength of functions, and vulnerability analysis.

Class AMA: *Maintenance of Assurance*, includes assurance maintenance plan, component categorization, evidence of assurance maintenance, and security impact analysis.

CS378: Information Assurance and Security

IA in the Military

Dr. Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: February 6, 2015 at 08:38

Why Study the Military

Why study IA in military contexts?

Why Study the Military

Why study IA in military contexts?

- Excellent case study for both defensive and offensive IA.
- Critically important protection domain that affects all of our lives.
- Historically, that's where IA has been developed.
- Most of the lessons of military IA can be adapted to other IA contexts.
- Others (?)

IA in the Military

Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

IA in the Military

Historically, much of the work in Information Assurance has been contracted/subsidized by the military. Why do you think that is? Why does the government (particularly) care about IA?

- The stakes are high: national security, national prestige, international advantage.
- IA is part of an intelligent defensive/offensive posture.
- The government has deep pockets and can afford to support broader research than other entities.
- Govt. concern for the national welfare goes well beyond strictly military matters. E.g., Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.
- Others?

U.S. DOD IA Emblem

McAfee Report Findings

McAfee's *Virtual Criminology Report 2009* was focused on cyber warfare. They reported three key findings:

1. Although there is no commonly accepted definition for cyber war today, we have seen nation-states involved in varying levels of cyber-conflict.
2. If a major cyber conflict between nation states were to erupt, it is very likely that the private sector would get caught in the crossfire.
3. Too much of the debate on policies related to cyber war is happening behind closed doors.

1940–1960: IA Prehistory

IA is an outgrowth of (predominately US) military thinking of the role of computers, and more generally, automated info processing in defense.

Initial military uses of computers were cryptography and mathematics

- Electromechanical "Bombe" deciphered Enigma messages.
- ENIAC and later computers were used for computing tables and trajectories.

Most security efforts at that time are focused on physical security and information security on paper and in transmission. Why do you think that's the case?

TEMPEST programs were begun to deal with emissions security, i.e., leaking information via electromagnetic emanations.

1960–1985: Multi-User Systems

Early systems were single-task, single-user machines. The 1960's saw the development of time-sharing and resource-sharing systems, and multi-processing.

What additional security challenges did this introduce?

1960–1985: Multi-User Systems

Military contexts have a specific protection model for document access control.

- Information containers (files) have associated classification levels (CONFIDENTIAL, SECRET, etc.)
- May have additional restrictions (NOFORN, EYES ONLY, etc.).
- Users assigned clearance according to their trustworthiness, job responsibilities.
- Information access may be further compartmented into "need-to-know" categories (CRYPTO, NUCLEAR, etc). Why?

Does this model translate well into the electronic world? Why or why not?

1960–1985: Multi-User Systems

Four models of operation were defined for computers handling classified information:

- **dedicated:** all users cleared for all information on machine; no need for access control (MILS);
- **system-high:** all users cleared, but must obey need-to-know compartments (discretionary access control).
- **compartmented:** all users cleared, but must be need-to-know compartments (mandatory access control). System must handle requests across classifications.
- **multi-level:** not all users cleared for all information; system enforces access control (MLS).

Multi-level is the most difficult so was not widely deployed. RAND Report R-609-1, "Security Controls for Computer Systems," (1970) summarizes best practice.

1985–1990: TCSEC

In 1985, the *Trusted Computer Systems Evaluation Criteria* (Orange Book) established a set of criteria by which the government could evaluate secure computer systems.

- Evaluation criteria for DoD purchase of COTS computer products.
- Criteria had four divisions: D (minimal protection) to A (verified protection), with several classes in most divisions (C1, C2, B1, B2).
- Most commercially viable systems did not seek certification. Why do you think that was?
- Only special purpose network products sought the highest certification levels (A1).

TCSEC was specifically for operating systems. No provisions for evaluating other security-related products.

TCSEC (2)

TCSEC was superceded by Common Criteria, which we'll discuss later in the semester.

"Rainbow series" of books attempted to apply TCSEC across a wider class of products. (see "Rainbow series" on Wikipedia)

Windows NT Workstation and many Unix-based operating systems achieved C2 rating (very weak, and often used configurations only generally of interest to the military).

Only Trusted XENIX and Multics operating systems obtained B2 rating. No general purpose operating system obtained A1 rating, only special purpose network products (Boeing MLS/LAN, Gemini Trusted Network Processor).

1960–1990: Military Networking

Early wide-area networks were based on person-to-person telegram messages, such as AUTODIN, begun in 1962.

ARPANET, for real-time data exchange, establishes first connection in 1969 between two researchers.

Computers on the early ARPANET network at many universities were accessible via dial-up, and these were not particularly secure. (ARPANET's password system was once compromised by two high school students.)

But some threats, such as viruses, were not yet known.

1980–present: Networking

Defense networks began to switch to TCP/IP in 1983. ARPANET was terminated in 1990 and replaced for military purposes by:

- **NSFNET:** (1985–1995) for research, which became the backbone of the Internet.
- **SIPRNET:** network for SECRET communication, has no connection to Internet. (Secret Internet Protocol Router NETwork)
- **NIPRNET:** DoD network for unclassified, but sensitive communication, from which user can access Internet. (Non-classified IPR network)

Highly secure military applications may not be connected to any external network. Example: U.S. Navy submarines connect to SIPRNET only when surfaced and in a non-CSI mission phase.

Nature of the Threat

Cyber war is not occurring right now but nation-states are definitely in competition. Cyber weapons exist, and we should expect that adversaries might use them.
–McAfee Virtual Criminology Report 2009, p. 13

America's failure to protect cyberspace is one of the most urgent national security problems facing the new administration that will take office in January 2009. ... It is a battle we are losing. Losing this struggle will wreak serious damage on the economic health and national security of the United States. –CSIS report on Securing Cyberspace for the 44th Presidency, Dec. 2008

Information Warfare

In recent years, conventional combat has been augmented (or replaced) by information warfare—attacking the cyber-infrastructure of the adversary.

> *In the very near future many conflicts will not take place on the open field of battle, but rather in spaces on the Internet, fought with the aid of information soldiers, that is hackers. This means that a small force of hackers is stronger than the multi-thousand force of the current armed forces. –Nikolai Kuryanovich, Russian Deputy of the State Duma, March 2006*

Thus, a large sponsor/consumer of IA activity is the military establishment.

Cyber Warfare

The 2009 Virtual Criminology Report from McAfee says that cyber strikes could have a devastating impact on national infrastructure with power grids, water supplies and financial markets all at risk.

In their 2007 report, McAfee reported that approximately 120 countries have been developing ways to use the Internet as a weapon and target financial markets, government computer systems and utilities.

> *Beijing is increasingly devoting itself to cyberwarfare. This is a cheap way to counter American dominance in traditional military fields. If the U.S. and China ever jostle with force, Beijing may hit us not with missiles but with cyberinfiltrations that shut down the electric grid, disrupt communications and tinker with the floodgates of dams. –Nicholas Kristof, The New York Times, January 18, 2010*

Information Operations

Information Operations actions implement Information Warfare.

1998 *Joint Doctrine for Information Operations* defines IO as: "actions taken to affect adversary information and information systems while defending one's own information and information systems."

Offensive Information Operations

- Target adversary decision makers and control systems
- "May have the greatest impact in peace and the initial stages of a crisis"
- Operations include "hacker brigades" that attempt to infiltrate and compromise adversary's network-accessible systems

Information Operations (2)

Defensive Information Operations:

- Integrates and coordinates policies and procedures, operations, personnel, and technology
- Types of operations include:
  - typical information assurance measures
  - operations security (OPSEC)—a process for protecting information that denies an adversary the ability to compromise it
  - physical security–protection of or with physical assets (e.g. perimeters, mechanical defenses)
  - counterdeception—negating an attacker's deception attempt
  - counterpropoganda—exposing attacker's propoganda

Information Operations Roadmap

In October, 2003, then-Secretary of Defense Donald Rumsfeld issued the *Information Operations Roadmap*, which was initially secret but subsequently released.

Google "Information Operations Roadmap 2003" to see a copy. You'll note that it's marked **SECRET/NOFORN**.

The release embarrassed the U.S. government because the document suggested that the U.S. was involved in significant PSYOPS activity, but didn't distinguish external adversaries from the American public.

The Smith-Mundt Act (1948, amended 1972 and 1998) expressly prohibits the government from propogandizing the American public with information and psychological operations directed at foreign audiences.

Information in War

Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

Information in War

Information Warfare (IW) is a key scenario for military IA. What does an attack look like? How do I prepare? How do I respond?

Military strategist John Boyd came up with a characterization of stategic response to threat called the *OODA Loop.*

- Observe: sensors transmit information about the attack to the commander.
- Orient: the information is interpreted by the commander.
- Decide: the commander forms a plan of operation.
- Act: the plan is carried out.

What do you think are the primary goals of the OODA loop?

OODA Loop

From the Wikipedia page on OODA Loop.

OODA Loop

The OODA Loop was originally applied to the combat operations process, but has been adapted for commercial operations and learning processes.

Ideally, an individual or an organization that can process the cycle quickly, observing and responding to unfolding events can gain a strategic advantage by "getting inside" the opponent's decision cycle.

Aside: Boyd's thinking was instrumental in moving the US Air Force from heavy, powerful jet fighters such as the F-4 Phantom to lighter and more responsive jets such as the F-16 Falcon. What is the relationship between OODA and jet fighters?

The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B's response?

The OODA Loop

The OODA Loop provides a framework for formulating/evaluating a response, but must take into account whether one can/will respond.

If A launches an attack on B, what factors are likely to influence B's response?

- *B's perception of the situation:* based on data and resources available and many other factors.
- *B's capacity to act:* resources available to B to make a response.
- *B's will to act:* human factor hardest for A to quantify or affect.

This suggests that an offensive strategy should take these factors into account and attempt to influence them, if possible.

Influencing the OODA Loop

What types of attack are possible?

Influencing the OODA Loop

What types of attack are possible?

- *Physical attack:* destruction intended to reduce B's capacity to respond. (Example: D-Day 1944—massive shelling followed by invasion at Normandy beaches)
- *Deception:* reduces B's effectiveness in responding through distortion, concealment and false indications. (D-Day: fake invasion plans and exercises targeting Pas-de-Calais instead of Normandy)
- *Psychological attack:* cause B to become disoriented. (D-Day: dummy paratroopers dropped behind enemy lines)
- *Information attack:* explicitly target B's sensors and information infrastructure. (D-Day: French resistance and special ops teams cut telephone lines)

Remote access need not include physical force or even physical presence. Can warfare exist primarily at the information level?

Some Information Attacks

First Persian Gulf War (1991): Iraq's command and control infrastructure is targeted. Radar and missile control network is fragmented and sections of radar coverage are taken offline without central control being aware of the outage.

Estonia (2007): Cyberattacks disabled the websites of government ministries, political parties, newspapers, banks, and companies. Russia was suspected of launching the attack in retaliation for the removal of the Bronze Soldier Soviet war memorial in central Tallinn.

Georgia (2008): Russian attacked the nation of Georgia in a dispute over the province of South Ossetia. In addition to the military attack, a concerted cyber DoS attack shut down much of Georgia's ability to communicate with the external world.

Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?

Some Information Attacks (2)

Is the U.S. at risk from cyber attack? Do you think that the U.S. has already been attacked?

Titan Rain: series of coordinated attacks on American computer systems since 2003. The attacks were labeled as Chinese in origin, although their precise nature (i.e., state-sponsored espionage, corporate espionage, or random hacker attacks) and their real identities are unknown.

Moonlight Maze: series of alleged coordinated attacks on American computer systems in 1999. The attacks were traced to a computer in Moscow but it is not known if that is where they originated. It was claimed, though not certain, that these hackers had obtained large stores of data that might include classified naval codes and information on missile guidance systems.

Credible U.S. security experts suggest that a successful widespread attack on U.S. computing infrastructure could largely shut down the U.S. economy for up to 6 months.

Objectives of Information Warfare

Information dominance: (typically at national level) obtain strategic and battlefield superiority, denying the enemy information or the systems on which to process it.

Information protection: (defensive) protect information systems from attack, and recover when attacks occur.

Information attack: (offensive)

- *Disruption (denial of service):* cause loss of or delay in accessing services
  - Attacks include jamming, physical destruction
  - Targets the *availability* of the information
- *Corruption:* change information or services; targets the *integrity* of the information
- *Exploitation:* gain access to protected information; targets the *confidentiality* of the information.

Examples of Information Attacks

- **International context:** information wars between nations (or proxies)
- **Corporate context:** industrial espionage and sabotage
- **Interpersonal context:** impersonation and identity theft
- **Asymmetric contexts:** terrorism and hacking

CyberWarfare Tactics

According to the Wikipedia article on CyberWarfare, these are the "methods of attack in cyberwarfare," *ranked from mildest to most severe*.

1. *Cyber espionage:* the act or practice of obtaining secrets from individuals, competitors, rivals, groups, governments and enemies also for military, political, or economic advantage using illegal exploitation methods on internet, networks, software and or computers.
2. *Web vandalism:* attacks that deface web pages, or denial-of-service attacks. This is normally swiftly combated and of little harm.
3. *Propaganda:* political messages can be spread through or to anyone with access to the internet or any device that receives digital transmissions from the Internet to include cell phones, PDAs, etc.

CyberWarfare Tactics (2)

4. *Gathering data:* classified information that is not handled securely can be intercepted and even modified, making espionage possible from the other side of the world. (Titan Rain and Moonlight Maze)
5. *Distributed Denial-of-Service Attacks:* large numbers of computers controlled by one person launch a DoS attack against systems
6. *Equipment disruption:* Military activities that use computers and satellites for coordination are at risk from this type of attack. Orders and communications can be intercepted or replaced, putting soldiers at risk.

CyberWarfare Tactics (3)

7. *Attacking critical infrastructure:* Power, water, fuel, communications, commercial and transportation are all vulnerable to a cyber attack.
8. *Compromised/Counterfeit Hardware:* Common hardware used in computers and networks that have malicious software hidden inside the software, firmware or even the microprocessors.

CyberWarfare Tactics (4)

The Wikipedia article on CyberWarfare ranks these *from mildest to most severe*.

1. Cyber espionage
2. Web vandalism
3. Propoganda
4. Gathering data
5. Distributed denial-of-service attacks
6. Equipment disruption
7. Attacking critical infrastructure
8. Compromised/counterfeit hardware

Do you agree with this ordering? Could it possibly be that compromised/counterfeit hardware is more of a threat than attacking critical infrastructure?

CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. Is that really a problem? Does it even happen?

CyberWarfare Tactics (5)

According to the Wikipedia article, the most severe attack strategy in CyberWarfare is: Compromised/Counterfeit Hardware. Is that really a problem? Does it even happen?

December 2009: "A federal grand jury has indicted four people accused of selling counterfeit Cisco Systems Inc. computer hardware through their Colorado-based company."

How is this relevant to CyberWarfare?

2008 DefenseTech Article

From: `defensetech.org/2008/04/01`:

> *Recent events have raised the concerns about hidden backdoors and malicious code inside of counterfeit hardware all the way down to the integrated circuit level. In fact, a 2005 report by the Pentagon's Defense Science Board addresses this issue. While this report assessed the problem, recent events have now raised the anxiety over cyber sabotage in bogus hardware. In fact, many consider the use of compromised counterfeit hardware as a strategic tactic in cyber warfare. In January of 2008, a joint task force seized $78 million of counterfeit Cisco networking hardware. This international effort resulted in over 400 seizures of counterfeit networking hardware that was shipped between China, Canada and the United States.*

The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

The Acquisition Problem

In addition to direct attacks on the national cyberstructure, the U.S. military is a consumer of vast amounts of commercial hardware/software. This is called *acquisition*, *procurement* or *supply chain*. Where do these products come from? How do we know they're reliable? Can we even tell? Is this just a problem for the military?

The trend in government acquisition is toward commercial-off-the-shelf (COTS) products and services.

- (1991) Sec. of Defense Perry announces DoD Strategic Acquisition Initiative mandating a preference for COTS products.
- (1997) Sec. of Defense Cohen launches Defense Acquisition Reform Initiative that accelerated the preference for COTS in defense acquisition.

What do you think motivated this preference for COTS over GOTS or contract developments?

Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices.

Do you think this is an an effective strategy?

Advantages of COTS Products

Preference for COTS products aims to obtain the latest technology at reduced cost, with shorter development and refresh cycles, and to leverage commercial investment and commercial best practices. Do you think this is an an effective strategy?

Experience has shown that COTS products are often more:

- flexible
- scalable
- configurable
- maintainable

than products produced solely for the government

These benefits are exemplified by a reported *ten-fold reduction in price for U.S. Navy submarine sonar and combat systems over a ten year period*, with significantly enhanced capabilities. (Stevens)

So What's the Downside

How could compromised hardware/software cause problems?

So What's the Downside

How could compromised hardware/software cause problems?

An adversary intent on damaging U.S. national interests might insert unauthorized or damaging functionality which could be:

active: code that

- alters the behavior of critical systems,
- exfiltrates sensitive information,
- modifies programs or data,
- crashes a machine or network

passive: e.g., a backdoor to allow a future intruder to bypass the security protections of the system.

Role of Acquisitions Policy

One of the CSIS recommendations "to make a noticeable improvement in the nations cybersecurity" is:

> *Use acquisitions policy to improve security. The federal government is the largest single consumer of information technology products. We recommend that the United States buy only secure products and services; standards and guidelines for secure products should be developed in partnership with industry. (CSIS report, p. 2)*

Well, isn't that the solution to the acquisition problem? Just buy only secure products. So, what's the problem?

Product Evaluation

Trust, but verify. – Ronald Reagan

Question: Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

Product Evaluation

Trust, but verify. – Ronald Reagan

Question: Isn't that what vulnerability scanners are for? Can't we just implement methods to ensure that acquired systems do not contain exploitable vulnerabilities?

Answer: Not completely. The problem of detecting arbitrary malicious functionality is *undecidable*—there is no algorithm that can reliably distinguish between malicious and benign code.

Malicious Software

Ken Thompson (1984 Turing Award lecture) noted that even complete control over source code is not sufficient to ensure the absence of malicious functionality, which can be introduced by the compiler, linker, loader, assembler, microcode, and even hardware.

> *You can't trust code that you did not completely create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. [...] As the level of program gets lower, these bugs will be harder and harder to detect. A well-installed microcode bug will be almost impossible to detect.* –*Ken Thompson*

But We Can Try

Example: The U.S. Army requires that all systems receive a "certificate of networthiness" (CoN) before being deployed on Army networks.

According to the Army's *Networthiness Certification Program for Information Systems*, networthiness encompasses:

> *network security, network impact, compatibility with the total infrastructure, infrastructure requirements, spectrum support, security policy compliance, Foreign Ownership and Influence (FOCI), Joint Technical Architecture-Army (JTA-A) standards compliance, communications and information manpower, training, logistics support, schedule, and funding.*

The Army currently has a backlog of several thousand applications awaiting CoN evaluation by the 3 or so guys working for the Certification Program.

Some Sobering Facts

- A recent study of 32,000 Websites found that *nearly 97% of sites carry a severe vulnerability*. –Web Application Security Consortium, Sept 2008
- "NSA found that inappropriate or incorrect software security configurations (most often caused by configuration errors at the local base level) were responsible for 80 percent of Air Force vulnerabilities." –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008, p. 55.
- "Some U.S. government computer systems have shown significant security lapses." –Bagchi, et al., Summer 2005

But the fact that these statistics are available at all implies that significant classes of vulnerabilities can be detected.

There is Some Hope

The fact that a problem is undecidable *doesn't mean that there aren't useful steps that can be taken.*

Most vulnerabilities in software systems were introduced inadvertantly rather than maliciously. In many cases, it is impossible to distinguish the two.

> *Sufficiently advanced incompetence is indistinguishable from malice. –Prof. Hovav Shachem*

Historically, most vulnerabilities have not been recognized as such until someone discovered a way to exploit them.

> *A good attack is one that the engineers never thought of. –security guru Bruce Schneier*

There is Some Hope

The most common approach is *vulnerability scanning*, which seems to be the main approach of the Army currently. Several automated scanners are used by the CoN certifiers:

- **Nessus**: proprietary network scan tool, easily configured with plugins, available for Windows and Unix platforms.
- **Retina**: commercial network monitoring tool (Windows, Unix, others).
- **DISA Gold**: detect, report and remediate vulnerabilities in Windows.

There are many other tools out there. How could you decide what tools are the most appropriate? What factors enter into the decision?

The Problem

As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know. And if one looks throughout the history of our country and other free countries, it is the latter category that tend to be the difficult ones. –*Donald Rumsfeld, Secy of Defense*

Scanners are excellent tools for discovering *known vulnerabilities*, but a sophisticated adversary will craft the attack until it defeats the scanners. Explain.

Example: In tests of 36 commercial anti-virus products, fewer than half of the newest malicious software programs were identified. (research by Stuart Staniford of FireEye, Nov. 2008) What's the lesson here?

Vulnerability Scanners

Vulnerability scanning has the following weaknesses:

- Scanners only test for known vulnerabilities; may not be effective against zero-day attacks.
- Only applicable to testable vulnerabilities; some may trigger on specific environmental conditions.
- Report presence/absence of vulnerabilities not potential for damage; e.g., foothold scenarios.
- May be limited to vulnerabilities on individual machines; some require a network of machines to exploit.

Explain zero-day attacks and foothold scenarios. How would you go about countering zero-day attacks?

Dimensions of the Analysis

There are multiple dimensions in which to evaluate an analysis methodology.

Objects of analysis: What artifacts are available to the analyst—code (source, intermediate or object), an executable system, test vectors, etc.?

Depth of analysis: How thorough is the analysis carried out with any given tool?

Required skillset: What expertise is required to use a given tool effectively?

Precision and accuracy: Are specific methods likely to find all and/or only genuine vulnerabilities?

Depth of Analysis

Another key dimension is how deep is the analysis.

Black box methods: take a purely external perspective on the object of analysis without knowledge of the internal details.

Gray box methods: apply limited knowledge of the internal working of the object to guide the analysis.

White box methods: relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

Depth of Analysis

Another key dimension is how deep is the analysis.

Black box methods: take a purely external perspective on the object of analysis without knowledge of the internal details.

Gray box methods: apply limited knowledge of the internal working of the object to guide the analysis.

White box methods: relies on internal knowledge of the software to guide the analysis.

These categories are typically applied to generation of test cases, but can be applied to any analysis methods. Why would you ever use a more shallow analysis if a deeper analysis is possible?

Which to use depends crucially on the available time and resources, toolset, artifacts for analysis, etc.

Precision vs. Accuracy

We say that a vulnerability detection scheme is

Precise: if it never reports legitimate functionality as harmful, i.e., *no false positives*;

Accurate: if it detects all genuine vulnerabilities, i.e., *no false negatives*.

It is easy to build a scheme that is either accurate or precise; it's hard to do both simultaneously. Why?

Which is worse: false positives or false negatives? How would you go about estimating the rate of false positives/negatives in your system?

Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

Example: Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

Base-Rate Fallacy

When searching for events that are relatively rare in a population, even a moderately accurate detection scheme will return a high proportion of false positives.

Example: Suppose that only 1% of traffic is attacks and the detection accuracy is 90%. What percentage of raised alarms do you think will be false alarms?

Approximately 92% of raised alarms will be false alarms.

What conclusions can you draw from this analysis?

Useful systems often have parameters that can be tuned to adjust the levels of false positives and false negatives depending on the environment and threat profile.

CS361C: Information Assurance and Security

IA in Business

Dr. Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: February 13, 2015 at 14:24

Relating IA to Business Needs

IA developed in a military context, but has obvious benefits for commercial enterprises. Like what?

Relating IA to Business Needs

IA developed in a military context, but has obvious benefits for commercial enterprises. Like what?

- Enabling safe operation of business services
- Safeguarding assets
- Providing for recovery in case of disaster
- Assisting the organization in meeting regulatory requirements
- Obviating embarrassing disclosures of security lapses

Imagine that you are a consultant or IA officer in a business context. Some of you may well have that role in the future.

What are your goals/responsibilities? How does IA in business contexts differ from IA in military contexts?

Importance of IA

Financial losses attributable to malicious hacking, online corporate espionage and other computer crimes have a huge impact on commercial activity in this country.

The Computer Security Institute estimates total losses due to computer crime of more than $10 billion annually, mostly from financial fraud and proprietary information theft.

In one survey, 59% of companies reported attacks initiated from the Internet, and 38% reported attacks initiated from internal company computers.

IA in Business Information Systems

There is no security on this earth; there is only opportunity. –Gen. Douglas MacArthur

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible. "Perfect security" is impossible to achieve in practice. Why?

IA in Business Information Systems

There is no security on this earth; there is only opportunity. –Gen. Douglas MacArthur

The traditional emphasis of IA in corporations is in information security, particularly for networks and multi-user systems. However, there are often misconceptions about what is possible. "Perfect security" is impossible to achieve in practice. Why?

- Real world systems are remarkably complex.
- Security cannot be just a feature of a product; it is part of a process to manage risk.
- The existence of countermeasures that could provide perfect security would imply that there is no risk—i.e., it has all been mitigated. However, it is likely that some threats and vulverabilities have not yet been identified.

Business IA Expectations

> *"One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if."* –*Ron Barrett, Making High Availability Pay for Itself (2009)*

Business planning always involves a tradeoff between cost and benefits. Why?

Business IA Expectations

> *"One of the most difficult achievements in technology is getting the resolve to spend on the possibilities of what if."* –*Ron Barrett, Making High Availability Pay for Itself (2009)*

Business planning always involves a tradeoff between cost and benefits. Why?

Business is inherently profit-driven. Deployment of security infrastructure in a business requires not only that costs must be justified, but that it meets the needs of the organization and users.

Costs come in various forms. If the security burden is so high for the users that it interferes with productivity, security functions will be bypassed reducing effectiveness of the system. Give some examples.

Business IA Expectations

Examples: A cumbersome login process may have users logged in for weeks at a time. An IDS that gives repeated false alarms will be disconnected.

> *"The number one reason for abandoning (on-line) transactions, as stated by survey respondents, was that the process was taking too long (48%). The research revealed people will opt for speed over the risks of maintaining their security online."* *(Online Security: A Human Perspective, Oracle Systems, 2010)*

Why Do Businesses Care?

If security is a cost, what motivates businesses to implement it?

Why Do Businesses Care?

If security is a cost, what motivates businesses to implement it?

- Potential for loss
- Business reputation
- Competitive advantage
- Legislative and regulatory mandates
- others (?)

Why Do Businesses Care?

"Now that the Privacy Rights Clearing House maintains a comprehensive list of all known data breaches since 2005, major breaches live on in infamy long after the incident." *(Real World Data Loss Prevention Benefits, Sophos report, 2010)*

"A recent survey reported that computer security is the critical attribute of corporate networks for 78 percent of executives. Another survey reported that security outweighed other concerns by a factor of three as the driving concern for IT improvements." *(Landoll, The Security Risk Assessment Handbook, 2006)*

Legislation Driving IA

- *Computer Security Act* (1987): minimum security standards for Federal Agencies
- *Family Educational Rights and Privacy Act* (1974): protects student records in education
- *Health Insurance Portability and Accountability Act* (1996): regulates privacy and security in health care
- *Children's Online Privacy Protection Act* (COPPA) (1998): regulates privacy of children's online information
- *Gramm-Leach-Bliley Act* (1999): regulates security and privacy of financial records
- *Government Information Reform Act* (2000): redefines minimal security standards for government systems
- *Sarbanes-Oxley Act* (2002): regulates financial disclosure and audit for publicly held companies
- *North American Electric Reliability Council Cyber Security Standards* (2004): regulates security within electric systems industry

Regulations and Best Practice

Regulations often define "best practice" within a *particular industry.* Different industries have different standards. Why should that be?

> *"The term best practices is commonly used to connote a set of documented strategies, procedures, or methods employed by highly successful organization to effectively achieve results in a particular circumstance."* –*The Perfect Online Course by Orellano et al., p. ix.*

Regulations and Best Practice

"There is no single definition of the 'best practices' for an information security program. ... In fact, the term 'best practices' for information security is really a misnomer or even could be considered a myth." *(Landoll)*

Discuss this assertion.

Security safeguards are generally identified as:

technical: access control, identification and authentication, encryption, intrusion detection, etc.

non-technical: management and operational controls (e.g., security policies), operational procedures, and personnel, physical, and environmental security.

FERPA

The *Family Educational Rights and Privacy Act* of 1974, is a federal law that pertains to the release of and access to educational records.

FERPA applies to personally identifiable information in educational records.

- student's name
- names of family members
- addresses
- personal identifiers such as social security numbers
- personal characteristics or other information that make the student's identity easily traceable.

FERPA

Educational records are all records that contain information directly related to a student and are maintained by an educational agency or institution, or by a party acting on its behalf.

These do not include:

- sole possession records: only accessible to the maker and used as personal memory aid.
- medical or psychological treatment records that include those maintained by physicians, psychiatrists, and psychologists;
- employment records, provided that employment is not contingent upon being a student;
- law enforcement records;
- records collected about an individual after that person is no longer a student.

Student Rights under FERPA

Any student has a right to

- inspect and review his or her educational records;
- request to amend his or her educational records;
- have some control over the disclosure of information from his or her educational records.

Directory Information

UT designates some information as *Directory information* that may be disclosed without the student's permission, including

- Student's name
- Local, permanent, and email addresses
- UT eid public username
- Telephone listing
- Date and place of birth
- Major fields of study
- Dates of attendance
- Enrollment status
- Degrees, awards, and honors received, including selection criteria
- Most recently attended previous educational institution
- Classification
- Expected graduation date
- Certain other.

Who Can See Your Records

Nondirectory information may not be released without prior written consent from the student. Exceptions include:

- access by appropriate university administrators, faculty members, or staff members who require access to educational records in order to perform their legitimate educational duties;
- officials of other schools in which the student seeks or intends to enroll;
- in connection with a student's application for, or receipt of, financial aid.

Which of the following does FERPA describe: goals, consequences, policies, mechanisms? Keep that question in mind for each of the other legislative mandates.

Regulations Driving IA: HIPAA

Health Insurance Portability and Accountability Act (HIPAA) (1996) establishes safeguards that health care providers must use to protect personal information. The goal is to:

> *... improve the portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and healthcare delivery, to promote medical savings accounts, to improve access to long-term care services and coverage, and to simplify the administration of health insurance.*

Regulations Driving IA: HIPAA

HIPAA is concerned with several issues:

- Addresses the ability to transfer insurance when changing jobs, and maintaining insurance after leaving a job.
- Addresses protecting the privacy of medical records as they are transferred among physicians, hospitals, clinics, pharmacies, and insurance providers.

HIPAA involves two separate rules with fairly specific IA components:

1. Security Standards Final Rule;
2. Standards for the Privacy of Individually Identifiable Health Information Final Rule.

In this context, explain the difference between security and privacy.

HIPAA: Security Standards Rule

Healthcare entities must:

- Ensure the confidentiality, integrity and availability of all "electronic protected health information" they create, receive, maintain, or transmit;
- Protect against anticipated threats or hazards to the security or integrity of such information;
- Protect against anticipated uses or disclosures of info that are not permitted or required;
- Ensure compliance by its workforce with all provisions of the bill.

HIPAA does not mandate specific technical solutions. Is this a good idea or not? Why "anticipated" threats?

HIPAA Admin Security Safeguards

HIPAA either requires (R) or addresses (A) various specific administrative security safeguards:

- *Security Management:* including risk analysis, risk management, sanction, system activity review.
- *Assigned Security Responsibility.*
- *Workforce Security:* authorization and supervision, clearance, termination procedures.
- *Information Access Management:* isolating clearinghouse functions, access authorization, access establishment and modification.

HIPAA Admin Security Safeguards (continued)

- *Security Awareness and Training:* reminders, malicious software, log-in monitoring, password management.
- *Security Incident Procedures:* response and reporting.
- *Contingency Planning:* data backup, disaster recovery, emergency mode plan, testing and revision, application and data criticality analysis.
- *Evaluation.*
- *Business Associate Contracts and Other Arrangements.*

HIPAA Physical Security Safeguards

HIPAA defines certain **physical security** safeguard categories:

- *Facility Access Controls:* contingency operations, facility security plan, access control and validation, maintenance records.
- *Workstation Use.*
- *Workstation Security.*
- *Device and Media Controls:* disposal, media reuse, accountability, data backup and storage.

HIPAA Technical Security Safeguards

HIPAA also defines certain **technical security** safeguard categories:

- *Access Control:* unique user ID, emergency access procedures, automatic logoff, encryption and decryption.
- *Audit Controls.*
- *Integrity:* mechanism to authenticate electronic protected health info.
- *Person or Entity Authentication.*
- *Transmission Security:* integrity controls, encryption.

HIPAA Privacy Requirements

The Privacy Rule is less specific than the Security Rule. It demands protection of "individually identifiable health information" defined as:

> *Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) relates to the past, present, or future physical or mental health, or condition of an individual; the provision of health care to an individual, or the past, present, or future payment for provision of health care to an individual, and (a) that identifies the individual, or (b) with respect to which there is reasonable basis to believe that the individual can be used to identify the individual.*

HIPAA Privacy Requirements

To disclose information, authorization is required including:

- description of the information
- identification of those authorized to disclose or use
- statement of purpose of the use or disclosure
- expiration date for the authorization
- signature of the individual, parent or guardian
- statement of and procedures for revoking the authorization
- consequences of not signing an authorization
- potential re-disclosure of the info by recipient

Items from a "limited data set" may be disclosed, but must not contain any specific identifying info such as names, SSNs, URLs, etc. What do you think this "limited data set" provision is about?

Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

The two together form the HIPAA-POTOMIS suite of regulations.

Other Health Related Mandates

The *Patient's Omnibus Transaction on Mandatory Information Security* is a follow-on to HIPAA and provides additional protection relating to financial reporting and disclosure.

The two together form the HIPAA-POTOMIS suite of regulations.

If you haven't figured it out by now, this slide is a joke and can safely be ignored.

HITECH Act

The Health Information Technology for Economic and Clinical Health Act (HITECH) is Title XIII of the 2009 American Recovery and Reinvestment Act (ARRA). It expands the reach of HIPAA.

Reserves $22 billion to "advance the use of health information technology" to move toward Obama's promised e-health records.

- Expands HIPAA data privacy and security requirements to include "business associates" of entities subject to HIPAA.
- Strengthens HIPAA enforcement measure to include civil and criminal penalties.
- Monetary penalties become mandatory for "willful neglect."

Penalties are funneled back to HHS Office of Civil Rights enforcement, leading some to fear that this may encourage more punitive enforcement.

Regulations Driving IA: Sarbanes-Oxley

Sarbanes-Oxley Act (SOX) (2002) affects all US publicly traded companies.

The rules were designed to: ...protect investors by improving the accuracy and reliability of corporate disclosures made persuant to the securities laws ... to protect the interests of investors and further the public interest in the preparation of informative, accurate, and independent audit reports for companies the securities of which are sold to, and held by and for, public investors.

Sarbanes-Oxley

- Congress dramatically increased fines and penalities for fraudulent corporate financial reporting.
- Section 404 requires disclosure of the management's internal controls over financial reporting.
- Provisions apply to all corporations required to file annual reports by U.S. Securities and Exchange Commission.
- CIOs are responsible for the security of the Enterprise Resource Planning (ERP) systems which generate financial reports.
- Does not mandate particular internal control methodology.

In a survey of 217 companies with annual revenues of $5 billion, average one-time start-up cost was $4.26 million, or 0.0825 percent of annual revenue.

Sarbanes-Oxley and IT

The IT community cares for the following two reasons:

1. Requires certifying the accuracy and attesting to the reliability of financial reports.
2. Mandates adequate internal controls to ensure the accuracy and reliability of IT systems and operational procedures used to generate financial reports.

A large percentage of these internal controls is expected to relate to the design, development, operation and interaction with information systems. I.e., ensuring data, information, systems, and network integrity.

What does this mean for IT management at a publicly traded company?

Regulations Driving IA: GLBA

Financial Services Modernization Act (1999) (also known as Gramm-Leach-Bliley Act or GLBA) eliminates many of the barriers between banks, brokerage firms, and insurance companies.

Title V of GLBA declares that:

> *"each financial institution has ... a continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."*

Nonpublic personal information is defined as:

> *"personally identifiable financial information: (i) provided by a consumer to a financial institution; (ii) resulting from any transaction with the consumer or any service performed for the consumer; or (iii) otherwise obtained by the financial institution."*

Regulations Driving IA: GLBA

It also requires banks:

- "to insure the security and confidentiality of customer records and information;
- to protect against any anticipated threats or hazards to the security or integrity of such records;
- to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."

Financial institutions must provide customers with information relating to their privacy policies and procedures (and changes to it). Customers can *opt out* of any disclosures they don't like.

Why "anticipated threats"? Discuss the pros and cons of opt out vs. opt in policies.

Regulations Driving IA: GLBA

Despite GLBA, a 2003 study found that:

1. 66 percent of financial institutions surveyed had one or more Web forms that collected personally identifiable information but did not use SSL encryption;
2. 91 percent of these institutions used weak SSL encryption, such as 40-bit RC4, rather than the 128-bit encryption then recommended by federal bank regulators.

Upshot: A regulation is only as good as its enforcement.

Do you think the figures would be a lot better today?

Regulations Driving IA: FISMA

From Wikipedia:

> *The Federal Information Security Management Act of 2002 is a federal law enacted in 2002. ... The act recognized the importance of information security to the economic and national security interests of the United States. The act requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems. ... FISMA has brought attention within the federal government to cybersecurity and explicitly emphasized a "risk-based policy for cost-effective security."*

Threats to Business Information

What do you think are the major threats to business information?

Threats to Business Information

What do you think are the major threats to business information?

- *Human error or failure:* mistakes of authorized users may compromise confidentiality, integrity, availability.
- *Intellectual property compromise:* software piracy, unauthorized duplication violating software licensing. Business Software Alliance (`www.bsa.org`) active to reduce this.
- *Espionage/trespass:*
  - Industrial espionage: companies gathering competitive information on other companies. May also involve national intelligence services.
  - Shoulder surfing or dumpster diving: opportunistic acquisition of carelessly guarded or discarded information.
  - Hackers: have techniques and tools to locate and target vulnerabilities in order to trespass.

Threats to Business Information

- *Extortion:*
  - After assets (e.g. credit card numbers) are stolen, blackmailing the target to pay
  - If the target refuses to pay, the assets might be sold to other criminals.
- *Sabotage:*
  - The most common form is web page defacement. 95% of large organizations reported in 2005 "more than 10 incidents" involving the website, though not all were successful attacks.
  - More damaging is damage to infrastructure control systems, for defense, utilities, telecommunications, etc. (In 1996 a juvenile hacker compromised the phone system used by Worchester, MA air traffic control, fire department and '911' system.)

Other Threats to Information

- *Theft:* loss of electronic assets more difficult to detect than loss of physical assets.
- *Software attacks (malware):* viruses, worms, trojan horses, DoS attacks, etc.
- *Forces of Nature:*
  - Major disasters: (fire, flood, earthquake, lightning, landslide, tornado, hurricane, tsunami); effects can often be mitigated via insurance and physical design
  - Small-scale attacks: (rodents, electrostatic damage, dust, conductive contamination).

Other Threats to Information

- *Other Factors:*
  - Quality of service issues:
    - Service providers (power, network connectivity) may experience failure or degradation in quality.
    - Backup services, where available, may not provide same quality of service as normal providers.
  - *Hardware and software failures*
  - *Technology obsolescence:* many organizations still depend on Windows NT or Window 2000, even though these are not actively maintained.

Business Impact of Computer Insecurity

According to a 2005 CSI/FBI Computer Crime and Security Survey:

- 56% of organizations had known, unauthorized use of computer systems.
- Approximately the same number of incidents resulted from insider threats as from outsiders.
- Top three causes of loss: viruses, unauthorized access, theft of proprietary information
- 97% of organizations use firewalls, 96% use antivirus software, approximately the same percentage as in 2004.
- Actual losses are typically not known, as only 20% of organizations report intrusions.
  - 43% claim reporting to law enforcement would hurt their stock/image
  - 33% claim competitors would use this to their advantage

Approaches to Business IA

There are several points in an org chart where IA decisions can originate. Organizations typically drive IA decisions in one of two patterns:

Bottom-up: IA decisions originate from those closest to the information assets such as system administrators and technologists.

Top-down: senior management determines the policies, goals and outcomes for IA projects.

If you were tasked to develop a comprehensive IA program for your company or agency, which approach would you choose (or perhaps some hybrid of the two)?

Bottom-up Approach to IA

In a *bottom-up* approach, those closest to information assets (system administrators) originate IA decisions.

- In the 1990s as companies attached to the Internet, system administrators often were responsible for identifying the need for security technology, selecting appropriate products, and deploying the products.
- Administrators have in-depth knowledge of the systems being managed, and are most aware of associated vulnerabilities and threats.
- Such IA projects are often funded as one-time special projects or as part of an overall infrastructure cost to the business of having IT services.

Bottom-up Approach

The bottom-up approach appears most frequently in:

- R&D organizations operating their own unique IT infrastructure
- groups creating or tracking emerging technologies
- small or decentralized organizations.

Evaluating the Bottom-up Approach

Is the bottom-up approach a viable long-term solution for business-critical information systems?

Evaluating the Bottom-up Approach

Is the bottom-up approach a viable long-term solution for business-critical information systems?

No!

- Solutions may not have buy-in from all involved parties, such as systems' end users.
- Approach likely does not have senior management awareness or participation. Costs and benefits not known to management, so cannot budget for IA.
- In large organizations, different IT teams may select incompatible technologies for solving similar problems.
- Turnover of IT staff may create an unrecognized knowledge gap.

Top-down Approach to IA

In a *top-down* approach, the IA program is initiated by senior business management, which determines policy, goals and outcomes for IA projects.

Program's processes may flow through organization in several ways:

1. Each level of management writes increasingly more specific statements on the IA process, and delegates implementation to the level below.
2. An IA project team may be set up, responsible for implementation and coordinating with each line-of-business.
3. A federated approach, such as in multinationals, in which each part of the company chooses an approach to implementation, but may be required to coordinate on selected areas across the organization.

Success Factors in Top-Down Approach

Top-down projects are often more likely to receive consistent funding, be integrated into organizational culture, and involve all necessary parties for a successful outcome.

The IA program should have a *champion* within senior management.

- Could be Chief Information Officer (CIO), Chief Information Security Officer (CISO), or VP of information technology or network operations.
- Establishes business goals of the program and ensures integration of requirements into budget and planning.
- The champion may also establish an integration roadmap or timeline to ensure that projects move ahead.

IA projects in a top-down approach typically follow a system development lifecycle model. The IA project is thus tracked similarly to other IT projects within the organization.

Senior Management Involvement

How should you organize IA management within your company? How does UT do it?

Chief Information Officer: establishes IA strategy and communicates with other managers.

Chief Information Security Officer: responsible for information security across the organization.

Chief Technology Officer: often responsible for special projects, not part of normal IT operations.

VP for Information Technology: responsible for IT services.

VP of Network Operations: responsible for operating data networks and related servers.

Other VPs and managers: may have their own IT infrastructure for line-of-business services.

Auditors: certify that the organization has correctly reported, and may validate the IA services that protect the data for such reports.

IA Project Teams

Possible roles with an IA deployment project:

- **Champion:** promotes the project and ensures its visibility to appropriate management.
- **Team leader:** manager who tracks the project status and ensures it meets goals.
- **Policy specialists:** identify security policies appropriate for the organization.
- **Risk assessment specialists:** coordinate risk assessment process used in IA and financial/business risk management.
- **Security professionals:** specialists in information security (technical and non-technical).
- **System administrators:** responsible for administering the systems and networks being protected.
- **End users:** selected users validate that the approach does not disrupt business activities.
- **Lead developers:** IA projects may need custom software engineering to integrate with existing systems.

Data Ownership and Flow

Three roles of data ownership:

- *Data owners* are responsible for the security and use of a particular category of data, and are typically senior managers.
- *Data custodians* are responsible for implementing the security and storage of data, often CISO or system administrators' responsibilities. Backup and recovery is of primary interest to the data custodian.
- *Data users* are the end users who interact with the data in order to fulfill a business function, and are typically integral in maintaining the security of data.

Explain the relationships among these various roles.

Data Ownership and Flow (2)

Multiple groups fill each role, as data flow throughout the organization.

- The process of creating new data, such as new accounts for customers in a database, is called *provisioning*.
- The authoritative database known to have correct (or best) information and supplies updates is called the *System of Record* database.

Communities of Interest

A *community of interest* is a group (may be distributed) with similar interests and a common goal within an organization.

Information Security: protects the organization's information systems and information from attack.

Information Technology:

- Manage IT costs, ease-of-use, timeliness, performance.
- May conflict with information security community as goals are not always aligned.

Organizational:

- General management, and the rest of the organization.
- To IT, these are "end users"; to Information Security, these are "subjects."
- Goals of IT and information security must be aligned with organizational goals.

Describe effects of having multiple communities of interest.

Other Organizational Roles in IA

A *security office* may be responsible for developing organizational security policies, and implementing certain policies, such as physical site security.

A *telecommunications office* may be responsible for maintaining the security of voice, video and data communications.

The functions of the *INFOSEC Officer* varies, and may include:

- managing an information security team
- reviewing operations which might impact information security (e.g., adding a modem dial-in line).
- performing risk assessments
- compiling documents of best practices for information security

Other Organizational Roles in IA

In government and contractor organizations:

- The *COMSEC Custodian* is responsible for safeguarding of communications security devices used in discussing classified information and training end users.
- The *OPSEC Manager* is responsible for identifying potential adversaries and their information targets, and developing security countermeasures.

A Security Systems Development Lifecycle

A security systems development lifecycle is a methodology:

- A methodology is a formal approach to problem solving based on a structured sequence of procedures.
- The lifecycle will have an end goal, as well as intermediate milestones, and a project team will be held accountable to meeting milestones and the end goal.

The process is started by an event or conditions, e.g. responding to a break-in or meeting shareholder/regulatory requirements.

A Security Systems Development Lifecycle

Often the lifecycle is based on the Waterfall model, and a feasibility analysis at the end of each phase:

1. Investigation
2. Analysis
3. Logical design
4. Physical design
5. Implementation
6. Maintenance and change

In some organizations, one or more of these phases may be outsourced. (According to a 2005 survey: 26% outsource up to 20% of security functions; 63% outsource none)

Phases of Security Systems Development Lifecycle

- *Investigation*
  - Specify objectives, constraints and scope of the project, and develop cost-benefit analysis.
  - Begin an *enterprise information security policy* document, as well as dictates from management of expected outcomes and budget.
  - Organize project teams, determine whether the organization has necessary resources and commitment for success.
- *Analysis*
  - Assess the organization, current systems and policies, and functions and interactions of the new system.
  - Analyze legal constraints, current threats and countermeasures.
  - Begin risk management process.

Phases of Security Systems Development Lifecycle

- *Logical design*
  - Create a system solution for the business need. Select applications, data, and ranges for technology alternatives. The logical design is implementation independent.
  - Establish IA policies, including
    - incident response: actions to take when an attack occurs
    - disaster recovery: immediate recovery of information and systems after a loss
    - continuity planning: how business will continue in the event of a loss.
- *Physical design*
  - Select specific technologies, perform build-vs-buy tradeoffs and establish success criteria
  - Develop *information security blueprint* document and physical security measures
  - Present entire solution to management for approval and signoff.

Phases of Security Systems Development Lifecycle

- *Implementation*
  - Create or acquire software and test components.
  - Train users and test whole system.
  - Provide sponsors with a performance review and acceptance test results.
- *Maintenance and Change*
  - Support and modify the system as needed for the rest of its life cycle.
  - Monitor and validate, upgrade countermeasures, repair and recover as needed.
  - Longest and possibly most expensive phase.

CS361C: Information Assurance and Security

Cryptography

Dr. Bill Young
Department of Computer Science
University of Texas at Austin

Last updated: March 10, 2015 at 15:05

Introduction to Cryptography

This is not a course in cryptography. The department offers one and you are advised to take it, if you plan to work in the security field.

Our point here will be to give some intuitions about:

- what are the key concepts of cryptography;
- how is it used as a tool for IA;
- how effective is it in that regard.

Introduction to Cryptography

Crypto is a key ingredient in any successful information assurance program. *But it's important to understand that cryptography is not the goal; it's a tool toward reaching one or more of several possible goals.*

> *If you think cryptography will solve your problem, then you don't understand cryptography ... and you don't understand your problem.* –*Bruce Schneier*

Why would Schneier say such a thing? Do you agree?

What is the Goal?

To what IA goals is cryptography likely to contribute?

What is the Goal?

To what IA goals is cryptography likely to contribute?

Confidentiality: the information in a message is accessible only to authorized parties

Authentication: the receiver of a message can ascertain its origin.

Integrity: modification to a message can be detected

Non-repudiation: a sender cannot falsely deny originating the message

Note that we've stated these goals in terms of data in transit; they also apply to data at rest. Explain this remark.

What is Good Encryption?

The value of an encryption algorithm depends on the use. An algorithm that is appropriate for computers might not be appropriate for use by an agent in the field.
Shannon (1949) listed characteristics of good ciphers.

1. The degree of secrecy required should determine the effort expending in encryption / decryption.
2. The keys and algorithm should be free from complexity.
3. The implementation should be as simple as possible.
4. Errors in encryption should not propagate.
5. The size of the ciphertext shouldn't be more than the size of the plaintext.

Which of these still apply to modern cryptography?

Other Criteria

Some of Shannon's criteria don't really apply to modern computer-based cryptography.

The following are suggested as other tests of worth for current cryptographic practice:

- is based on sound mathematics;
- has been analyzed by competent experts and found to be sound;
- has stood the test of time.

Symmetric and Asymmetric Systems

There are two basic types of encryption:

symmetric algorithms (also called "secret key") use a single key for both encryption and decryption;

asymmetric algorithms (also called "public key") use different keys for encryption and decryption.

For any encryption approach, there are two major challenges:

Key distribution: how do we convey keys to those who need them to establish secure communication.

Key management: given a large number of keys, how do we preserve their safety and make them available as needed.

Encryption / Decryption

The purpose of encryption is to render the message less useful / meaningful to the intruder. Conceptually, the process of encryption is quite simple:

as is the process of decryption:

Do these pictures apply equally well to symmetric and asymmetric algorithms?

Some Vocabulary

Be sure that you understand the following terms:

- encryption, decryption
- key, keyspace
- plaintext, ciphertext
- cryptography, cryptanalysis, cryptology

What is the relationship between the key size and the keyspace?
Does reference to keyspace always make sense?

Cryptanalysis

Attacks on an encryption algorithm can be classified according to what information is available to the attacker.

Ciphertext-only attack: available is only the ciphertext of several messages encrypted with the same key/algorithm

Known plaintext: available is a quantity of ciphertext and corresponding plaintext.

Chosen plaintext attack: cryptanalyst can control the plain text to be encrypted and see the resulting ciphertext.

Adaptive chosen plaintext attack: chosen plaintext attack where the choice of plaintext may depend on the ciphertext from earlier attempts.

Cryptanalysis

Chosen ciphertext attack: the attacker selects a ciphertext and is given the corresponding plaintext. E.g., attacker gains access to the decryption device but not the key.

Chosen key attack: cryptanalyst has knowledge of the relationship among different keys.

Rubber-hose cryptanalysis: breaking cipher through threats, blackmail, or torture.

Cryptanalysis

Recall *the Principle of Easiest Penetration*. Often it is more effective to attack the human users rather than the cryptographic algorithms. Many successful attacks succeed because the users are hurried, lazy, careless, naive or uninformed. Sometimes users can be bribed or coerced.

Why Cryptosystems Fail

Excellent paper: "Why Cryptosystems Fail" by Ross Anderson, available on-line.

> *It turns out that the threat model commonly used by cryptosystem designers was wrong: most frauds were not caused by cryptanalysis or other technical attacks, but by implementation errors and management failures. This suggests that a paradigm shift is overdue in computer security.* *(from the abstract)*

Symmetric Ciphers

Also called "secret key" ciphers, require that sender and receiver have access to a single key.

The main issue with symmetric encryption is *key distribution*. Presents a "chicken and egg" problem: if I have a secure channel to get the key to you, why don't I just use that channel to send the message? How would you answer that question?

Some symmetric encryption algorithms: AES, Blowfish, DES, 3DES, Serpent, Twofish, CAST-128, IDEA, Skipjack.

Diffie-Hellman

Recall that symmetric encryption requires that the parties agree on a secret key. How do you distribute the key if you don't have a secure channel? Is it even possible?

Diffie-Hellman

Recall that symmetric encryption requires that the parties agree on a secret key. How do you distribute the key if you don't have a secure channel? Is it even possible?

Diffie-Hellman (1976) is the first viable approach for key exchange over an insecure channel.

Steps in the algorithm:

1. Alice and Bob agree on a prime number p and a base g.
2. Alice chooses a secret number a, and sends Bob $(g^a \mod p)$.
3. Bob chooses a secret number b, and sends Alice $(g^b \mod p)$.
4. Alice computes $((g^b \mod p)^a \mod p)$.
5. Bob computes $((g^a \mod p)^b \mod p)$.

Both Alice and Bob can use this number as their key.

By itself, this protocol is vulnerable to a man-in-the-middle attack. What is a man-in-the-middle attack? Describe this attack?

Diffie-Hellman Man in the Middle

The Diffie-Hellman key exchange is vulnerable to a man-in-the-middle attack. In this attack, an opponent Carol intercepts Alice's public value and sends her own public value to Bob. When Bob transmits his public value, Carol substitutes it with her own and sends it to Alice. Carol and Alice thus agree on one shared key and Carol and Bob agree on another shared key. After this exchange, Carol simply decrypts any messages sent out by Alice or Bob, and then reads and possibly modifies them before re-encrypting with the appropriate key and transmitting them to the other party. This vulnerability is present because Diffie-Hellman key exchange does not authenticate the participants. Possible solutions include the use of digital signatures and other protocol variants.
–RSA labs

Stream and Block Ciphers

Another important distinction in symmetric algorithms is between stream and block ciphers.

Stream ciphers convert one bit/symbol of plaintext directly into a symbol of ciphertext.

Block ciphers encrypts a group of plaintext bits/symbols as one block.

Most modern symmetric encryption algorithms are block ciphers. The distinction is not as clear cut as you might think at first. Why is that?

Public Key Encryption

In a symmetric algorithm, the key must remain secret for the algorithm to be secure. In 1976, Diffie and Hellman proposed *public key encryption* (asymmetric encryption) in which a key does not have to be kept secret.

In 1997, it was publicly disclosed that asymmetric key algorithms were developed by James H. Ellis, Clifford Cocks, and Malcolm Williamson at GCHQ in the UK in the early 1970s. The researchers independently developed Diffie-Hellman key exchange and a special case of RSA. The GCHQ cryptographers referred to the technique as *non-secret encryption*.

Public Key Systems Explained

For an asymmetric (public key) encryption system each subject has two keys:

Encryption key: K_e

Decryption key: K_d

Encryption is done with the encryption key K_e; decryption *can only be performed* with the corresponding decryption key K_d.

These have the following property:

$$M = \{\{M\}_{K_e}\}_{K_d}$$

Public Key Systems: Confidentiality

In an asymmetric (or public-key) system *for confidentiality*, each subject S has two keys:

Public key: K_S is the encryption key and is widely disseminated.

Private key: K_S^{-1} is the decryption key known only to S.

Anyone who wants to communicate confidentially with S can do so by encrypting a message with S's public key:

$$\{M\}_{k_s}$$

No-one but S can decrypt the message, because doing so requires S's private key, which is known only to S.

Public Key Systems: Authenticity

In an asymmetric (or public-key) system *for authenticity*, each subject S has two keys:

Private key: K_S^{-1} is the encryption key known only to S.

Public key: K_S is the decryption key and is widely disseminated.

If S wants to *sign* a message (i.e., send it in such a way that anyone can verify it came from S), then S signs (encrypts) the message with S's private key:

$$\{M\}_{k_s^{-1}}$$

Anyone can check the signature (i.e., decrypt the message) using S's public key. By assumption, only S has S's private key, so only S could have signed the message.

Public Key Systems: Confidentiality and Authenticity

If the public key algorithm has the following property:

$$M = \{\{M\}_{k_S^{-1}}\}_{K_S} = \{\{M\}_{K_S}\}_{K_S^{-1}}$$

then either key can be used to encrypt and the other to decrypt.

In a system with this property, the same pair of public/private keys can be used for both confidentiality and authenticity. RSA is the only known public key algorithm with this property.

If the system does not have this property, then two pairs of keys are needed: one pair for confidentiality and one for authentication (signing).

Public Key Encryption

Having only one (or two) pair(s) of keys per subject, drastically reduces the number of keys that have to be protected when compared to a symmetric system. Explain this assertion.

Explain why public key systems largely solve the key distribution problem.

Alternative Notation

Particularly with public key systems, a different notation is common. The public key for subject A is denoted K_A and the corresponding private key is K_A^{-1}.

Encryption or decryption of a message M with key K is denoted as $\{M\}_K$. Thus, what we previously wrote as:

$$P = D(K_{pub}, E(K_{priv}, P))$$

would be denoted

$$P = \{\{P\}_{K_A^{-1}}\}_{K_A}$$

assuming that the keys were associated with subject A.

Using the Notation

This notation (for both symmetric and asymmetric crypto) is often used in protocols

For example, the Needham-Schroeder protocol is:

1. $A \rightarrow S : A, B, N_a$
2. $S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$
3. $A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$
4. $B \rightarrow A : \{N_b\}_{K_{ab}}$
5. $A \rightarrow B : \{N_b - 1\}_{K_{ab}}$

Using the Notation

And here are the message exchanges PGP uses for:

Authentication:

$$S \rightarrow R : \{h(M)\}_{K_S^{-1}}, M$$

and Confidentiality:

$$S \rightarrow R : \{K\}_{K_r}, \{M\}_K$$

Signing

In a *symmetric* encryption system, sending a message provides confidentiality and authentication (sort of). Explain.

What guarantees do you get sending a message in an *asymmetric* encryption system?

Signing

In a *symmetric* encryption system, sending a message provides confidentiality and authentication (sort of). Explain.

What guarantees do you get sending a message in an *asymmetric* encryption system?

- *Confidentiality:* if S sends to R the message $\{M\}_{K_R}$, then no one but R can recover M.
- *Authenticity:* if S sends to R the message $\{M\}_{K_S^{-1}}$, then no one but R knows the message must have come from S. Why?

Can you get both confidentiality and authentication in one message? Explain why or why not.

Signing and Non-RSA

Suppose you're using a public key system for which the following is *not* true:

$$P = D(K_{priv}, E(K_{pub}, P)) = D(K_{pub}, E(K_{priv}, P))$$

How could you use the system for both confidentiality and authenticity?

Signing and Non-RSA

Suppose you're using a public key system for which the following is *not* true:

$$P = D(K_{priv}, E(K_{pub}, P)) = D(K_{pub}, E(K_{priv}, P))$$

How could you use the system for both confidentiality and authenticity?

You'd need *two pairs* of keys: one pair for confidentiality and one for authenticity.

$$(K_{enc}, K_{dec}) \text{ and } (K_{sign}, K_{verify})$$

Think about how that would work? Which is private and which public in each pair? For the second pair, which encrypts and which decrypts?

Public Key Systems

The basis of any public key system is the identification of a function that is easily computed, but difficult to invert without additional information. This is called a *one-way* function.

For example, it is straightforward to multiply two large primes p_1 and p_2 together. However, given the result $p_1 p_2$, it can be very difficult to factor it to recover the p_1 and p_2.

However, given $p_1 p_2$ and either of p_1 or p_2, it is again straightforward to recover the other, simply by dividing.

Thus, multiplication is a one-way function, because computing the inverse is effectively infeasible for products of large primes.

RSA Algorithm

The **Rivest-Shamir-Adelman (RSA)** algorithm is a public key system which relies on the difficulty of factoring large numbers.

Two keys, d and e, are used for encryption and decryption. Because the use of the keys in RSA is symmetric, either can be the private key. The algorithm is such that:

$$\{\{P\}_d\}_e = P = \{\{P\}_e\}_d.$$

A plaintext block P is encrypted as $(P^e \bmod n)$. The decrypting key is chosen so that: $(P^e)^d \bmod n = P$.

Because the encrypting exponentiation is performed modulo n, an interceptor would have to factor P^e to recover the plaintext. This is difficult. However, the legitimate receiver knows d and merely computes $(P^e)^d \bmod n = P$. This is much easier.

Other Public Key Algorithms

A public key system can be based on any one-way function. A rich source of these is the set of NP-complete problems. These are infeasible to solve (requiring at least exponential time) but a proposed solution can be checked in polynomial time.

Merkle and Hellman proposed a public key system based on the *knapsack problem*: given a set of integers and a target sum, find a subset of the integers that sum to the target.

The algorithm is theoretically very secure, but has practical weaknesses. Just because a problem is difficult, in general, doesn't mean it is difficult in specific instances. Explain.

Efficiency of Encryption

If public key systems have real benefits, why not just scrap symmetric encryption?

Efficiency of Encryption

If public key systems have real benefits, why not just scrap symmetric encryption?

Public key systems simplify key distribution but are typically very slow. Thus, they are used only for specialized purposes.

A public key encryption *may take 10,000 times as long* to perform as a symmetric encryption, because it depends on multiplication and division, rather than simple bit operations.

For this reason, symmetric encryption is the work horse of commercial cryptography. Still, asymmetric encryption plays some important functions.

Hybrid Systems

Some commercially important systems use a combination of symmetric and asymmetric encryption, utilizing the best features of each.

Pretty Good Privacy (PGP): email encryption system.

Secure Socket Layer (SSL): add-on to the HTTP standard to allow secure network communication

For example, to send confidentially a message M in PGP, you do the following:

$$S \rightarrow R : \{K\}_{K_R}, \{M\}_K$$

where K is a new session key.

To send an authenticated message, use:

$$S \rightarrow R : \{h(M)\}_{K_S^{-1}}, M$$

Digital Signatures

What is a digital signature? What is it for? What characteristics would you want it to have?

Digital Signatures

What is a digital signature? What is it for? What characteristics would you want it to have?

Any signature scheme should have the following characteristics:

- **authentic:** convinces the recipient that the signer deliberately signed the document
- **unforgeable:** no other party could have produced the signature
- **not reusable:** signature is bound to the document and cannot be transferred to another document
- **unalterable:** after signing, the signature cannot be modified
- **cannot be repudiated:** the signer cannot later deny having signed the document.

The signature is typically a function $S(P, M)$ of the signer's identity P and the message M.

Signing

What mechanism do we already have that provides some of these capabilities?

Signing

What mechanism do we already have that provides some of these capabilities?

Public key cryptosystems provide a convenient framework for digital signing of documents because *the underlying assumption is that only A has access to A's private key.* Why is that assumption crucial?

If S wishes to send a signed, confidential message to R, then S can send:

$$\{\{M\}_{K_S^{-1}}\}_{K_R}$$

Upon receipt, R knows that the message came from S and that its confidentiality was protected. Explain how. Could we have done the two encryptions in the opposite order? Why or why not?

Key Bindings

For a public key system to work, there must be a way for a party to get the public keys of others in the system. How might that work?

Key Bindings

For a public key system to work, there must be a way for a party to get the public keys of others in the system. How might that work?

- You could get the key directly from each party.
- You could get the key from a trusted key server/central repository.
- You could obtain the key from a trusted third party willing to "vouch for" the association.

What are the pros and cons of each of these?

Given the public key K_R for some entity R, how do you know for sure that the key is actually R's public key?

This question is at the very heart of any public key infrastructure (PKI). Because if these *bindings* are not accurate, then trust breaks down in the system. Why?

Certificates

Certification addresses the need for *trust* in computer systems. How do two entities that are mutually suspicious establish a relationship of trust. One way is to rely on a third party who "vouches for" the trustworthiness of one or both of the parties.

We may believe a party's affiliation or ask for independent validation. In general, we have a *trust threshold*, a degree of trust we're willing to confer without going further in the certification process. This threshold may depend on the size or nature of the transaction.

The police, Chamber of Commerce, Better Business Bureau, and credit reporting agencies all function in part as certification authorities for such transactions in the "real" world.

Certificates

Electronically, certification is accomplished with digital signatures and hash functions.

A public key and user's identity are bound together in a *certificate*. This is then signed by a *certification authority (CA)*, vouching for the accuracy of the binding.

Certificates (Cont.)

The following are possible steps. Suppose X is the president of the company and her immediate subordinate is Y. Each have a public key pair.

1. X publishes K_X to all employees.
2. Y securely passes message $M = \{Y, K_Y\}$ to X.
3. X produces a hash H of the message, i.e., $h(\{Y, K_Y\})$.
4. X produces $\{M, \{H\}_{K_X^{-1}}\}$.

This last then becomes Y's *certificate*.

What has been accomplished? What assurances does the certificate provide to a third party? What assumptions are required?

Certificates (Cont.)

Y's certificate is X's affirmation of her identity. Anyone can validate the signature with X's public key. Only X could have produced it. The hash ensures that it was not altered.

Now Y can certify the identify of her subordinates in a similar manner. She appends her certificate to each of theirs. This provides a chain of validations back to X.

Thus, an individual's certificate contains a chain of evidence rooted at some authority.

Certificates (Cont.)

There is also a need for trust in situations where there is not a single hierarchy, such as on the Internet. Two individuals may not have a common "superior." Some entity may be designated as a certification authority (notary public, personnel office, security officer in a company, etc.).

On the Internet, several groups serve as "root certification authorities": C & W HTK, SecureNet, Verisign, Baltimore Technologies, Deutsche Telecom, Certiposte, and several others. These tend to be structured around national boundaries.

Why should a user trust the root CAs any more than any other certifier?

The Certification Authority Tree

There are four base structures that certification authorities can adopt:

Single root: one agency acredits every other certification authority.

Multiple roots: many certification authorities with separate spheres of control.

Peers: each organization has its own CA and a collection of CAs from which it will accept certificates.

Bridge: one organization may have many CAs specializing in specific areas or relationships.

Consider the advantages and disadvantages of each of these schemes. When would each be appropriate?

X.509 Certificates

The International Telecommunications Union (ITU) has issued a standard (X.509) for digital certificates that is the basis for many other protocols. An X.509v3 certificate has the following components:

1. *Version:* version of X.509 used;
2. *Serial number:* unique among certificates issued by this issuer;
3. *Signature algorithm identifier:* identifies the algorithm and params used to sign the certificate;
4. *Issuer's distinguished name:* with serial number, makes all certificates unique;
5. *Validity interval:* start and end times for validity;
6. *Subject's distinguished name:* identifies receiver of the certificate;
7. *Subject's public key info:* identifies algorithm, params, and public key;

X.509 Certificates (Cont.)

8. *Issuer's unique id:* used if an Issuer's distinguished name is ever reused;
9. *Subject's unique id:* same as field 8, but for the subject;
10. *Extensions:* version specific information;
11. *Signature:* identifies the algorithm and params, and the signature (encrypted hash of fields 1 to 10).

To validate the certificate, the user obtains the issuer's public key for the algorithm (field 3) and deciphers the signature (field 11). Then uses the information in the signature field (field 11) to recompute the hash and compare with the received value. Finally, check the validity interval.

Key Management

Modern secure systems use symmetric, asymmetric and hybrid methods for a variety of purposes. This imposes significant requirements for generating, protecting, distributing, storing and managing keys.

Comment on how symmetric and asymmetric systems differ with regard to these functions:

- generating keys
- distributing keys
- managing keys (how many are there)

Key Management and Key Distribution

A key management system must control keying material through the lifetime of the keys to prevent unauthorized disclosure, modification, substitution, replay and improper use.

- *Data confidentiality:* keys and other data are kept confidential when transmitted or stored.
- *Modification detection:* counter the threat of modification of data items.
- *Replay detection/timeliness:* have old data been interjected into current conversations or storage.

Key Management and Key Distribution (2)

- *Entity authentication:* corroborate that identities are as claimed.
- *Data origin authentication:* is the source of a message as claimed.
- *Nonrepudiation of Reception:* proof that a message was actually received.
- *Notarization:* register messages to attest content and origin.

Key Management Services

A key management system must provide a set of management services:

- *Entity Registration:* establish a registry of identities/credentials to allow authentication to the system.
- *Key generation:* allow producing keys that are of sufficient quality, secure, and not predictable.
- *Certification:* issue certificates for authentication purposes.
- *Authentication/Verification:* verify identities; three basic types:
  - entity authentication
  - message content authentication
  - message origin authentication

Key Management Services

- *Key Distribution:* secure provide keys to parties requiring them
  - *encipherment:* key may be protected by encrypting with another key
  - *modification detection codes:* add redundancy to detect changes whether accidental or malicious
  - *replay detection:* measures to detect an attempt to foist off an old message as current
  - *proof of knowledge of the key:* allows proving that a party has and is able to use the key (e.g., challenge/response).

Key Management Services

- *Key Maintenance:* preserve, protect and dispose of keys as needed
  - *Key Storage:* secure facility for protecting and accessing keys.
  - *Key Archival:* keys for notarization or non-repudiation may need long term storage.
  - *Key Replacement:* update key material when stale or compromised.
  - *Key Recovery:* re-establish keys lost through human error, software bugs or hardware malfunction
  - *Key Deletion:* securely destroy keys no longer needed.

NSA Encryption Classes

The National Security Agency oversees encryption for the U.S. government. They classify encryption devices into four categories:

- **Type 1:** NSA endorsed classified or controlled cryptographic item for classified or sensitive U.S. government information.
- **Type 2:** NSA endorsed unclassified cryptographic equipment, assemblies or components for sensitive but unclassified U.S. government information.
- **Type 3:** Unclassified cryptographic equipment, assembly, or component used, when appropriately keyed, for encrypting or decrypting unclassified sensitive U.S. Government or commercial information,
- **Type 4:** algorithms that are registered by the NIST but are not FIPS published. Unevaluated commercial cryptographic equipment, assemblies, or components that neither NSA nor NIST certify for any Government usage.

NSA Encryption Classes (2)

In addition NSA recognizes two classes or "suites" of algorithms:

- Suite A: NSA unpublished algorithms intended for highly sensitive communication and critical authentication systems.
- Suite B: NSA endorsed cryptographic algorithms for use as an interoperable cryptographic base for both unclassified information and most classified information.

Don't the NSA restrictions violate the "no security by obscurity" dictum? Explain this apparent contradiction.

Maintaining Secrecy and Integrity

One might try to protect encryption technology by:

- restricting access to all implementations of the algorithm
- keeping the algorithm secret (security through obscurity)
  - NSA Type 1 and Type 2 encryption devices may implement classified algorithms
  - Kerchoff's law says that the best designs should allow the attacker to know everything but the plaintext and key.
  - A Type 3 algorithm is widely published, with several open source implementations.
- Hardware encryption devices typically use tamper-resistance technologies to prevent all but the most determined attackers from compromising the device
  - For consumer-grade devices, tamper-resistance may mean encasing the circuit in epoxy ("potting")
  - Banking devices such as the IBM 4758 automatically zero-out the secret keys if drilled into, frozen or X-rayed
- Keep keys secret (depends on secure transfer of keys—bootstrapping problem). Explain this remark.

Export Control

Many governments regulate the import, export and use of cryptography. Crypto is classified as a "munition" (weapon of war) or "dual use" (having civilian applications) technology.

During the Cold War, CoCom embargoed trade of munitions (including crypto) from the 23 member states of the Soviet Bloc.

CoCom is an acronym for Coordinating Committee for Multilateral Export Controls. CoCom was established in 1947, during the Cold War, to put an embargo on Western exports to East Bloc countries.

Export Control (2)

Until 1996, export of encryption technology from the U.S. required individual case-by-case licensing for each customer *when key sizes of greater than 40 bits could be used.*

Popular products (e.g. Netscape browser and Lotus Notes) were released in two forms: one with an effective 40-bit key where the other bits were revealed in each protocol exchange) and another allowing 128 bits.

While still regulated, the U.S. and other signatories to the Wassenaar Arrangement are more lenient. License exemptions exist for exporting open source crypto.

Some Poetry

What does this poem mean?

Mary had a little key
(It's all she could export)
And all the email that she sent
Was opened at the Fort.

–Ron Rivest

CS378: Information Assurance and Security

Metrics for IA

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Last updated: March 23, 2015 at 08:42

Metrics for IA

Things have their due measure; there are ultimately fixed limits, beyond which, or short of which, something must be wrong. –*Horace*

It is a well-known fact that it is nearly impossible to manage, monitor, control or improve anything without measuring it. –*Debra Herrmann, Complete Guide to Security and Privacy Metrics, p. 4*

Is this True?

The following is quoted from *How to Measure Anything* by Douglas W. Hubbard:

1. Your problem is not as unique as you think.
2. You have more data than you think.
3. You need less data than you think.
4. There is a useful measurement that is much simpler than you think.

What do you think about this quote? To which domains does it apply?

Metrics for IA

The goal of security metrics is to provide the information an organization needs to prevent attack by establishing a quantitative basis for measuring security.

Name some useful security metrics.

What do you think are the fundamental difficulties in defining useful security metrics?

Metrics for IA

According to Herrmann, there are three major types of security/privacy metrics:

Compliance metrics: measure compliance with current security and privacy regulations and standards, such as HIPAA, Sarbanes-Oxley, GLBA, etc.

Resilience metrics: measure the resilience of controls relating to physical security, personnel security, IT security, and operational security both before and after a product, system or network is deployed.

Return on investment (ROI) metrics: measure the ROI in physical, personnel, IT, and operational security controls to guide capital investment.

Metrics

The collection and validation of security and privacy metrics should be embedded in the security engineering life cycle and tied to measurement goals and decision making. –*Herrmann, p. 36*

Patient, accurate data collection and recording is the key to producing accurate measurements. If not well organized, data collection can become very expensive. To contain these costs, the information gathering should be integrated with verification and validation activities. –*IEEE Standards 982.1 and 982.2*

If there are no prestated objectives on how the results will be used, there should be no measurements. –*IEEE Standard 982.2*

Discuss these three assertions. Are they reasonable? Do you agree or disagree? Why?

Terms

Metric: a proposed measure or unit of measure that is designed to facilitate decision making and improve the performance and accountability through collection, analysis, and reporting of relevant data.

Measurement: process by which numbers or symbols are assigned to entities in the real world in such a way as to describe them according to clearly defined rules. The comparison of a property of an object to a similar property of a standard reference.

Primitive: data relating to the development or use of software that is used in developing measures of quantitative descriptions of software. Primitives are directly measurable or countable. Examples include error, fault, failure, time interval, date, and number of an item.

Does this relate to the distinction between data and information?
Be able to explain the relationships among these three notions.

Goals for Metrics

Metrics should provide a means for comparison:

- Between alternatives
- Change over time
- Relative to others: "benchmarking" an organization

Explain these goals. Give examples of each.

Goals for Metrics

Metrics and process-based measures together allow organizations to compare themselves to others. Difference between an organization and others is a "performance gap".

- *Best practices* are often cited as general recommendations.
  - *Gold standard* are the best possible practices.
  - *Best current practice* (BCP) are often recommended based on current technology or environments.
- *Standard of due care:* what any organization would do in similar circumstances.
- *Due diligence* is the process that an organization ensures standards provide adequate protections.

Why do organizations care about these? Which of these are necessary? Which are most desirable?

Regulations and Best Practice

Recall from our slideset on IA in Business:

Regulations often define "best practice" within a *particular industry.* Different industries have different standards. Why do you suppose that is?

> *"There is no single definition of the 'best practices' for an information security program. ... In fact, the term 'best practices' for information security is really a misnomer or even could be considered a myth."* *(Landoll)*

Due Diligence

Due diligence is a term used for a number of concepts involving either the performance of an investigation of a business or person, or the performance of an act with a certain standard of care.

First came into common use as a result of the U.S. Securities Act of 1933. So long as broker/dealers conducted a "Due Diligence" investigation into the company whose equity they were selling, and disclosed to the investor what they found, they would not be held liable for nondisclosure of information they failed to uncover in the process of that investigation.

What is the driver for this? I.e., what does it require and why do organizations strive for due diligence?

Malfeasance

Nonfeasance is failure to perform an official duty or legal requirement. *Malfeasance* is misconduct or wrongdoing esp. by a public official.

Information security due diligence is often undertaken during the information technology procurement process to ensure risks are known and managed.

Using Metrics

There are two important aspects of metrics:

- How you compute them
- How you use them

Think about the metrics used to evaluate the competence of K–12 teachers. Are they susceptible to misuse?

Classifying and Prioritizing Threats

An important fact to measure is *how secure your system is*. Various frameworks have been devised for this, some more successful than others.

The driving reality is that *not all vulnerabilities are equally serious.*

> *In a perfect world [...] we would tell you that if there's even the slightest chance of a single attacker being able to compromise a single user for even the smallest nuisance attack, that you should hold off the product release until every single possible vulnerability has been eliminated from the code. ... You'd never actually ship any code.* –*Sullivan and Liu, A Beginner's Guide to Web Application Security*

STRIDE

STRIDE is a threat classification system designed by Microsoft. It does not attempt to rank or prioritize vulnerabilities, only to classify them:

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Many vulnerabilities may cross boundaries and some are "threshold attacks" that lead to others.

IIMF

The IIMF model classifies potential vulnerabilities according to four categories:

- Interception
- Interruption
- Modification
- Fabrication

Again, there may be overlap. Compare and contrast IIMF and STRIDE.

CIA

CIA classifies potential vulnerabilities according to violations on the traits we want a system to have:

- Confidentiality
- Integrity
- Availability

Some groups (notably NSA) add two more high level security goals to derive CIA-AN:

- Authenticity
- Nonrepudiation

Common Weakness Enumeration (CWE)

The Common Weakness Enumeration (maintained by the MITRE Corporation) is a general list of types of software vulnerabilities, such as:

- SQL injection (CWE-89)
- Buffer overflow (CWE-120)
- Missing encryption of sensitive data (CWE-311)
- Cross-site request forgery (CWE-352)
- Use of a broken or weak crypto algorithm (CWE-327)
- Integer overflow (CWE-190)

MITRE (in conjunction with the SANS Institute) also publishes an annual list of the top 25 most dangerous CWE issues. Find and investigate the CWE list.

DREAD

DREAD is another system from Microsoft. Unlike STRIDE, it not only classifies potential threats, but also ranks them. Compute 5 potential subscores for each vulnerability (scale 1..10) and for each of:

- Damage potential
- Reproducibility (or Reliability)
- Exploitability
- Affected users
- Discoverability

Add scores together and divide by 5 to get an overall DREAD score. Critique this approach. Having Discoverability as a component of the score is often criticized. Can you see why?

Critique of DREAD

- Not all of the DREAD criteria are necessarily equal in ranking any vulnerability, even though they are treated that way in the method.
- The ratings are highly subjective.
- In security, it might be best to take a pessimistic view and assume that if the vulnerability is present, it will be discovered and exploited.

DREAD has fallen out of favor, even within Microsoft.

Common Vulnerability Scoring System (CVSS)

A more common metric for rating vulnerabilities is the CVSS, created by a consortium of software vendors and security organizations, including: CMU CERT, Cisco, DHS, MITRE, eBay, IBM, Microsoft, others.

CVSS is currently maintained by the Forum of Incident Response and Security Teams (FIRST).

Rate each vulnerability in three dimensions on a scale 0..10:

- Base equations: objective characteristics of the vulnerability
- Temporal score: how may the risk change over time
- Environmental score: how is the vulnerability specific to your organization

CVSS

Unlike DREAD, the components are weighted according to a complicated formula.

Rather than compute by hand, use one of the CVSS online calculators. For example, one is hosted at the National Vulnerability Database (NVD) site:

`nvd.nist.gov/cvss.cfm?calculator`

Cost Metrics for Security and IA

Multiple costs combine into *Total Cost of Ownership* (TCO):

- direct costs: labor, equipment
- indirect costs: contractor overhead
- hidden costs: inefficiency and opportunity costs

What are opportunity costs?

Cost metrics are often used to compare similar companies:

- Number of staff, or number of staff-hours
- Amount spent per project, year or total on IA

Costs of Security and IA

Within a typical large company or government organization, security is a small part of the overall budget.

- Joint Security Commission of 1994 found security, in general, to be less then one percent of total operating costs. Do you think that's still true?
- However, this rule does not hold for SECRET/TOP SECRET projects: in unacknowledged programs 40% of the costs may be security.

According to Security500,2/14/11:

> *IT security staff at small and midsize businesses spend 127 hours every month managing their on-premises security infrastructure, according to a new survey by Webroot.*

Asset Value and Cost-Benefit Analysis

Benefit is the value an organization receives by using controls and countermeasures associated with a specific vulnerability.

- Typically by valuing the exposed asset and finding the percentage exposed.
- Asset valuation is often difficult or inconsistent across organizations.
  - Assets may have intrinsic value as well as acquired value (a storage array may have a higher value than the value of the underlying disks and controllers).
  - Intellectual property valuation may depend on the cost to acquire or produce the intellectual property, its worth (e.g. how much it can make over its lifetime), and how much it costs to protect it.

Some Metrics

Single Loss Expectancy: depends on percentage loss if a vulnerability is exploited; (SLE = asset value * exposure factor).

Exposure factor is the impact of the risk over the asset, or percentage of asset lost.

Annualized Rate of Occurence (ARO): how many times the attack will occur.

Annualized Loss Expectancy (ALE): (ALE = SLE * ARO)

Cost Benefit = (ALE_{before} - ALE_{after}) - Cost of safeguard

Identifying the Risk

Security planning is really about *risk management*—how much to spend on protection against what. This should be done within the broader framework of managing non-IT risks.

One common tool is the *annualized loss expectancy* (ALE), which is a table of possible losses, their likelihood, and potential cost. Example, for a bank with the following ALE, where should they put their security dollars?

Loss type	**Amount**	**Incidence**	**ALE**
SWIFT fraud	$50,000,000	.005	$250,000
ATM fraud (large)	$250,000	.2	$100,000
ATM fraud (small)	$20,000	.5	$10,000
Teller theft	$3,240	200	$648,000

Financial Metrics

38% of organizations in CSI/FBI survey use *Return On Investment* (ROI) to compare security investments. ROI is a percentage (benefit/cost) over time, e.g. 3 years:

$$\frac{[(b/(1+d)) + (b/(1+d)^2) + (b/(1+d)^3)]}{c}$$

where b is the benefit, d is the discount rate, and c is the initial cost.

18% use *Net Present Value (NPV)*. NPV is a currency value of expected return (benefits-cost) over time.

19% use *Internal Rate of Return (IRR)*. IRR is a discount rate chosen so that NPV would be 0. The investment with the highest IRR is preferred.

MTBF

Failure rate is the number of failures of a part in a population, divided by the sum total of time expended by all the parts in the population.

Mean-time-between-failure (MTBF) is the reciprocal of the failure rate. MTBF of a system depends on the interrelationship of the parts.

MTBF (continued)

In an architecture with the possibility of serial failures, failure of any one component part will fail whole system.

- Serial failures combine the failure rates of each of the parts.
- Redundancy allows for continued operation even if one part fails, so long as
  - there is a redundant path (e.g. two power supplies plugged in and both connected to the bus),
  - there are adequate standby parts which have not failed to take over, and
  - the failure detection circuit is working correctly, and is able to lock out the failed part. Typically redundancy is used to protect a few subassembles which have a high failure rate but it is possible to detect and recover, such as a bad power supply, bad network cable, or disk in a RAID array.

MTBF (continued)

MTBF only provides an estimate, useful during the design phases, to highlight areas where high failure rates might be predicted. Actual experiences may differ from MTBF as:

- Parts quality may not be the same as the part for which MTBF was originally estimated.
- Parts may be subjected to conditions outside of the bounds by which MTBF was estimated.

Recovery, MTTR and Availability

Mean time to repair (MTTR) after a failure (or attack). Goal is to reduce downtime costs

- In 2000, Amazon estimated losses due to downtime at $180,000 per hour.
- Ebay estimates $225,000 per hour (and had a 22 hour outage).

Availability is the percentange of uptime. Inherent availability is

$$(A = MTBF \ / \ (MTBF + MTTR))$$

Marketing literature quotes "5 nines" availability: 99.999%

- translates to 5 minutes downtime/year;
- however, requires "pre-defined, pre-tested environments"

If availability is particularly important to your organization, how might you enhance it?

Recovery, MTTR and Availability (continued)

Operational availability must take into account the time between maintenance (not just failure), and the downtime due to maintenance.

Availability metrics may no longer be valid if environment changes.

- In particular the introduction of new threats!
- Or when running in a "degraded capability."

Quality

ISO 9000/9001 quality typically implies that organizations have and follow documented, measurable procedures.

Data quality metrics are often used when reviewing the state of a database, such as when reviewing the database for use in a new project.

- Data decay: data in a database may lose currency or value over time as it becomes out of date. A significant issue affecting Customer Relationship Management (CRM) databases.
- Attacks may corrupt database. Yet few metrics have been defined for the quality of security-sensitive databases (password files, etc.)

ISO 9000

ISO 9000 is a family of standards for quality management systems, maintained by the International Organization for Standardization and is administered by accreditation and certification bodies.

- a set of procedures covering all key processes in the business;
- monitoring processes ensuring effectiveness;
- keeping adequate records;
- checking output for defects, with appropriate corrective action;
- regularly reviewing individual processes and the quality system itself for effectiveness; and
- facilitating continual improvement.

A "product," in ISO vocabulary, can mean a physical object, or services, or software, but "service sectors now account by far for the highest number of ISO 9001:2000 certificates - about 31% of the total."

ISO 9001: Key Features

- Quality manual is required
- Decisions made on recorded data and regularly audited
- Records show how and where materials acquired and processed
- Documented procedure to control quality documents
- Provide suitable infrastructure, resources, information, equipment, conditions
- Clear quality objectives for each product
- Determine key monitoring points in the process
- Set clear requirements for purchased product
- Establish procedures for customer information
- Plan stages of development for new products
- Review performance through internal audits
- Document procedures for nonconformance

Quality (continued)

Quality of service (QoS) metrics are often incorporated by contracts with service providers.

- Service providers face financial and indirect penalties if QoS cannot be met.
- May not be able to meet levels while under attack, after a natural threat has occurred, and during recovery.

Effectiveness of Protection

Monitoring is essential to determine if countermeasures are having the desired effect. However, determining the appropriate metrics may be difficult as the underlying landscape is changing.

- New threats not anticipated by current countermeasures may cause a change of metric to be required, which hinders long-timescale or cross-organization comparison.

Often, organizations may wish to compare the number of successful attacks to the number of total attempts.

- However, this metric needs to take into account the impact of the attack. For example, many organizations do not consider attacks against their external web site to be significant unless they succeed.
- Furthermore, finding the total number of attack attempts may be difficult. Is every packet that a firewall detects coming from a hacker scanning the Internet for vulnerabilities an 'attack'?

Effectiveness of Protection (continued)

Metrics are not yet consistent for other events, such as human error, and in many cases the underlying protection mechanisms do not yet give adequate reports.

Instructor Materials Chapter 1: A World of Wizard, Heroes, and Criminals

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 1:
A World of Wizard, Heroes, and Criminals

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 1 - Sections & Objectives

- 1.1 Characteristics of Cybersecurity World
  - Describe the common characteristics comprising the cybersecurity world
- 1.2 Criminals and Cybersecurity Professionals
  - Differentiate the characteristics of cyber criminals and heroes
- 1.3 Comparing Cybersecurity Threats
  - Compare how cybersecurity threats affect individuals, businesses, and organizations
- 1.4 Cybercrime Growth Factors
  - Analyze the organizations and efforts committed to expanding the cybersecurity workforce

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.1 The Cybersecurity World

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Overview of the Kingdoms

- Websites and Power of Data
  - Great businesses have been created by collecting and harnessing the power of data and data analytics
  - These businesses have the responsibility to protect this data from misuse and unauthorized access
  - The growth of data has created great opportunities for cybersecurity specialists
- Kingdoms
  - Business large and small have recognized the power of big data and data analytics
  - Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
  - The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Overview of the Kingdoms (Cont.)

- Cyber wizards now have the technology to track worldwide weather trends, monitor the oceans, and track the movement and behavior of people, animals and objects in real time.
- New technologies, such as Geospatial Information Systems (GIS) and the Internet of Everything (IoE), have emerged. Each depends on collecting and analyzing tremendous amounts of data.
- This growing collection of data can help people save energy, improve efficiencies, and reduce safety risks.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.2 Cyber Criminals versus Cyber Professionals

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Criminals

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.

  White hat attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.

  Gray hat attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.

  Black hat attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists -** Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers -** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations. Most countries in the world participate to some degree in state-sponsored hacking.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Specialists

Thwarting the cyber criminals is a difficult task, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database**: The Nation Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all know vulnerabilities. http://www.cvedetails.com/
- **Early Warning Systems**: The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualization of attacks. https://www.honeynet.org/node/960
- **Share Cyber Intelligence**: InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the and the private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks. https://www.infragard.org/

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Specialist (Cont.)

- **ISM Standards**: The ISO 27000 standards are an example of Information Security Management Standards. The standards provide a framework for implementing cybersecurity measures within an organization. http://www.27000.org/
- **New Laws**: The ISACA group track law enacted related to cyber security. These laws can address individual privacy to protection of intellectual property. Examples of these laws include: Cybersecurity Act, Federal Exchange Data Breach Notification Act and the Data Accountability and Trust Act. http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Tools for Thwarting Cybercrime

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.3 Threats to the Kingdom

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threat Arenas

- The term cyber wizards refers to the innovators and visionaries that build the cyber kingdom
- Cyber wizards possess the insight to recognize the influence of data and harness that power to build great organizations, provide services and protect people from cyberattacks
- Cyber wizards recognize the threat that data poses if used against people
- A cybersecurity threat is the possibility that a harmful event, such as an attack, will occur
- Cyber vulnerability is a weakness that makes a target susceptible to an attack
- Cyber threats are particularly dangerous to certain industries and the type of information they collect and protect

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threat Arenas (Cont.)

The following examples are just a few sources of data that can come from established organizations:

- **Personal Information**
- **Medical Records**
- **Education Records**
- **Employment and Financial Records**

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threats to the Kingdom

Threat Arenas (Cont.)

Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

- Criminals use packet-sniffing tools to capture data streams over a network. Packet sniffers work by monitoring and recording all information coming across a network.
- Criminals can also use rogue devices, such as unsecured Wi-Fi access points.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threats to the Kingdom

Threat Arenas (Cont.)

Sectors of the kingdom include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Threat Arenas (Cont.)

- On a personal level, everyone needs to safeguard his or her identity, data, and computing devices.
- At the corporate level, it is the employees' responsibility to protect the organization's reputation, data, and customers.
- At the state level, national security and the citizens' safety and well-being are at stake.
- In the U.S., the National Security Agency (NSA) is responsible for intelligence collection and surveillance activities.
- The efforts to protect people's way of life often conflicts with their right to privacy.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.4 The Dark Forces of Cybersecurity

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Spread of the Dark Forces

Attacks can originate from within an organization or from outside of the organization, as shown in the figure.

Internal Security Threats

- An internal user, such as an employee or contract partner, can accidently or intentionally
- Internal threats have the potential to cause greater damage than external threats because internal users have direct access to the building and its infrastructure devices. Internal attackers typically have knowledge of the corporate network, its resources, and its confidential data. They may also have knowledge of security countermeasures, policies and higher levels of administrative privileges.

External Security Threats

- External threats from amateurs or skilled attackers can exploit vulnerabilities in networked devices, or can use social engineering, such as trickery, to gain access.
- External attacks exploit weaknesses or vulnerabilities to gain access to internal resources.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Spread of the Dark Forces (Cont.)

Vulnerabilities of Mobile Devices - In the past, employees typically used company-issued computers connected to a corporate LAN.

- Today, mobile devices such as iPhones, smartphones, tablets, and thousands of other devices, are becoming powerful substitutes for, or additions to, the traditional PC.
- More and more people are using these devices to access enterprise information. Bring Your Own Device (BYOD) is a growing trend.
- The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Spread of the Dark Forces (Cont.)

- **Emergence Internet-of-Things** - The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet.
- IoT technologies enable people to connect billions of devices to the Internet. These devices include appliances, locks, motors, and entertainment devices, to name just a few.
- This technology affects the amount of data that needs protection. Users access these devices remotely, which increases the number of networks requiring protection.
- With the emergence of IoT, there is much more data to be managed and secured. All of these connections, plus the expanded storage capacity and storage services offered through the Cloud and virtualization, has led to the exponential growth of data.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Spread of the Dark Forces (Cont.)

Impact of Big Data – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

There are numerous examples of big corporate hacks in the news. As a result, enterprise systems require dramatic changes in security product designs and substantial upgrades to technologies and practices. Additionally, governments and industries are introducing more regulations and mandates that require better data protection and security controls to help guard big data.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Sophistication of the Dark Forces

Advanced Weapons

- Advanced persistent threat (APT) is a continuous computer hack that occurs under the radar against a specific object. Criminals usually choose an APT for business or political motives.
- Algorithm attacks can track system self-reporting data, like how much energy a computer is using, and use that information to select targets or trigger false alerts. Algorithmic attacks are more devious because they exploit designs used to improve energy savings, decrease system failures, and improve efficiencies.
- Intelligent selection of victims. In the past, attacks would select the low hanging fruit or most vulnerable victims. Many of the most sophisticated attacks will only launch if the attacker can match the signatures of the targeted victim.

Broader Scope and Cascade Effect

- Federated identity management refers to multiple enterprises that let their users use the same identification credentials gaining access to the networks of all enterprises in the group. The goal of federated identity management is to share identity information automatically across castle boundaries.
- The most common way to protect federated identity is to tie login ability to an authorized device.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Sophistication of the Dark Forces (Cont.)

Safety Implications

- There are many safety implication associated with the dark forces of cyber security including emergency call centers in the U.S. are vulnerable to cyberattacks that could shut down 911 networks, jeopardizing public safety.
- A telephone denial of service (TDoS) attack uses phone calls against a target telephone network tying up the system and preventing legitimate calls from getting through.
- The next generation 911 call centers are vulnerable because they use Voice-over-IP (VoIP) systems rather than traditional landlines.

Heightened Recognition of Cybersecurity Threats

- The defenses against cyberattacks at the start of the cyber era were low. A smart high school student or script kiddie could gain access to systems.
- Now, countries across the world have become more aware of the threat of cyberattacks. The threat posed by cyberattacks now head the list of greatest threats to national and economic security in most countries.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.5 Creating More Heroes

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Creating More Heroes

A Workforce Framework for Cybersecurity

Addressing the Shortage of Cybersecurity Specialists

- In the U.S., the National Institute of Standards and Technologies (NIST) created a framework for companies and organizations in need of cybersecurity professionals. The framework enables companies to identify the major types of responsibilities, job titles, and workforce skills needed.

The Seven Categories of Cybersecurity Wizards

The Workforce Framework categorizes cybersecurity work into seven categories.

- **Operate and Maintain** includes providing the support, administration, and maintenance required to ensure IT system performance and security
- **Protect and Defend** includes the identification, analysis, and mitigation of threats to internal systems and networks
- **Investigate** includes the investigation of cyber events and/or cyber crimes involving IT resources
- **Collect and Operate** includes specialized denial and deception operations and the collection of cybersecurity information

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

A Workforce Framework for Cybersecurity (Cont.)

- **Analyze** includes highly specialized review and evaluation of incoming cybersecurity information to determine if it is useful for intelligence
- **Oversight and Development** provides for leadership, management, and direction to conduct cybersecurity work effectively
- **Securely Provision** includes conceptualizing, designing, and building secure IT systems

Within each category, there are several specialty areas. The specialty areas then define common types of cybersecurity work.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Online Cybersecurity Communities

Professional Organizations

- Cybersecurity specialists must collaborate with professional colleagues frequently. International technology organizations often sponsor workshops and conferences. Visit each site with your class and explore the resources available.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Online Cybersecurity Communities

Cybersecurity Student Organizations and Competitions

- Cybersecurity specialists must have the same skills as hackers, especially black hat hackers, in order to protect against attacks.
- How can an individual build and practice the skills necessary to become a cybersecurity specialist?
- Student skills competitions are a great way to build cybersecurity knowledge skills and abilities.
- There are many national cybersecurity skills competitions available to cybersecurity students.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Certifications

Industry Certifications

In a world of cybersecurity threats, there is a great need for skilled and knowledgeable information security professionals. The IT industry established standards for cybersecurity specialists to obtain professional certifications that provide proof of skills, and knowledge level.

- **CompTIA Security+ -** Security+ is a CompTIA-sponsored testing program that certifies the competency of IT administrators in information assurance.
- **EC-Council Certified Ethical Hacker (CEH) –** CEH is an intermediate-level certification asserts that cybersecurity specialists holding this credential possess the skills and knowledge for various hacking practices.
- **SANS GIAC Security Essentials (GSEC) -** The GSEC certification is a good choice for an entry-level credential for cybersecurity specialists who can demonstrate that they understand security terminology and concepts and have the skills and expertise required for “hands-on” security roles. The SANS GIAC program offers a number of additional certifications in the fields of security administration, forensics, and auditing.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Creating More Heroes

Cybersecurity Certifications (Cont.)

- **(ISC)^2 Certified Information Systems Security Professional (CISSP) -** The CISSP certification is a vendor-neutral certification for those cybersecurity specialists with a great deal of technical and managerial experience. It is also formally approved by the U.S. Department of Defense (DoD) and is a globally recognized industry certification in the security field.
- **ISACA Certified Information Security Manager (CISM) -** Cyber heroes responsible for managing, developing and overseeing information security systems at the enterprise level or for those developing best security practices can qualify for CISM.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Certifications (Cont.)

Company Sponsored Certifications - Another important credential for cybersecurity specialists are company-sponsored certifications. These certifications measure knowledge and competency in installing, configuring, and maintaining vendor products. Cisco and Microsoft are examples of companies with certifications that test knowledge of their products. Click here to explore the matrix of the Cisco certifications shown in the figure.

Cisco Certified Network Associate Security (CCNA Security) - The CCNA Security certification validates that a cybersecurity specialist has the knowledge and skills required to secure Cisco networks.

Cisco Certifications

	Entry	Associate	Professional	Expert
Architect				CCAr Architect
Cloud		CCNA Cloud	CCNP Cloud	
Collaboration		CCNA Collaboration	CCNP Collaboration	CCIE Collaboration
Data Center		CCNA Data Center	CCNP Data Center	CCIE Data Center
Design	CCENT	CCDA	CCDP	CCDE
Industrial / IoT		CCNA Industrial		
Routing & Switching	CCENT	CCNA Routing & Switching	CCNP Routing & Switching	CCIE Routing & Switching
Security	CCENT	CCNA Security	CCNP Security	CCIE Security
Service Provider		CCNA SP	CCNP SP	CCIE SP
Wireless	CCENT	CCNA Wireless	CCNP Wireless	CCIE Wireless
Other Certifications	Certified Technician			
Specialist	Business	Data Center	Internet of Things	Network Programmability
	Security	Operating System Software	Service Provider	Collaboration

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Certifications (Cont.)

How to Become a Cyber Hero

Heroes must be able to respond to threats as soon as they occur. This means that the working hours can be somewhat unconventional. Cyber heroes also analyze policy, trends, and intelligence to understand how cyber criminals think. Many times, this may involve a large amount of detective work. Here is good advice for becoming a cybersecurity hero:

- **Study**: Learn the basics by completing courses in IT. Be a life-long learner. Cybersecurity is an ever-changing field, and cybersecurity specialists must keep up.
- **Pursue Certifications**: Industry and company sponsored certifications from organizations such as Microsoft and Cisco prove that one possesses the knowledge needed to seek employment as a cybersecurity specialist.
- **Pursue Internships**: Seeking out a security internship as a student can lead to opportunities down the road.
- **Join Professional Organizations**: Join computer security organizations, attend meetings and conferences, and join forums and blogs to gain knowledge from the experts.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

1.6 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter Summary

Summary

- This chapter explained the structure of the cybersecurity world and the reason it continues to grow with data and information as the prized currency.
- It explored the motivation of cyber criminals.
- It explored the spread of the dark forces due to the ever-expanding technical transformations taking place throughout the world.
- It provided details on how to become a cyber hero to help defeat the cyber criminals that empower the dark forces.
- It surveyed the resources available to help create more heroes.
- It explained that cyber professionals must have the same skills as the cyber criminals.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials Chapter 2: The Cybersecurity Sorcery Cube

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 2:
The Cybersecurity Sorcery Cube

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 2 - Sections & Objectives

2.1 The Cybersecurity Sorcery Cube

Describe the three dimensions of the McCumber Cube.

2.2 CIA TRIAD

Describe the principles of confidentiality, integrity, and availability.

2.3 States of Data

Differentiate the three states of data.

2.4 Cybersecurity Countermeasures

Compare the types of cybersecurity countermeasures.

2.5 IT Security Management Framework

Describe the ISO Cybersecurity Model

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.1 The Cybersecurity Sorcery Cube

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Three Dimensions

The Principles of Security

- The first dimension of the cybersecurity sorcery cube identifies the goals to protect the cyber world. The goals identified in the first dimension are the foundational principles of the cybersecurity world.
- These three principles are confidentiality, integrity and availability.
- The principles provide focus and enable the cyber wizard to prioritize actions in protecting the cyber world.
- Use the acronym CIA to remember these three principles.

The States of Data

- The cyber world is a world of data; therefore, cyber wizards focus on protecting data. The second dimension of the cybersecurity sorcery cube focuses on the problems of protecting all of the states of data in the cyber world. Data has three possible states:

  1) Data at rest or in storage 2) Data in transit 3) Data in process

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Three Dimensions (Cont.)

Cybersecurity Safeguards

- The third dimension of the cybersecurity sorcery cube defines the types of powers used to protect the cyber world. The sorcery cube identifies the three types of powers:
- **Technologies -** devices, and products available to protect information systems and fend off cyber criminals.
- **Policies and Practices -** procedures, and guidelines that enable the citizens of the cyber world to stay safe and follow good practices.
- **People -** Aware and knowledgeable about their world and the dangers that threaten their world.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.2 CIA TRIAD

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Confidentiality

The Principle of Confidentiality

- Confidentiality prevents the disclosure of information to unauthorized people, resources and processes. Another term for confidentiality is privacy.
- Organizations need to train employees about best practices in safeguarding sensitive information to protect themselves and the organization from attacks.
- Methods used to ensure confidentiality include data encryption, authentication, and access control.

Protecting Data Privacy

- Organizations collect a large amount of data and much of this data is not sensitive because it is publicly available, like names and telephone numbers.
- Other data collected, though, is sensitive. Sensitive information is data protected from unauthorized access to safeguard an individual or an organization.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Confidentiality (Cont.)

Controlling Access

Access control defines a number of protection schemes that prevent unauthorized access to a computer, network, database, or other data resources. The concepts of AAA involve three security services: Authentication, Authorization and Accounting. ***Authentication*** verifies the identity of a user to prevent unauthorized access. Users prove their identity with a username or I.D.

Authorization services determine which resources users can access, along with the operations that users can perform. Authorization can also control when a user has access to a specific resource.

Accounting keeps track of what users do, including what they access, the amount of time they access resources, and any changes made.

© 2008 Cisco Systems, Inc. All rights reserved.

Confidentiality (Cont.)

Confidentiality and privacy seem interchangeable, but from a legal standpoint, they mean different things.

- Most privacy data is confidential, but not all confidential data is private. Access to confidential information occurs after confirming proper authorization. Financial institutions, hospitals, medical professionals, law firms, and businesses handle confidential information.
- Confidential information has a non-public status. Maintaining confidentiality is more of an ethical duty.
- Privacy is the appropriate use of data. When organizations collect information provided by customers or employees, they should only use that data for its intended purpose.

U.S. Laws

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- Gramm-Leach-Bliley Act (GLBA)
- California Senate Bill 1386 (SB 1386)
- U.S. Banking Rules and Regulations
- Payment Card Industry Data Security Standard (PCI DSS)
- Fair Credit Reporting Act (FCRA)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Integrity

Principle of Data Integrity

- Integrity is the accuracy, consistency, and trustworthiness of data during its entire life cycle.
- Another term for integrity is quality.
- Methods used to ensure data integrity include hashing, data validation checks, data consistency checks, and access controls.

Need for Data Integrity

- The need for data integrity varies based on how an organization uses data. For example, Facebook does not verify the data that a user posts in a profile.
- A bank or financial organization assigns a higher importance to data integrity than Facebook does. Transactions and customer accounts must be accurate.
- Protecting data integrity is a constant challenge for most organizations. Loss of data integrity can render entire data resources unreliable or unusable.

Integrity Checks

- An integrity check is a way to measure the consistency of a collection of data (a file, a picture, or a record). The integrity check performs a process called a hash function to take a snapshot of data at an instant in time.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Availability

Data availability is the principle used to describe the need to maintain availability of information systems and services at all times. Cyberattacks and system failures can prevent access to information systems and services.

- Methods used to ensure availability include system redundancy, system backups, increased system resiliency, equipment maintenance, up-to-date operating systems and software, and plans in place to recover quickly from unforeseen disasters.
- High availability systems typically include three design principles: eliminate single points of failure, provide for reliable crossover, and detect failures as they occur.

Organizations can ensure availability by implementing the following:

1. Equipment maintenance
2. OS and system updates
3. Test backups
4. Plan for disasters
5. Implement new technologies
6. Monitor unusual activity
7. Test to verify availability

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.3 States of Data

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

States of Data

Data at Rest

- Stored data refers to data at rest. Data at rest means that a type of storage device retains the data when no user or process is using it.
- A storage device can be local (on a computing device) or centralized (on the network). A number of options exist for storing data.
- Direct-attached storage (DAS) is storage connected to a computer. A hard drive or USB flash drive is an example of direct-attached storage.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data at Rest (Cont.)

- Redundant array of independent disks (RAID) uses multiple hard drives in an array, which is a method of combining multiple disks so that the operating system sees them as a single disk. RAID provides improved performance and fault tolerance.
- A network attached storage (NAS) device is a storage device connected to a network that allows storage and retrieval of data from a centralized location by authorized network users. NAS devices are flexible and scalable, meaning administrators can increase the capacity as needed.
- A storage area network (SAN) architecture is a network-based storage system. SAN systems connect to the network using high-speed interfaces allowing improved performance and the ability to connect multiple servers to a centralized disk storage repository.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data In Transit

Data transmission involves sending information from one device to another. There are numerous methods to transmit information between devices including:

- **Sneaker net** – uses removable media to physically move data from one computer to another
- **Wired networks** – uses cables to transmit data
- **Wireless networks** – uses the airwaves to transmit data

The protection of transmitted data is one of the most challenging jobs of a cybersecurity professional. The greatest challenges are:

- **Protecting data confidentiality** – cyber criminals can capture, save and steal data in-transit.
- **Protecting data integrity** – cyber criminals can intercept and alter data in-transit.
- **Protecting data availability** - cyber criminals can use rogue or unauthorized devices to interrupt data availability.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data In Process

The third state of data is data in process. This refers to data during initial input, modification, computation, or output.

- Protection of data integrity starts with the initial input of data.
- Organizations use several methods to collect data, such as manual data entry, scanning forms, file uploads, and data collected from sensors.
- Each of these methods pose potential threats to data integrity.
- Data modification refers to any changes to the original data such as users manually modifying data, programs processing and changing data, and equipment failing resulting in data modification.
- Processes like encoding/decoding, compression/decompression and encryption/decryption are all examples of data modification. Malicious code also results in data corruption.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.4 Cybersecurity Countermeasures

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Technologies

Software-based Technology Safeguards

- Software safeguards include programs and services that protect operating systems, databases, and other services operating on workstations, portable devices, and servers. There are several software-based technologies used to safeguard an organization's assets.

Hardware-based Technology Safeguards

- Hardware based technologies are appliances that are installed within the network faculties. They can include: Firewall appliances, Intrusion Detection Systems (IDS),Intrusion Prevention Systems (IPS) and Content filtering systems.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Technologies

Network-based Technology Safeguards

Technological countermeasures can also include network-based technologies.

- **Virtual Private Network (VPN)** is a secure virtual network that uses the public network (i.e., the Internet). The security of a VPN lies in the encryption of packet content between the endpoints that define the VPN.
- **Network access control (NAC)** requires a set of checks before allowing a device to connect to a network. Some common checks include up-to-data antivirus software or operating system updates installed.
- **Wireless access point security** includes the implementation of authentication and encryption.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Technologies

Cloud-based Technology Safeguards

- Technological countermeasures now also include cloud-based technologies. Cloud-based technologies shift the technology component from the organization to the cloud provider.
- **Software as a Service (SaaS)** allows users to gain access to application software and databases. Cloud providers manage the infrastructure. Users store data on the cloud provider's servers.
- **Infrastructure as a Service (IaaS)** provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components.
- **Virtual security appliances** run inside a virtual environment with a pre-packaged, hardened operating system running on virtualized hardware.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Implementing Cybersecurity Education and Training

A security awareness program is extremely important for an organization. An employee may not be purposefully malicious but just unaware of what the proper procedures are.

There are several ways to implement a formal training program:

- Make security awareness training a part of the employee's onboarding process
- Tie security awareness to job requirements or performance evaluations
- Conduct in-person training sessions
- Complete online courses

Security awareness should be an ongoing process since new threats and techniques are always on the horizon.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Policies and Procedures

- A security **policy** is a set of security objectives for a company that includes rules of behavior for users and administrators and specifies system requirements. These objectives, rules, and requirements collectively ensure the security of a network, the data, and the computer systems within an organization.
- **Standards** help an IT staff maintain consistency in operating the network. Standards provide the technologies that specific users or programs need in addition to any program requirements or criteria that an organization must follow.
- **Guidelines** are a list of suggestions on how to do things more efficiently and securely. They are similar to standards, but are more flexible and are not usually mandatory. Guidelines define how standards are developed and guarantee adherence to general security policies.
- **Procedure** documents are longer and more detailed than standards and guidelines. Procedure documents include implementation details that usually contain step-by-step instructions and graphics.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.5 IT Security Management Framework

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The ISO Model

Security professionals need to secure information from end-to-end within the organization. This is a monumental task, and it is unreasonable to expect one individual to have all of the requisite knowledge.

The **International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC)** developed a comprehensive framework to guide information security management.

The ISO cybersecurity model is to cybersecurity professionals what the OSI networking model is to network engineers. Both provide a framework for understanding and approaching complex tasks.

© 2008 Cisco Systems, Inc. All rights reserved.

The ISO Model (Cont.)

ISO/IEC 27000 is an information security standard published in 2005 and revised in 2013. ISO publishes the ISO 27000 standards. Even though the standards are not mandatory, most countries use them as a de facto framework for implementing information security.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Using the ISO Cybersecurity Model

- The ISO 27000 is a universal framework for every type of organization. In order to use the framework effectively, an organization must narrow down which domains, control objectives, and controls apply to its environment and operations.
- The ISO 27001 control objectives serve as a checklist. The first step an organization takes is to determine if these control objectives are applicable to the organization.

ISO/IEC 27002 Section	Primary Objective		
	Confidentiality	Integrity	Availability
5			
5.1			
5.1.1	√	√	√
5.1.2	√	√	√
6			
6.1			
6.1.1	√	√	√
6.1.2		√	√
6.1.3			√
6.1.4	√		√
6.1.5	√		
6.1.6	√	√	√
6.1.7	√	√	√
6.1.8	√	√	√

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Using the ISO Cybersecurity Model (Cont.)

The ISO Cybersecurity Model and the States of Data

- Different groups within an organization may be responsible for data in each of the various states.
- For example, the network security group is responsible for data during transmission.
- Programmers and data entry people are responsible for data during processing.
- The hardware and server support specialists are responsible for stored data. The ISO Controls specifically address security objectives for data in each of the three states.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Using the ISO Cybersecurity Model (Cont.)

The ISO Cybersecurity Model and Safeguards

- The ISO 27001 control objectives relate directly to the organization's cybersecurity policies, procedures and guidelines which upper management determines.
- The ISO 27002 controls provide technical direction. For example, upper management establishes a policy specifying the protection of all data coming in to or out of the organization. Implementing the technology to meet the policy objectives would not involve upper management.
- It is the responsibility of IT professionals to properly implement and configure the equipment used to fulfill the policy directives set by upper management.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.6 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

- This chapter discussed the three dimensions of the cybersecurity sorcery cube. The central responsibility of a cybersecurity wizard is to protect an organization's systems and data.
- The chapter explained how each of the three dimensions contributes to that effort.
- The chapter also discussed the ISO cybersecurity model. The model represents an international framework to standardize the management of information systems.
- This chapter explored the twelve domains. The model provides control objectives that guide the high-level design and implementation of a comprehensive information security management system (ISMS).
- The chapter also discussed how security professionals use controls to identify the technologies, devices, and products to protect the organization.
- If you would like to further explore the concepts in this chapter, please check out the Additional Resources and Activities page in Student Resources.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials
Chapter 3: Malware and Malicious Code

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 3:
Malware and Malicious Code

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 3 - Sections & Objectives

3.1 Malware and Malicious Code

Differentiate the types of malware and malicious code.

3.2 Trickery

Describe the tactics, techniques and procedures used by cyber criminals.

3.3 Attacks

Compare the different methods used in social engineering.

Compare different types of cyberattacks.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

3.1 Malware and Malicious Code

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Malware

Cyber criminals target user's end devices through the installation of malware.

Viruses - A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.

Worms - Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Malware (Cont.)

- **Logic Bomb** - A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens. Once activated, a logic bomb implements a malicious code that causes harm to a computer.

- **Ransomware** - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually works by encrypting data in the computer with a key unknown to the user.

- **Backdoors and Rootkits** - A backdoor or rootkit refers to the program or code introduced by a criminal who has compromised a system. The backdoor bypasses the normal authentication used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.

© 2008 Cisco Systems, Inc. All rights reserved.

Email and Browser Attacks (Cont.)

Email is a universal service used by billions worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Spam - Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

Spyware - Spyware is software that enables a criminal to obtain information about a user's computer activities. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Email and Browser Attacks (Cont.)

Adware - Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware - Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Email and Browser Attacks (Cont.)

Phishing - Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials or account information by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing - Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Email and Browser Attacks (Cont.)

Vishing - Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate.

Pharming - Pharming is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.

Whaling - Whaling is a phishing attack that targets high profile targets within an organization such as senior executives.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Email and Browser Attacks (Cont.)

Plugins - The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.

SEO Poisoning - Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a malicious website appear higher in search results.

Browser Hijacker - A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

3.2 Trickery

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Art of Trickery

Social Engineering - Social engineering is a completely non-technical means for a criminal to gather information on a target. Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information.

Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. These are some types of social engineering attacks:

Pretexting - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Something for Something (Quid pro quo) - This is when an attacker requests personal information from a party in exchange for something, like a gift.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Trickery

Shoulder Surfing and Dumpster Diving – refers to picking up PINs, access codes or credit card numbers. An attacker can be in close proximity to his victim or the attacker can use binoculars or closed circuit cameras to shoulder surf.

Impersonation and Hoaxes - Impersonation is the action of pretending to be someone else. For example, a recent phone scam targeted taxpayers. A criminal, posing as an IRS employee, told the victims that they owed money to the IRS.

Piggybacking and Tailgating - Piggybacking occurs when a criminal tags along with an authorized person to gain entry into a secure location or a restricted area. Tailgating is another term that describes the same practice.

Online, Email, and Web-based Trickery - Forwarding hoax emails and other jokes, funny movies, and non-work-related emails at work may violate the company's acceptable use policy and result in disciplinary actions.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

3.3 Attacks

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Cyber Attacks

Denial-of-Service (DoS) Attacks - are a type of network attack. A DoS attack results in some sort of interruption of network services to users, devices, or applications. DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

Sniffing - Sniffing is similar to eavesdropping on someone. It occurs when attackers examine all network traffic as it passes through their NIC, independent of whether or not the traffic is addressed to them or not. Criminals accomplish network sniffing with a software application, hardware device, or a combination of the two.

Spoofing - Spoofing is an impersonation attack, and it takes advantage of a trusted relationship between two systems. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Cyber Attacks

Man-in-the-middle - A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user's knowledge.

Zero-Day Attacks - A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor. The term zero hour describes the moment when someone discovers the exploit.

Keyboard Logging - Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wireless and Mobile Attacks (Cont.)

Grayware and SMiShing

- Grayware includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user. Grayware is becoming a problem area in mobile security with the popularity of smartphones.
- SMiShing is short for SMS phishing. It uses Short Message Service (SMS) to send fake text messages. The criminals trick the user into visiting a website or calling a phone number. Unsuspecting victims may then provide sensitive information such as credit card information. Visiting a website might result in the user unknowingly downloading malware that infects the device.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wireless and Mobile Attacks (Cont.)

Rogue Access Points - A rogue access point is a wireless access point installed on a secure network without explicit authorization. A rogue access point can be set up in two ways.

RF Jamming - Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

Bluejacking and Bluesnarfing - Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wireless and Mobile Attacks (Cont.)

WEP and WPA Attacks

Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network (WLAN) with the same level of security as a wired LAN. Since physical security measures help to protect a wired LAN, WEP seeks to provide similar protection for data transmitted over the WLAN with encryption.

- WEP uses a key for encryption.
- There is no provision for key management with WEP, so the number of people sharing the key will continually grow.

Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by observing traffic.

- WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and a legitimate user.
- Cyber criminals use a packet sniffer and then run attacks offline on the passphrase.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Wireless and Mobile Attacks (Cont.)

Defending Against Wireless and Mobile Device Attacks

There are several steps to take to defend against wireless and mobile device attacks.

- Most WLAN products use default settings. Take advantage of the basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement with the network by placing these devices outside the firewall or within a demilitarized zone (DMZ) which contains other untrusted devices such as email and web servers.
- WLAN tools such as NetStumbler may discover rogue access points or unauthorized workstations. Develop a guest policy to address the need when legitimate guests need to connect to the Internet while visiting. For authorized employees, utilize a remote access virtual private network (VPN) for WLAN access.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Application Attacks

Cross-site scripting (XSS) - is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code. Cross-site scripting has three participants: the criminal, the victim, and the website. The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application. Criminals inject client-side scripts into web pages viewed by users, the victims.

Code Injections Attacks - One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

Buffer Overflow - A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Application Attacks

Remote Code Executions vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

ActiveX Controls and Java controls provide the capability of a plugin to Internet Explorer.

- ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program's functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Application Attacks

Defending Against Application Attacks

- The first line of defense against an application attack is to write solid code.
- Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile.
- Validate all inputs as if they were hostile.
- Keep all software including operating systems and applications up to date, and do not ignore update prompts.
- Not all programs update automatically, so at the very least, always select the manual update option.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

3.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

Threats, vulnerabilities, and attacks are the central focus of the cybersecurity wizards.

- This chapter discussed the various cybersecurity attacks that cyber criminals launch.
- The chapter explained the threat of malware and malicious code.
- The chapter discussed the types of trickery involved with social engineering. Maneuvering explained the types of attacks that both wired and wireless networks experience.
- Finally, the chapter discussed the vulnerabilities presented by application attacks.

Understanding the types of possible threats allows an organization to identify the vulnerabilities that make it a target. The organization can then learn how to defend itself against cybersecurity trickery and maneuvering.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials Chapter 4: The Art of Protecting Secrets

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 4:
The Art of Protecting Secrets

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 4 - Sections & Objectives

4.1 Cryptography

Explain how encryption techniques protect confidentiality.

4.2 Access Control

Describe access control techniques used to protect confidentiality.

4.3 Obscuring Data

Describe the concept of obscuring data.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

4.1 Cryptography

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cryptography
Overview

Cryptology is the science of making and breaking secret codes. Cryptography is a way to store and transmit data so only the intended recipient can read or process it. Modern cryptography uses computationally secure algorithms to make sure that cyber criminals cannot easily compromise protected information.

The history of cryptography started in diplomatic circles thousands of years ago. Messengers from a king's court took encrypted messages to other courts. Occasionally, other courts not involved in the communication, attempted to steal messages sent to a kingdom they considered an adversary. Not long after, military commanders started using encryption to secure messages.

Each encryption method uses a specific algorithm, called a cipher, to encrypt and decrypt messages. A cipher is a series of well-defined steps used to encrypt and decrypt messages. There are several methods of creating ciphertext:

- Transposition
- Substitution
- One-time pad

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Overview (Cont.)

Two Types of Encryption

There are two classes of encryption algorithms:

- **Symmetric algorithms** - These algorithms use the same pre-shared key, sometimes called a secret key pair, to encrypt and decrypt data. Both the sender and receiver know the pre-shared key before any encrypted communication begins.
- **Asymmetric algorithms** - Asymmetrical encryption algorithms use one key to encrypt data and a different key to decrypt data. One key is public and the other is private. In a public-key encryption system, any person can encrypt a message using the public key of the receiver, and the receiver is the only one that can decrypt it using his private key. Parties exchange secure messages without needing a pre-shared key. Asymmetric algorithms are more complex. These algorithms are resource intensive and slower to execute.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Private-Key Encryption

Symmetrical Encryption Process - Symmetric algorithms use pre-shared key to encrypt and decrypt data, a method also known as private-key encryption. Numerous encryption systems use symmetric encryption. Some of the common encryption standards that use symmetric encryption include the following:

- **3DES (Triple DES):** Digital Encryption Standard (DES) is a symmetric block cipher with 64-bit block size that uses a 56-bit key. Triple DES encrypts data three times and uses a different key for at least one of the three passes, giving it a cumulative key size of 112-168 bits.
- **IDEA:** The International Data Encryption Algorithm (IDEA) uses 64-bit blocks and 128-bit keys. IDEA performs eight rounds of transformations on each of the 16 blocks that results from dividing each 64-bit block. IDEA was the replacement for DES, and now PGP (Pretty Good Privacy) uses it.
- **AES:** The Advanced Encryption Standard (AES) has a fixed block size of 128-bits with a key size of 128, 192, or 256 bits. The National Institute of Standards and Technology (NIST) approved the AES algorithm in December 2001. The U.S. government uses AES to protect classified information.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Public-Key Encryption

Asymmetrical Encryption Process - Asymmetric encryption, also called public-key encryption, uses one key for encryption that is different from the key used for decryption. A criminal cannot calculate the decryption key based on knowledge of the encryption key, and vice versa, in any reasonable amount of time. The asymmetric algorithms include:

- **RSA (Rivest_Shamir-Adleman)** - uses the product of two very large prime numbers with an equal length of between 100 and 200 digits. Browsers use RSA to establish a secure connection.
- **Diffie-Hellman** - provides an electronic exchange method to share the secret key. Secure protocols, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), Secure Shell (SSH), and Internet Protocol Security (IPsec), use Diffie-Hellman.
- **ElGamal** - uses the U.S. government standard for digital signatures. This algorithm is free to use because no one holds the patent.
- **Elliptic Curve Cryptography (ECC)** - uses elliptic curves as part of the algorithm. In the U.S., the National Security Agency uses ECC for digital signature generation and key exchange.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Symmetrical versus Asymmetrical Encryption

Comparing Encryption Types

- It is important to understand the differences between symmetric and asymmetric encryption methods. Symmetric encryption systems are more efficient and can handle more data. However, key management with symmetric encryption systems is more problematic and harder to manage.
- Asymmetric cryptography is more efficient at protecting the confidentiality of small amounts of data, and its size and speed make it more secure for tasks such as electronic key exchange which is a small amount of data rather than encrypting large blocks of data.

© 2008 Cisco Systems, Inc. All rights reserved.

Symmetrical versus Asymmetrical Encryption

Application

There are many applications for both symmetric and asymmetric algorithms. A one-time password-generating token is a hardware device that uses cryptography to generate a one-time password. A one-time password is an automatically generated numeric or alphanumeric string of characters that authenticates a user for one transaction of one session only. The number changes every 30 seconds or so. The session password appears on a display and the user enters the password.

- The electronic payment industry uses 3DES.
- Operating systems use DES to protect user files and system data with passwords.
- Most encrypting file systems, such as NTFS, use AES.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Symmetrical versus Asymmetrical Encryption

Application

Four protocols use asymmetric key algorithms:

- Internet Key Exchange (IKE), which is a fundamental component of IPsec Virtual Private Networks (VPNs).
- Secure Socket Layer (SSL), which is a means of implementing cryptography into a web browser.
- Secure Shell (SSH), which is a protocol that provides a secure remote access connection to network devices.
- Pretty Good Privacy (PGP), which is a computer program that provides cryptographic privacy and authentication to increase the security of email communications.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Symmetrical versus Asymmetrical Encryption

Application

A VPN is a private network that uses a public network, usually the Internet, to create a secure communication channel. A VPN connects two endpoints such as two remote offices over the Internet to form the connection.

- VPNs use IPsec. IPsec is a suite of protocols developed to achieve secure services over networks.
- IPsec services allow for authentication, integrity, access control, and confidentiality.
- With IPsec, remote sites can exchange encrypted and verified information.
- Data in use is a growing concern to many organizations. When in use, data no longer has any protection because the user needs to open and change the data.
- System memory holds data in use and it can contain sensitive data such as the encryption key.
- If criminals compromise data in use, they will have access to data at rest and data in motion.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

4.2 Access Control

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Access Control

Physical Access Controls - actual barriers deployed to prevent direct contact with systems. The goal is to prevent unauthorized users from gaining physical access to facilities, equipment, and other organizational assets. Physical access control determines who can enter (or exit), where they can enter (or exit), and when they can enter (or exit).

Logical Access Controls - hardware and software solutions used to manage access to resources and systems. These technology-based solutions include tools and protocols that computer systems use for identification, authentication, authorization, and accountability.

Administrative Access Controls - policies and procedures defined by organizations to implement and enforce all aspects of controlling unauthorized access. Administrative controls focus on personnel and business practices.

© 2008 Cisco Systems, Inc. All rights reserved.

Access Control Strategies

Mandatory access control (MAC) - restricts the actions that a subject can perform on an object. A subject can be a user or a process. An object can be a file, a port, or an input/output device. An authorization rule enforces whether or not a subject can access the object.

Discretionary access control (DAC) - DAC grants or restricts object access determined by the object's owner. As the name implies, controls are discretionary because an object owner with certain access permissions can pass on those permissions to another subject.

Role-based access control (RBAC) - is based on the role of the subject. Roles are job functions within an organization. Specific roles require permissions to perform certain operations. Users acquire permissions through their role. RBAC can work in combination with DAC or MAC by enforcing the policies of either one.

Rule-based access control - uses access control lists (ACLs) to help determine whether to grant access. A series of rules is contained in the ACL, as shown in the figure. The determination of whether to grant access depends on these rules. An example of such a rule is one that states that no employee may have access to the payroll file after hours or on weekends.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Identification

Identification enforces the rules established by the authorization policy:

- A subject requests access to a system resource.
- Every time the subject requests access to a resource, the access controls determine whether to grant or deny access.
- Cybersecurity policies determine which identification controls should be used.
- The sensitivity of the information and information systems determine how stringent the controls.
- The increase in data breaches has forced many organizations to strengthen their identification controls.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Authentication Methods

What You Know - Passwords, passphrases, or PINs are all examples of something that the user knows. Passwords are the most popular method used for authentication.

What You Have - Smart cards and security key fobs are both examples of something that users have in their possession.

Who You Are - A unique physical characteristic, such as a fingerprint, retina, or voice, that identifies a specific user is called biometrics.

Multi-factor Authentication - Multi-factor authentication uses at least two methods of verification. A security key fob is a good example. The two factors are something you know, such as a password, and something you have, such as a security key fob.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Authorization

Authorization controls what a user can and cannot do on the network after successful authentication:

- After a user proves his or her identity, the system checks to see what network resources the user can access and what the users can do with the resources.
- Authorization uses a set of attributes that describes the user's access to the network.
- The system compares these attributes to the information contained within the authentication database, determines a set of restrictions for that user, and delivers it to the local router where the user is connected.
- Defining authorization rules is the first step in controlling access. An authorization policy establishes these rules.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Accountability

Accountability traces an action back to a person or process making the change to a system, collects this information, and reports the usage data:

- The organization can use this data for such purposes as auditing or billing.
- The collected data might include the log in time for a user, whether the user log in was a success or failure, or what network resources the user accessed.
- This allows an organization to trace actions, errors, and mistakes during an audit or investigation.
- Implementing accountability consists of technologies, policies, procedures, and education.
- Log files provide detailed information based on the parameters chosen.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Security Controls

Preventative Controls - Prevent means to keep something from happening. Preventative access controls stop unwanted or unauthorized activity from happening.

Deterrent Controls - A deterrent is the opposite of a reward. A reward encourages individuals to do the right thing, while a deterrent discourages them from doing the wrong thing. Cybersecurity professionals and organizations use deterrents to limit or mitigate an action or behavior. Deterrents do not always stop these actions.

Detective Controls - Detection is the act or process of noticing or discovering something. Access control detections identify different types of unauthorized activity. Detection systems can be very simple, such as a motion detector or security guard. They can also be more complex, such as an intrusion detection system.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Security Controls

Corrective Controls - Corrective counteracts something that is undesirable. Organizations put corrective access controls in place after a system experiences a threat. Corrective controls restore the system back to a state of confidentiality, integrity, and availability. They can also restore systems to normal after unauthorized activity occurs.

Recovery Controls - Recovery is a return to a normal state. Recovery access controls restore resources, functions, and capabilities after a violation of a security policy. Recovery controls can repair damage, in addition to stopping any further damage. These controls have more advanced capabilities over corrective access controls.

Compensative Controls - Compensate means to make up for something. Compensative access controls provide options to other controls to bolster enforcement in support of a security policy. A compensative control can also be a substitution used in place of a control that is not possible under the circumstances.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

4.3 Obscuring Data

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data Masking

Data Masking is a technology that secures data by replacing sensitive information with a non-sensitive version. The non-sensitive version looks and acts like the original. This means that a business process can use non-sensitive data and there is no need to change the supporting applications or data storage facilities.

In the most common use case, masking limits the propagation of sensitive data within IT systems by distributing surrogate data sets for testing and analysis.

There are data masking techniques that can ensure that data remains meaningful but changed enough to protect it:

- **Substitution** - replaces data with authentic looking values to apply anonymity to the data records.
- **Shuffling** - derives a substitution set from the same column of data that a user wants to mask. This technique works well for financial information in a test database, for example.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Steganography

Steganography conceals data (the message) in another file such as a graphic, audio, or other text file.

The advantage of steganography over cryptography is that the secret message does not attract any special attention. No one would ever know that a picture actually contained a secret message by viewing the file either electronically or in hardcopy.

There are several components involved in hiding data:

- There is the embedded data, which is the secret message.
- Cover-text (or cover-image or cover-audio) hides the embedded data producing the stego-text (or stego-image or stego-audio).
- A stego-key controls the hiding process.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Data Obfuscation

Data obfuscation - is the use and practice of data masking and steganography techniques in the cybersecurity and cyber intelligence profession:

- Obfuscation is the art of making the message confusing, ambiguous, or harder to understand.
- A system may purposely scramble messages to prevent unauthorized access to sensitive information.
- Software watermarking protects software from unauthorized access or modification.
- Software watermarking inserts a secret message into the program as proof of ownership.
- The secret message is the software watermark. If someone tries to remove the watermark, the result is nonfunctional code.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

4.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter Summary

Summary

- This chapter discussed the principles of cryptology used to secure communications.
- The chapter explained both symmetric and asymmetric encryption algorithms, compared the two algorithms, and provided examples of their use.
- The chapter explained how access control prevents unauthorized access to a building, a room, a system, or a file using identification, authentication, authorization, and accountability. In addition, the chapter also described the different access control models and access control types.
- The chapter concluded by discussing the various ways users mask data. Data obfuscation and steganography are two techniques used to accomplish data masking.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials Chapter 5: The Art of Ensuring Integrity

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 5:
The Art of Ensuring Integrity

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 5 - Sections & Objectives

5.1 Types of Data Integrity Controls

Explain the processes used to ensure integrity.

5.2 Digital Signatures

Explain the purpose of digital signatures.

5.3 Certificates

Explain the purpose of digital certificates.

5.4 Database Integrity Enforcement

Explain the need for database integrity enforcement.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.1 Types of Data Integrity Controls

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Hashing Algorithms

- Hashing is a tool that ensures data integrity by taking binary data (the message) and producing a fixed-length representation called the hash value or message digest.
- Hashing is a one-way mathematical function that is relatively easy to compute, but significantly harder to reverse. Grinding coffee beans is a good analogy of a one-way function. It is easy to grind coffee beans, but it is almost impossible to put all of the tiny pieces back together to rebuild the original beans.

  A cryptographic hash function has the following properties:

  - The input can be any length.
  - The output has a fixed length.
  - The hash function is one way and is not reversible.
  - Two different input values will always result in different hash values.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Hashing Algorithms

There are many modern hashing algorithms widely used today. Two of the most popular are MD5 and SHA.

- **Message Digest 5 (MD5) Algorithm -** is a hash algorithm developed by Ron Rivest that produces a 128-bit hash value.
- **Secure Hash Algorithm (SHA) –** was developed by the U.S. National Institute of Standards and Technology (NIST) and can be implemented in different strengths:
- SHA-224 (224 bit)
- SHA-256 (256 bit)
- SHA-384 (384 bit)
- SHA-512 (512 bit)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Salting

- Salting is used to make hashing more secure. If two users have the same password, they will also have the same password hashes. A salt, which is a random string of characters, is an additional input to the password before hashing.
- This creates a different hash result for the two passwords as shown in the figure. A database stores both the hash and the salt.

		Salt		Hash Value
Hash ("password"	+	QxLUF1bIAdeQX)	=	b3bad1e5324f057753a4b8d7cef293e4
Hash ("password"	+	R9PeIC7sxQXb8)	=	713c7beb54841a26a7c81eb06d6cf066

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of Data Integrity Controls

HMAC

- HMACs strengthens hashing algorithms by using an additional secret key as input to the hash function.
- The use of HMAC goes a step further than just integrity assurance by adding authentication.
- An HMAC uses a specific algorithm that combines a cryptographic hash function with a secret key, as shown in the figure.

The same procedure is used for generation and verification of secure fingerprints.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.2 Digital Signatures

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Signatures and the Law

- Digital signatures provide the same functionality as handwritten signatures for electronic documents.
- A digital signature is used to determine if someone edits a document after the user signs it.
- A digital signature is a mathematical method used to check the authenticity and integrity of a message, digital document, or software.
- In many countries, digital signatures have the same legal importance as a manually signed document.
- Digital signatures also provide repudiation.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

How Digital Signature Technology Works

Asymmetric cryptography is the basis for digital signatures. A public key algorithm like RSA generates two keys: one private and the other public. The keys are mathematically related.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.3 Certificates

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Basics of Digital Certicates

- A digital certificate is equivalent to an electronic passport.
- Digital certificates enable users, hosts, and organizations to exchange information securely over the Internet.
- A digital certificate authenticates and verifies that users sending a message are who they claim to be.
- Digital certificates can also provide confidentiality for the receiver with the means to encrypt a reply.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Constructing a Digital Certificate

- Digital certificate must follow a standard structure so that any entity can read and understand it regardless of the issuer.
- TheX.509 is the standard for construction of digital certificates and the public key infrastructure (PKI) used to manage digital certificates.
- PKI is the policies, roles, and procedures required to create, manage, distribute, use, store, and revoke digital certificates.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.4 Database Integrity Enforcement

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity

- Databases provide an efficient way to store, retrieve, and analyze data.
- As data collection increases and data becomes more sensitive, it is important for cybersecurity professionals to protect the growing number of databases.
- Data integrity refers to the accuracy, consistency, and reliability of data stored in a database.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity (Cont.)

The four database integrity rules or constraints are as follows:

- **Entity Integrity**: All rows must have a unique identifier called a Primary Key.
- **Domain Integrity**: All data stored in a column must follow the same format and definition.
- **Referential Integrity**: Table relationships must remain consistent. Therefore, a user cannot delete a record which is related to another one.
- **User-defined Integrity**: A set of rules defined by a user which does not belong to one of the other categories. For example, a customer places a new order. The user first checks to see if this is a new customer. If it is, the user adds the new customer to the customers table.

ID	Company	First Name	Last Name
8	Company H	Elizabeth	Andersen
18	Company R	Catherine	Autier Miconi
3	Company C	Thomas	Axen
17	Company Q	Jean Philippe	Bagel
1	Company A	Anna	Bedecs
12	Company L	John	Edwards

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity Enforcement

Database Validation

A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy and consistency of data. The criteria used in a validation rule include the following:

- Size – checks the number of characters in a data item
- Format – checks that the data conforms to a specified format
- Consistency – checks for the consistency of codes in related data items
- Range – checks that data lies within a minimum and maximum value
- Check digit – provides for an extra calculation to generate a check digit for error detection.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity Enforcement

Database Integrity Requirements

- Maintaining proper filing is critical in maintaining the trustworthiness and usefulness of the data within the database.
- Tables, records, fields, and data within each field make up a database.
- In order to maintain the integrity of the database filing system, users must follow certain rules.
- Entity integrity is an integrity rule, which states that every table must have a primary key and that the column or columns chosen to be the primary key must be unique and not NULL.
- Null in a database signifies missing or unknown values. Entity integrity enables proper organization of data for that record.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity Requirements (Cont.)

Table One - Inventory

Part ID	Quantity	Cost	Description
0102003	1232	$5.50	Light Gray w/
0122023	2234	$2.32	Bright LED
0132001	556	$8.23	Lab burner w/

Primary Key

Table Two - Customers

LName	Account#	Email	Item Ordered
Smith	0090-0909	Smithj23@yah	0102003
Jones	0090-0569	Bill.Jones@gm	0203883
Johnson	0090-0789	Johnsonj@ex	0132001

Foreign Key

- Another important integrity check is referential integrity which deals with foreign keys. A foreign key in one table references a primary key in a second table. The primary key for a table uniquely identifies entities (rows) in the table. Referential integrity maintains the integrity of foreign keys.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Database Integrity Requirements (Cont.)

SSN 243-27-3361	• Must have nine integers • Format xxx-xx-xxxx • Entered or modified by customer only • Must be validated
Credit Card Number 4539 4769 0728 4479	• Must have sixteen integers • Format xxxx-xxxx-xxxx-xxxx • Entered or modified by customer only • Must be validated
Email Address tortor@odio.com	• Must have no more that 128 characters • Format xxxx@xxxx.xxx • Entered or modified by customer only • Validated by email response

- Domain integrity ensures that all the data items in a column fall within a defined set of valid values. Each column in a table has a defined set of values, such as the set of all numbers for credit card numbers, social security numbers, or email addresses. Limiting the value assigned to an instance of that column (an attribute) enforces domain integrity. Domain integrity enforcement can be as simple as choosing the correct data type, length and or format for a column.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

5.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

- Chapter five presented the art of integrity which is used to ensure that data remains unchanged by anyone or anything over its entire life cycle.
- The chapter introduced types of data integrity controls including:
  - hashing algorithms
  - password salting
  - keyed-hash message authentication code (HMAC)
- These tools provide a way for cybersecurity specialists to verify the authenticity of messages and documents.
- The chapter concluded with a discussion of database integrity enforcement.
- Having a well-controlled and well-defined data integrity system increases the stability, performance, and maintainability of a database system.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials
Chapter 6: The Realm of Five Nines

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 6:
The Realm of Five Nines

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 6 - Sections & Objectives

6.1 High Availability

Explain the concept of high availability.

6.2 Measures to Improve Availability

Explain how high availability measures are used to improve availability.

6.3 Incident Response

Describe how an incident response plan improves high availability.

6.4 Disaster Recovery

Describe how disaster recovery planning plays an important role in implementing high availability.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.1 High Availability

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Five Nines

What is Five Nine?

- Five nines mean that systems and services are available 99.999% of the time. It also means that both planned and unplanned downtime is less than 5.26 minutes per year. High availability refers to a system or component that is continuously operational for a given length of time. To help ensure high availability:
- Eliminate single points of failure
- Design for reliability
- Detect failures as they occur

Availability	Downtime per Year
99%	87 hours 36 mins
99.5%	43 hours 48 mins
99.95%	4 hours 23 mins
99.99%	53 mins
99.999%	5 mins

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

The Five Nines (Cont.)

Environments That Require Five Nines

Although the cost of sustaining high availability may be too costly for some industries, several environments require five nines.

- The finance industry needs to main high availability for continuous trading, compliance, and customer trust.
- Healthcare facilities require high availability to provide around-the-clock care for patients.
- The public safety industry includes agencies that provide security and services to a community, state, or nation.
- The retail industry depends on efficient supply chains and the delivery of products to customers. Disruption can be devastating, especially during peak demand times such as holidays.

Finance Industry

Health Care Facilities

Public Safety

© 2008 Cisco Systems, Inc. All rights reserved.

The Five Nines (Cont.)

Threats to Availability

There are many different types of threats to high availability, the threats can range from failure of a mission-critical application to severe storm such as a hurricane or tornado. Threats can also include catastrophic event such as a terrorist attack, building bombing, or building fires.

Designing a High Availability System

High availability incorporates three major principles to achieve the goal of uninterrupted access to data and services:

- Elimination or reduction of single-points of failure
- System Resiliency
- Fault Tolerance

Finance Industry

Health Care Facilities

Public Safety

© 2008 Cisco Systems, Inc. All rights reserved.

2.2 Measures to Improve Availability

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Asset Management

An organization needs to know what hardware and software assets they have in order to protect them. Asset management includes a complete inventory of hardware and software. This means that the organization needs to know all of components that can be subject to security risks, including:

- Every hardware system
- Every operating system
- Every hardware network device
- Every network device operating system
- Every software application
- All firmware
- All language runtime environments
- All individual libraries

Many organizations may choose an automated solution to keep track of assets.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Asset Management (Cont.)

- **Asset classification -** assigns all resources of an organization into a group based on common characteristics. An organization should apply an asset classification system to documents, data records, data files, and disks.
- **Asset Standardization -** as part of an IT asset management system, an organization specifies the acceptable IT assets that meet its objectives
- **Threat Identification -** The United States Computer Emergency Readiness Team (US-CERT) and the U.S. Department of Homeland Security sponsor a dictionary of common vulnerabilities and exposure (CVE). The CVE identification contains a standard identifier number with a brief description, and references to related vulnerability reports and advisories.
- **Risk Analysis -** is the process of analyzing the dangers posed by natural and human-caused events to the assets of an organization. A user performs an asset identification to help determine which assets to protect.
- **Mitigation -** Mitigation involves reducing the severity of the loss or the likelihood of the loss from occurring. Many technical controls mitigate risk including authentication systems, file permissions, and firewalls.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Defense in Depth

Defense in depth will not provide an impenetrable cyber shield, but it will help an organization minimize risk by keeping it one step ahead of cyber criminals. To make sure data and information remains available, an organization must create different layers of protection:

- A **layered** approach provides the most comprehensive protection. If cyber criminals penetrate one layer, they still have to contend with several more layers with each layer being more complicated than the previous one. Layering is creating a barrier of multiple defenses that coordinate together to prevent attacks.
- **Limiting** access to data and information reduces the possibility of a threat. An organization should restrict access so that users only have the level of access required to do their job.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Defense in Depth

- **Diversity** refers to changing the controls and procedures at different layers. Breaching one layer of security does not compromise the whole system. An organization may use different encryption algorithms or authentication systems to protect data in different states.
- **Obscuring** information can also protect data and information. An organization should not reveal any information that cyber criminals can use to figure out what version of the operating system a server is running or the type of equipment it uses.
- Complexity does not necessarily guarantee security. If the process or technology are too complex, misconfigurations or failure to comply can result. **Simplicity** can actually improve availability.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy

A **single point of failure** must be identified and addressed. A single point of failure can be a specific piece of hardware, a process, a specific piece of data, or even an essential utility.

- Single points of failure are the weak links in the chain that can cause disruption of the organization's operations.
- Generally, the solution to a single point of failure is to modify the critical operation so that it does not rely on a single element.
- The organization can also build redundant components into the critical operation to take over the process should one of these points fail.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

- **N+1 redundancy** ensures system availability in the event of a component failure.
- Components (N) need to have at least one backup component (+1).
- For example, a car has four tires (N) and a spare tire in the trunk in case of a flat (+1).

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

- A **redundant array of independent disks (RAID)** combines multiple physical hard drives into a single logical unit to provide data redundancy and improve performance.
- RAID takes data that is normally stored on a single disk and spreads it out among several drives. If any single disk is lost, the user can recover data from the other disks where the data also resides.
- RAID can also increase the speed of data recovery.
- Using multiple drives makes retrieving requested data faster, instead of relying on just one disk to do the work.
- A RAID solution can be either hardware-based or software-based. The following terms describe how RAID stores data on the various disks:
  - **Parity** - Detects data errors.
  - **Striping** - Writes data across multiple drives.
  - **Mirroring** - Stores duplicate data on a second drive.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

Spanning Tree is a network protocol that provides for redundancy:

- The basic function of STP is to prevent loops on a network when switches interconnect via multiple paths.
- STP ensures that redundant physical links are loop-free. It ensures that there is only one logical path between all destinations on the network.
- STP intentionally blocks redundant paths that could cause a loop.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

The default gateway is typically the router that provides devices access to the rest of the network or to the Internet. If there is only one router serving as the default gateway, it is a single point of failure. Router redundancy involves:

- Choosing to install an additional standby router.
- The ability of a network to dynamically recover from the failure of a router acting as a default gateway is known as first-hop redundancy.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

Router Redundancy Options - options available for router redundancy include:

- **Hot Standby Router Protocol (HSRP)** - HSRP provides high network availability by providing first-hop routing redundancy.
- **Virtual Router Redundancy Protocol (VRRP)** - A VRRP router runs the VRRP protocol in conjunction with one or more other routers attached to a LAN. In a VRRP configuration, the elected router is the virtual router master, and the other routers act as backups, in case the virtual router master fails.
- **Gateway Load Balancing Protocol (GLBP)** - GLBP protects data traffic from a failed router or circuit, like HSRP and VRRP, while also allowing load balancing (also called load sharing) between a group of redundant routers.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Redundancy (Cont.)

Location Redundancy - An organization may need to consider location redundancy depending on its needs. The following outlines three forms of location redundancy:

- **Synchronous -** Synchronizes both locations in real time, requires high bandwidth and locations must be close together to reduce latency.
- **Asynchronous Replication -** Not synchronized in real time but close to it, requires less bandwidth and sites can be further apart because latency is less of an issue.
- **Point-in-time-Replicatio**n - Updates the backup data location periodically and is the most bandwidth conservative option because it does not require a constant connection.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

System Resilience

Resiliency defines the methods and configurations used to make a system or network tolerant of failure. Routing protocols provide resiliency. Resilient design is more than just adding redundancy. Resiliency is critical to understand the business needs of the organization, and then incorporate redundancy to create a resilient network.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

6.3 Incident Response Phases

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Incident Response Phases

Incident response defines the procedures that an organization follows after an event occurs outside the normal range. When an incident occurs, the organization must know how to respond. Organizations needs to develop an incident response plan and put together a Computer Security Incident Response Team (CSIRT) to manage the response. Incident response has consist of four phases:

1. **Preparation** – planning for potential incidents
2. **Detection and Analysis** - discovering the incident
3. **Containment and Eradication, and Recovery** - efforts to immediately contain or eradicate the threat and begin recovery efforts
4. **Post-Incident Follow-Up** – investigate the cause of the incident and ask questions to better understand the nature of the threat

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Incident Response Technologies

There are many technologies that are used to implement an incident response:

- **Network Admission Control (NAC)** - allows network access for authorized users with compliant systems. A compliant system meets all of the policy requirements of the organization.
- **Intrusion Detection Systems (IDSs)** - monitor the traffic on a network. IDS systems are passive.
- **Intrusion Prevention Systems** - operates in inline mode. It can detect and immediately address a network problem.
- **NetFlow and IPFIX** - NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a Cisco router or multilayer switch. The Internet Engineering Task Force (IETF) used Cisco's NetFlow Version 9 as the basis for IP Flow Information Export (IPFIX).
- **Advanced Threat Intelligence** - can help organizations detect attacks during one of the stages of the cyberattack (and sometimes before with the right information).

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

2.4 Disaster Recovery

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Disaster Recovery Planning

Types of Disasters - It is critical to keep an organization functioning when a disaster occurs. A disaster includes any natural or human-caused event that damages assets or property and impairs the ability for the organization to continue operating.

- **Natural Disasters -** geological disasters (earthquakes, landslides, volcanoes, and tsunamis), meteorological disasters (hurricanes, tornadoes, snow storms, lightning, and hail), health disasters (widespread illnesses, quarantines, and pandemics) and miscellaneous disasters (fires, floods, solar storms, and avalanches).
- **Human-caused Disasters -** Human-caused disasters - labor events (strikes, walkouts, and slowdowns), social-political events (vandalism, blockades, protests, sabotage, terrorism, and war), materials events (hazardous spills and fires) and utilities disruptions (power failures, communication outages, fuel shortages, and radioactive fallout)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Business Continuity Planning

Need for Business Continuity - Business continuity is one of the most important concepts in computer security. Even though companies do whatever they can to prevent disasters and loss of data, it is impossible to predict every scenario. It is important for companies to have plans in place that ensure business continuity regardless of what may occur.

Business Continuity Considerations - Business continuity controls are more than just backing up data and providing redundant hardware. Business Continuity Considerations should include:

- Documenting configurations
- Establishing alternate communications channels
- Providing power
- Identifying all dependencies for applications and processes
- Understanding how to carry out automated tasks manually

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Business Continuity Planning

Business Continuity Best Practices

1. Write a policy that provides guidance to develop the business continuity plan and assigns roles to carry out the tasks.
2. Identify critical systems and processes, and prioritize them based on necessity.
3. Identify vulnerabilities, threats, and calculate risks.
4. Identify and implement controls and countermeasures to reduce risk.
5. Devise methods to bring back critical systems quickly.
6. Write procedures to keep the organization functioning when in a chaotic state.
7. Test the plan.
8. Update the plan regularly.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

6.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

- This chapter began by explaining the concept of five nines, a high availability standard that allows for 5.26 minutes of downtime per year.
- The chapter discussed the various approaches that organizations take to ensure system availability.
- Solid system design includes accommodating measures that provide redundancy and resiliency so that an organization can recover quickly and continue operation.
- The chapter also discussed how an organization responds to an incident by establishing procedures that it follows after an event occurs.
- The chapter concluded with a discussion of disaster recovery and business continuity planning.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

Instructor Materials
Chapter 7: Fortifying the Kingdom

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 7:
Fortifying the Kingdom

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 7 - Sections & Objectives

7.1 Defending Systems and Devices

Describe how cybersecurity domains are used within the CIA triad.

Explain how technologies, processes and procedures protect systems.

7.2 Server Hardening

Explain how to protect servers on a network.

7.3 Network Hardening

Explain how to implement security measures to protect network devices.

7.4 Physical Security

Explain how physical security measures are implemented to protect network equipment.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

7.1 Defending Systems and Devices

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Host Hardening

Operating System Security - The operating system plays a critical role in the operation of a computer system and is the target of many attacks.

- An administrator hardens an operating system by modifying the default configuration to make it more secure to outside threats.
- This process includes the removal of unnecessary programs and services.
- Another critical requirement of hardening operating systems is the application of security patches and updates.

Antimalware - Malware includes viruses, worms, Trojan horses, keyloggers, spyware, and adware.

- They all invade privacy, steal information, damage the system, or delete and corrupt data.
- It is important to protect computers and mobile devices using reputable antimalware software.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Host Hardening (Cont.)

Patch Management - Patches are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack. Manufacturers combine patches and upgrades into a comprehensive update application called a service pack.

Host-based Firewalls - A software firewall is a program that runs on a computer to allow or deny traffic between the computer and other connected computers. The software firewall applies a set of rules to data transmissions through inspection and filtering of data packets.

Host Intrusion Detection Systems - A host intrusion detection system (HIDS) is software that runs on a host computer that monitors suspicious activity.

Secure Communications (VPNs) - When connecting to the local network and sharing files, the communication between computers remains within that network. To communicate and share resources over a network that is not secure, users employ a Virtual Private Network (VPN). A VPN is a private network that connects remote sites or users together over a public network, like the Internet.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Hardening Wireless and Mobile Devices

Wired Equivalent Privacy (WEP) - One of the most important components of modern computing are mobile devices. The majority of devices found on today's networks are laptops, tablets, smart phones and other wireless devices. WEP is one of the first widely used Wi-Fi security standards. The WEP standard provides authentication and encryption protections.

WPA/WPA2 - The next major improvement to wireless security was the introduction of WPA and WPA2. Wi-Fi Protected Access (WPA) was the computer industry's response to the weakness of the WEP standard. The WPA standard provided several security improvements.

Mutual Authentication - The imposter can launch a man-in-the-middle attack which is very difficult to detect and can result in stolen login credentials and transmitted data. To prevent rogue access points, the computer industry developed mutual authentication. Mutual authentication, also called two-way authentication, is a process or technology in which both entities in a communications link authenticate to each other.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Host Data Protection

File Access Control – This consists of permissions that limit folder or file access for an individual or for a group of users.

File Encryption – File encryption is a tool used to protect data stored in the form of files. Encryption transforms data using a complicated algorithm to make it unreadable. Software programs can encrypt files, folders, and even entire drives.

System and Data Backups - A data backup stores a copy of the information from a computer to removable backup media. Backing up data is one of the most effective ways of protecting against data loss. If the computer hardware fails, the user can restore the data from the backup after the system is again functional.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Images and Content Control

Content Screening and Blocking

Content control software restricts the content that a user can access with a web browser over the Internet.

Content control software can block sites that contain certain types of material such as pornography or controversial religious or political content.

Disk Cloning and Deep Freeze

- Many third-party applications are available to restore a system back to a default state. This allows the administrator to protect the operating system and configuration files for a system.
- Disk cloning copies the contents of the computer's hard disk to an image file.
- Deep Freeze "freezes" the hard drive partition. When a user restarts the system, the system reverts to its frozen configuration. The system does not save any changes that the user makes, so any applications installed or files saved are lost when the system restarts.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Physical Protection and Workstations

Security Cables and Locks - There are several methods of physically protecting computer equipment:

- Use cable locks
- Keep telecommunication rooms locked.
- Use security cages around equipment.

Logout Timers - An employee gets up and leaves his computer to take a break. If the employee does not take any action to secure his workstation, any information on that system is vulnerable to an unauthorized user.

Idle Timeout and Screen Lock - Employees may or may not log out of their computer when they leave the workplace. Therefore, it is a security best practice to configure an idle timer that will automatically log the user out and lock the screen.

Login Times - In some situations, an organization may want employees to log in during specific hours, such as 7 a.m. to 6 p.m. The system blocks logins during the hours that fall outside of the allowed login hours.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Physical Protection and Workstations

GPS Tracking – uses satellites and computers to determine the location of a device. GPS technology is a standard feature on smartphones that provides real-time position tracking. GPS tracking can pinpoint a location within 100 meters.

Inventory and RFID Tags - Radio frequency identification (RFID) uses radio waves to identify and track objects. RFID inventory systems use tags attached to all items that an organization wants to track.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

7.2 Server Hardening

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Secure Remote Access

Managing Remote Access - Remote access refers to any combination of hardware and software that enables users to access a local internal network remotely.

Telnet, SSH, and SCP - Secure Shell (SSH) is a protocol that provides a secure (encrypted) management connection to a remote device.

- **SSH** should replace Telnet for management connections.
- **Telnet** is an older protocol that uses unsecure plaintext transmission of both the login authentication (username and password) and the data transmitted between the communicating devices.
- **Secure copy (SCP)** securely transfers computer files between two remote systems. SCP uses SSH for data transfer (including the authentication element), so SCP ensures the authenticity and confidentiality of the data in transit.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Administrative Measures

Securing Ports and Services - Cyber criminals exploit the services running on a system because they know that most devices run more services or programs than they need. An administrator should look at every service to verify its necessity and evaluate its risk. Remove any unnecessary services.

Privileged Accounts - Cyber criminals exploit privileged accounts because they are the most powerful accounts in the organization. Privileged accounts have the credentials to gain access to systems and they provide elevated, unrestricted access. Administrators use these accounts to deploy and manage operating systems, applications, and network devices. These account should be secured or removed to mitigate these risks.

Group Policies - In most networks that use Windows computers, an administrator configures Active Directory with Domains on a Windows Server. An administrator configures user account policies such as password policies and lockout policies by adding users to groups and setting policy at a group level.

Enable Logs and Alerts - A log records events as they occur on a system. Log entries make up a log file, and a log entry contains all of the information related to a specific event. Logs that relate to computer security have grown in importance.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Physical Protection of Server

Power - A critical issue in protecting information systems is electrical power systems and power considerations. A continuous supply of electrical power is critical in today's massive server and data storage facilities.

Heating, Ventilation, and Air Conditioning (HVAC) - HVAC systems are critical to the safety of people and information systems in the organization's facilities. When designing modern IT facilities, these systems play a very important role in the overall security. HVAC systems control the ambient environment (temperature, humidity, airflow, and air filtering) and must be planned for and operated along with other data center components such as computing hardware, cabling, data storage, fire protection, physical security systems and power.

Hardware Monitoring - Hardware monitoring is often found in large server farms. A server farm is a facility that houses hundreds or thousands of servers for companies.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

7.3 Network Hardening

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Securing Network Devices

Operation Centers - The Network Operation Center (NOC) is one or more locations containing the tools that provide administrators with a detailed status of the organization's network. The NOC is ground zero for network troubleshooting, performance monitoring, software distribution and updates, communications management, and device management.

Switches, Routers, and Network Appliances - Network devices ship with either no passwords or default passwords.

- **Network switches** are the heart of the modern data communication network. The main threat to network switches are theft, hacking and remote access, attacks against network protocols like ARP/STP or attacks against performance and availability.
- **VLANs -** provide a way to group devices within a LAN and on individual switches. VLANs use logical connections instead of physical connections.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Securing Network Devices (Cont.)

- **Firewalls -** are hardware or software solutions that enforce network security policies. A firewall filters unauthorized or potentially dangerous traffic from entering the network.
- **Routers -** Routers form the backbone of the Internet and communications between different networks. Routers communicate with one another to identify the best possible path to deliver traffic to different networks. Routers use routing protocols to make routing decision.
- **Wireless and Mobile Devices** - Wireless and mobile devices have become the predominant type of devices on most modern networks. They provide mobility and convenience but pose a host of vulnerabilities. These vulnerabilities include theft, hacking and unauthorized remote access, sniffing, man-in-the-middle attacks, and attacks against performance and availability.
- **Network and Routing Services** - Cyber criminals use vulnerable network services to attack a device or to use it as part of the attack. Securing network services ensures that only necessary ports are exposed and available. Network services include; DHCP, DNS, ICMP, Routing Services (RIP-OSPF-ISS), NTP and others.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Voice and Video Equipment

VoIP Equipment - uses networks such as the Internet to make and receive phone calls. The equipment required for VoIP includes an Internet connection plus a phone.

Cameras - An Internet camera sends and receives data over a LAN and/or the Internet. A user can remotely view live video using a web browser on a wide range of devices including computer systems, laptops, tablets, and smartphones. Cameras come in various forms including the traditional security camera.

Videoconferencing Equipment - allows two or more locations to communicate simultaneously using telecommunication technologies. These technologies take advantage of the new high definition video standards. Videoconferencing is now part of normal day-to-day operations in industries like the medical field.

Network and IoT Sensors - One of the fastest sectors of information technology is the use of intelligent devices and sensors. The computer industry brands this sector as the Internet of Things (IoT). Businesses and consumers use IoT devices to automate processes, monitor environmental conditions, and alert the user of adverse conditions.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

7.4 Physical Security

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Physical Access Control

Fencing and Barricades - Physical barriers are the first thing that comes to mind when thinking about physical security. This is the outermost layer of security, and these solutions are the most publicly visible. A perimeter security system typically consists of perimeter fence system, security gate system, bollards, vehicle entry barriers and guard shelters.

Biometrics - are the automated methods of recognizing an individual based on a physiological or behavioral characteristic. Biometric authentication systems include measurements of the face, fingerprint, hand geometry, iris, retina, signature, and voice. Biometric technologies can be the foundation of highly secure identification and personal verification solutions.

Badges and Access Logs – A badge allows an individual to gain access to an area with automated entry points. An entry point can be a door, a turnstile, a gate, or other barrier. Access badges use various technologies such as a magnetic stripe, barcode, or biometrics. The system logs the transaction for later retrieval. Reports reveal who entered what entry points at what time.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Surveillance

Guards and Escorts - All physical access controls including deterrent and detection systems ultimately rely on personnel to intervene and stop the actual attack or intrusion. In highly secure information system facilities, guards control access to the organization's sensitive areas.

Video and Electronic Surveillance – This type of surveillance can supplement or in some cases, replace security guards. The benefit of video and electronic surveillance is the ability to monitor areas even when no guards or personnel are present, the ability to record and log surveillance videos and data for long periods, and the ability to incorporate motion detection and notification.

RFID and Wireless Surveillance – These types of surveillance are used to manage and locate important information system assets.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

7.5 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

- This chapter discussed the technologies, processes and procedures that cyber wizards use to defend the systems, devices, and data that make up the network infrastructure.
- Host hardening includes securing the operating system, implementing an antivirus solution, and using host-based solutions such as firewalls and intrusion detection systems.
- Server hardening includes managing remote access, securing privileged accounts, and monitoring services.
- Data protection includes file access control and implementing security measures to ensure the confidentiality, integrity, and availability of data.
- Device hardening also involves implementing proven methods of physically securing network devices. Fortifying the kingdom is an on-going process to secure an organization's network infrastructure and requires a constant vigilance to threats against the kingdom.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.

Instructor Materials Chapter 8: Joining the Order of Cybersecurity Specialist

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 8:
Joining the Order of Cybersecurity Specialist

Cybersecurity Essentials v1.0

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 8 - Sections & Objectives

8.1 Cybersecurity Domains

Describe resources available to students interested in pursuing a career in cybersecurity.

8.2 Understanding the Oath of Membership

Explain how ethics provide guidance.

8.3 Next Step

Explain how to take the next step to become a cybersecurity professional.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

8.1 Cybersecurity Domains

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

User Domain

Common User Threats and Vulnerabilities

- The User Domain includes the users who access the organization's information system.
- Users can be employees, customers, business contractors and other individuals that need access to data.
- Users are often the weakest link in the information security systems and pose a significant threat to the confidentiality, integrity, and availability of the organization's data.

Managing User Threats

- Conduct security awareness training and user education.
- Enable and automate content filtering and antivirus scanning.
- Disable internal CD drives and USB ports.
- Minimize permissions, restrict access, track and monitor users and enable intrusion detection.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Device Domain

Common Threats to Devices

- Unattended workstations, user downloads, unpatched software
- Malware, use of unauthorized media, and violations of the acceptable use policy.

Device Domain Threats	Countermeasure to Manage Threat
Unattended workstations	Establish user account policies for passwords and threshold lockouts
User downloads	Establish access control policies, standards, procedures, and guidelines
Unpatched software	Update and apply security patches according to defined policies, standards, procedures, and guidelines
Malware	Enable an automated antivirus solution to scan systems and update antivirus software
Unauthorized media	Disable internal CD drives and USB ports
Acceptable Use Policy Violation	• Use content filtering • Use antivirus scanning for downloaded files • Disable internal CD drives and USB port

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Local Area Network Domain

Common Threats to the LAN

- Unauthorized LAN access, unauthorized access to systems, applications, wireless networks and data
- Network operating system software vulnerabilities, misconfigurations and failure to perform updates
- Unauthorized network probing and port scanning

LAN Domain Threats	Countermeasure to Manage Threat
Unauthorized LAN access	• Secure wiring closets, data centers, computer rooms • Define strict access control policies, procedures, and guidelines
Unauthorized access to systems, applications, and data	• Define strict access control policies, procedures, and guidelines • Restrict access privileges for folders and files based on need
Network operating system software vulnerablitities	• Implement policy to patch and update operating systems
Network operating system unpatched	• Implement policy to patch and update operating systems
Unauthorized access by rogue users	• Require passphrases or authentication for wireless networks
Exploits of data in-transit	• Implement encryption between devices and wireless networks
LAN servers with different hardware or operating systems	• Implement LAN server configuration standards
Unauthorized network probing and port scanning	• Conduct post-configuration penetration tests
Firewall misconfiguration	• Conduct post-configuration penetration tests

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Private Cloud (WAN) Domain

Common Threats to the Private Cloud:

- Unauthorized network probing, port scanning and access to resources.
- Router, firewall, or network device operating system software vulnerability and misconfiguration.
- Remote users accessing the organization's infrastructure and downloading sensitive data.

Private Cloud Domain Threats	Countermeasure to Manage Threat
Unauthorized network probing and port scanning	• Disable ping, probing, and port scanning
Unauthorized access to resources	• Implement intrusion detection and prevention systems
Router, firewall, or network device operating system software vulnerability	• Update devices with security fixes and patches
Router, firewall, or network device configuration error	• Conduct penetration tests post configuration • Test inbound and outbound traffic
Remote users download sensitive data	• Implement data classification standard • Implement file transfer monitoring and scanning

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Public Cloud Domain

Common Threats to the Public Cloud:

- Data breaches, loss or theft of intellectual property and compromised credentials.
- Federated identity repositories are a high-value target.
- Account hijacking, social engineering attacks and lack of understanding on the part of the organization.

Public Cloud Domain Threats	Countermeasure to Manage Threat
Data breaches	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Loss or theft of intellectual property	• Due diligence • Use of encryption • Data backup
Compromised credentials	• Multifactor authentication • Use of encryption • One-time passwords, phone-based authentication, and smartcards
Use of federated identity repositories	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Account hijacking	• Multifactor authentication • Implement one-time passwords, phone-based authentication, and smartcards
Lack of understanding on the part of organization	• Due diligence on agreement responsibilities
Social engoneering attacks that lure the victim	• Security awareness programs
Compliance violations	• Due diligence • Policies

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Physical Facilities Domain

Common Threats to Physical Facilities:

- Natural threats including weather problems, geological hazards, and power interruptions
- Unauthorized access to the facilities, open lobbies, theft, unlocked data center, lack of surveillance
- Social engineering, breach of electronic perimeter defenses

Physical Facilities Domain Threats	Countermeasure to Manage Threat
Natural threats including weather and geological problems	• Develop a disaster recovery plan • Develop a business continuity plan
Unauthorized access to facilities	• Implement badge encryption for entry access
Power interruptions	• Develop a disaster recovery plan
Social engineering	• Implement badge encryption for entry access • Conduct security awareness training regularly
Breach of electronic perimeter defenses	• Test building security using both cyber and physical means to covertly gain access
Theft	• Implement an asset tagging system • Establish policies and procedures for visitors
An open lobby	• Implement badge encryption for entry access
Lack of surveillance	• Implement CCTV coverage of all entrances • Test building security using both cyber and physical means to covertly gain access
An unlocked data center	• Implement badge encryption for entry access

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Application Domain

Common Threats to Applications:

- Unauthorized access to data centers, computer rooms, and wiring closets
- Server downtime for maintenance, IT systems down for extended periods
- Network operating system software vulnerability
- Unauthorized access to systems
- Data loss

Application Domain Threats	Countermeasure to Manage Threat
Unauthorized access to data centers, computer rooms, and wiring closets	• Policies, standards, and procedures for staff and visitors
Server downtime for maintenance	• Disaster recovery plan • Business continuity plan
Network operating system software vulnerability	• Patches and updates completed regularly
Unauthorized access to systems	• Multi-factor authentication • Monitor log files
Data loss	• Data classification standards • Backup procedures
Downtime of IT systems for an extended period	• Disaster recovery plan • Business continuity plan
Software development vulnerabilities	• Conduct software testing prior to launch

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

8.2 Understanding the Oath of Membership

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Ethics and Guiding Principles

Ethics of a Cybersecurity Specialist

Ethics is the little voice in the background guiding a cybersecurity specialist as to what he should or should not do, regardless of whether it is legal. The organization entrusts the cybersecurity specialist with the most sensitive data and resources. The cybersecurity specialist needs to understand how the law and the organization's interests help to guide ethical decisions.

Computer Ethics Institute

The Computer Ethics Institute is a resource for identifying, assessing, and responding to ethical issues throughout the information technology industry. CEI was one of the first organizations to recognize the ethical and public policy issues arising from the rapid growth of the information technology field.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cyber Laws and Liability

Cybercrime

Laws prohibit undesired behaviors. Unfortunately, the advancements in information system technologies are much faster than the legal system can accomodate. A number of laws and regulations affect cyberspace.

Cybercrime

A computer may be involved in a cybercrime in a couple of different ways. There is computer-assisted crime, computer-targeted crime, and computer-incidental crime. Child pornography is an example of computer-incidental crime; the computer is a storage device and is not the actual tool used to commit the crime.

Organizations Created to Fight Cybercrime

There are a number of agencies and organizations out there to aid the fight against cybercrime.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cyber Laws and Liability (Cont.)

Civil, Criminal, and Regulatory Cyber Laws

In the United States, there are three primary sources of laws and regulations: statutory law, administrative law, and common law. All three sources involve computer security. The U.S. Congress established federal administrative agencies and a regulatory framework that includes both civil and criminal penalties for failing to follow the rules.

Industry Specific Laws

- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Payment Card Industry Data Security Standard (PCI DSS)
- Import/Export Encryption Restrictions

Security Breach Notification Laws

- Electronic Communications Privacy Act (ECPA)
- Computer Fraud and Abuse Act (1986)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cyber Laws and Liability (Cont.)

Protecting Privacy

- Privacy Act of 1974
- Freedom of Information ACT (FOIA)
- Family Education Records and Privacy Act (FERPA)
- U.S. Computer Fraud and Abuse Act (CFAA)
- U.S. Children's Online Privacy Protection Act (COPPA)
- U.S. Children's Internet Protection Act (CIPA)
- Video Privacy Protection Act (VPPA)
- Health Insurance Portability & Accountability Act
- California Senate Bill 1386 (SB 1386)

International Laws

- Convention on Cybercrime
- Electronic Privacy Information Center (EPIC)

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Information Websites

National Vulnerability Database (NVD) - is a U.S. government repository of standards-based vulnerability management data that uses the Security Content Automation Protocol (SCAP).

CERT - The Software Engineering Institute (SEI) at Carnegie Mellon University helps government and industry organizations to develop, operate, and maintain software systems that are innovative, affordable, and trustworthy. It is a Federally Funded Research and Development Center sponsored by the U.S. Department of Defense.

Internet Storm Center - provides a free analysis and warning service to Internet users and organizations. It also works with Internet Service Providers to combat malicious cyber criminals. The Internet Storm Center gathers millions of log entries from intrusion detection systems every day using sensors covering 500,000 IP addresses in over 50 countries.

The Advanced Cyber Security Center (ACSC) - is a non-profit organization that brings together industry, academia, and government to address advanced cyber threats. The organization shares information on cyber threats, engages in cybersecurity research and development, and creates education programs to promote the cybersecurity profession.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cybersecurity Weapons

Vulnerability Scanners - assess computers, computer systems, networks, or applications for weaknesses. Vulnerability scanners help to automate security auditing by scanning the network for security risks and producing a prioritized list to address weaknesses.

Penetrating Testing (or pen testing) - is a method of testing the areas of weaknesses in systems by using various malicious techniques. Pen testing is not the same as vulnerability testing. Vulnerability testing just identifies potential problems. Pen testing involves a cybersecurity specialist who hacks a website, network, or server with the organization's permission to try to gain access to resources without the knowledge of usernames, passwords, or other normal means.

Packet Analyzers (or packet sniffers) - intercept and log network traffic. The packet analyzer captures each packet, shows the values of various fields in the packet, and analyzes its content. A sniffer can capture network traffic on both wired and wireless networks.

Security Tools - There is no one size fits all when it comes to the best security tools. Much depends on the situation, circumstance, and personal preference. A cybersecurity specialist must know where to go to get sound information.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

8.3 Next Step

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Next Step

Exploring the Cybersecurity Profession

Defining the Roles of Cybersecurity Wizards

The ISO standard defines the role of cybersecurity wizards. The ISO 27000 framework requires:

- A senior manager responsible for IT and ISM (often the audit sponsor)
- Information security professionals and security administrators
- Site/physical security manager and facilities contacts
- HR contact for HR matters such as disciplinary action and training
- Systems and network managers, security architects and other IT professionals

Job Search Tools

A variety of websites and mobile applications advertise information technology jobs. Each site targets varying job applicants and provides different tools for candidates researching their ideal job position:

- Indeed.com
- CareerBuilder.com
- USAJobs.gov

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

8.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Summary

- This chapter categorizes the information technology infrastructure created by the advancement of technology into seven domains.
- The chapter discussed the laws that affect technology and cybersecurity requirements.
- Laws such as FISMA, GLBA, and FERPA focus on protecting confidentiality.
- Laws that focus on the protection of integrity include FISMA, SOX, and FERPA, and laws that concern availability include FISMA, GLBA, SOX, and CIPA.
- In addition to the laws in force, the cybersecurity specialist needs to understand how the use of computers and technology affect both individuals and society.
- The chapter also explored the opportunity to become a cybersecurity specialist.
- Finally, this chapter discussed several tools available to cybersecurity specialists.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Cisco | Networking Academy®

Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

© 2008 Cisco Systems, Inc. All rights reserved.

Chapter 1: The Need for Cybersecurity

Instructor Materials

Introduction to Cybersecurity v2.1

Chapter 1: The Need for Cybersecurity

Introduction to Cybersecurity v2.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 1: The Need for Cybersecurity

Introduction to Cybersecurity v2.1

Chapter 1 - Sections & Objectives

- 1.1 Personal Data
  - Explain the characteristics and value of personal data.
    - Define personal data.
    - Explain why personal data is profitable to hackers.
- 1.2 Organization Data
  - Explain the characteristics and value of data within an organization.
    - Describe types of data used by governments and organizations.
    - Describe the impact of a security breach.
- 1.3 Attackers and Cybersecurity Professionals
  - Explain the characteristics and motives of cyber attackers and the legal and ethical issues for cybersecurity professionals.
    - Describe the characteristics and motives of an attacker.
- 1.4 Cyberwarfare
  - Explain the characteristics and purpose of cyberwarfare.
    - Describe cyberwarfare.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.1 Personal Data

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction to Personal Data

- What is Cybersecurity?
  - Protection of networked system and data from unauthorized use or harm
- Your Online and Offline Identity
  - Offline Identity
    - Your identity that interacts on a regular basis at home, school or work
  - Online Identity
    - Your identity while you are in cyberspace
    - Should only reveal a limited amount of information about you
    - Username or alias
      - Should not include any personal information
      - Should be appropriate and respectful
      - Should not attract unwanted attention

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction to Personal Data

- Your Data
  - Medical Records
    - electronic health records (EHR) – physical, mental, and other personal information
    - prescriptions
  - Education Records
    - Grades, test scores, courses taken, awards and degrees rewarded
    - Attendance
    - Disciplinary reports
  - Employment and Financial Records
    - Income and expenditures
    - Tax records – paycheck stubs, credit card statements, credit rating and banking statement
    - Past employment and performance

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction to Personal Data

- Where is Your Data?
  - Medical records: doctor's office, insurance company
  - Store loyalty cards
    - Stores compile your purchases
    - Marketing partner uses the profiles for target advertisement
  - Online pictures: friends, strangers may also have a copy
- Your Computer Devices
  - Data storage and your portal to your online data
  - List some example of your computing devices

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Personal Data as a Target

- How do the criminals get your money?
  - Online credentials
    - Gives thieves access to your accounts
  - Creative schemes
    - Trick into wiring money to your friends or family
- Why do they want your identity?
  - Long-term profits
  - Medical benefits
  - File a fake tax return
  - Open credit card accounts
  - Obtain loans

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.2 Organizational Data

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Introduction to Organizational Data

- Types of Organizational Data
  - Traditional Data
    - Personnel – application materials, payroll, offer letter, employee agreements
    - Intellectual – patents, trademarks, product plans, trade secrets
    - Financial – income statements, balance sheets, cash flow statements
  - Internet of Things and Big Data
    - IoT – large network of physical objects, such as sensors
    - Big Data – data from the IoT
- Confidentiality, Integrity and Availability
  - Confidentiality – privacy
  - Integrity – accuracy and trustworthiness of the information
  - Availability – information is accessible

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Compare Data with a Hash

Networking Academy

Lab – Compare Data with a Hash

Objectives

Use a hashing program to verify the integrity of data.

Background / Scenario

It is important to understand when data has been corrupted or it has been tampered with. A hashing program can be used to verify if data has changed, or if it has remained the same. A hashing program performs a hash function on data or a file, which returns a (usually much shorter) value. There are many different hash functions, some very simple and some very complex. When the same hash is performed on the same data, the value that is returned is always the same. If any change is performed on the data, the hash value returned will be different.

Note: You will need installation privileges and some knowledge of the process to install Windows programs.

Required Resources

- PC with Internet access

Step 1: Create a Text file

a. Search your computer for the Notepad program and open it.

b. Type some text in the program.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Impact of a Security Breach

- The Consequences of a Security Breach
  - Not feasible to prevent every attack
  - Attackers will always find new ways
  - Ruined reputation, vandalism, theft, revenue lost, damaged intellectual property
- Security Breach Example - LastPass
  - An online password manager
  - Stolen email addresses, password reminders, and authentication hashes
  - Requires email verification or multi-factor authentication when logging in from an unknown device
  - Users should use complex master password, change master password periodically, and beware of phishing attacks

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Impact of a Security Breach

- Security Breach Example - Vtech
  - Vtech is a high tech toy maker for children
  - exposed sensitive information including customer names, email addresses, passwords, pictures, and chat logs.
  - Vtech did not safeguard information properly
  - Hackers can create email accounts, apply for credits, and commit crimes using the children's information
  - Hackers can also take over the parents' online accounts
- Security Breach Example - Equifax
  - Equifax is a consumer credit reporting agency.
  - Attackers exploited a vulnerability in web application software.
  - Equifax established a dedicated web site with a new domain name that allowed nefarious parties to create unauthorized websites for phishing scheme

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – What Was Taken?

Networking Academy

Lab – What was Taken?

Objectives

Search for and read about a few recent occurrences of security breaches.

Background / Scenario

Security breaches occur when individuals or applications are trying to gain unauthorized access to data, applications, services, or devices. During these breaches, the attackers, whether they are insiders or not, attempt to obtain information that they could use for financial gains or other advantages. In this lab, you will explore a few security breaches to determine what was taken, what exploits were used, and what you can do to protect yourself.

Required Resources

- PC or mobile device with Internet access

Security Breach Research

a. Use the two provided links to security breaches from different sectors to fill out the table below.

b. Search for a few additional interesting breaches and record the findings in the table below.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.3 Attackers and Cybersecurity Professionals

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Attackers

- Amateurs
  - Script kiddies with little or no skill
  - Using existing tools or instructions found online for attacks
- Hackers - break into computers or networks to gain access
  - White hats – break into system with permission to discover weaknesses so that the security of these systems can be improved
  - Gray hats – compromise systems without permission
  - Black hats - take advantage of any vulnerability for illegal personal, financial or political gain
- Organized Hackers - organizations of cyber criminals, hacktivists, terrorists, and state-sponsored hackers.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Internal and External Threats

- Internal Security Threats
  - Can be an employee or contract partner
    - Mishandle confidential data
    - Threaten the operations of internal servers or network infrastructure devices
    - Facilitate outside attacks by connecting infected USB media into the corporate computer system
    - Accidentally invite malware onto the network through malicious email or websites
    - Can cause great damage because of direct access
- External Security Threats
  - exploit vulnerabilities in network or computing devices
  - use social engineering to gain access

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.4 Cyberwarfare

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is Cyberwarfare

- What is Cyberwarfare?
  - Conflict using cyberspace
  - Stuxnet malware
    - Designed to damage Iran's nuclear enrichment plant
    - Used modular coding
    - Used stolen digital certificates

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Purpose of Cyberwarfare

- Use to gain advantage over adversaries, nations or competitors
  - Can sabotage the infrastructure of other nations
  - Give the attackers the ability to blackmail governmental personnel
  - Citizens may lose confidence in the government's ability to protect them.
  - Affect the citizens' faith in their government without ever physically invading the targeted nation.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

1.5 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary

- Define personal data.
- Explain the characteristics and value of personal data.
- Explain the characteristics and value of data within an organization.
- Describe the impact of security breach.
- Describe the characteristics and motives of an attacker.
- Describe the legal and ethical issues facing a cybersecurity professional.
- Explain the characteristics and purpose of cyberwarfare.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO

Chapter 2: Attacks, Concepts and Techniques

Instructor Materials

Introduction to Cybersecurity v2.1

Chapter 2: Attacks, Concepts and Techniques

Introduction to Cybersecurity v2.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 2: Attacks, Concepts and Techniques

Introduction to Cybersecurity v2.1

Chapter 2 - Sections & Objectives

- 2.1 Analyzing a Cyberattack
  - Explain the characteristics and operation of a cyber attack.
    - Explain how a security vulnerability is exploited.
    - Identify examples of security vulnerabilities.
    - Describe types of malware and their symptoms.
    - Describe methods of infiltration.
    - Describe methods used to deny service.
- 2.2 The Cybersecurity Landscape
  - Explain trends in the cyberthreat landscape.
    - Describe a blended attack.
    - Describe the importance of impact reduction.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.1 Analyzing a Cyberattack

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Finding Security Vulnerabilities

- An *exploit* is the term used to describe a program written to take advantage of a known vulnerability.
- An *attack* is the act of using an exploit against a vulnerability.
- Software vulnerability
  - Errors in OS or application code
  - SYNful Knock – Vulnerability in Cisco IOS
    - allows attackers to gain control of the routers
    - monitor network communication
    - infect other network devices.
  - Project Zero – Google formed a permanent team dedicated to finding software vulnerabilities.

- Hardware vulnerability
  - Hardware design flaws
  - Rowhammer - RAM memory exploit allows data to be retrieved from nearby address memory cells.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Categorizing Security Vulnerabilities

- Buffer Overflow
  - Data is written beyond the limits of a buffer
- Non-validated Input
  - Force programs to behave in an unintended way
- Race Conditions
  - Improperly ordered or timed events
- Weaknesses in Security Practices
  - Protect sensitive data through authentication, authorization, and encryption
- Access-control Problems
  - Access control to physical equipment and resources
  - Security practices

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Malware

- Malware is used to steal data, bypass access controls, cause harm to, or compromise a system.
- Types of Malware
  - **Spyware** - track and spy on the user
  - **Adware** - deliver advertisements, usually comes with spyware
  - **Bot** - automatically perform action
  - **Ransomware** - hold a computer system or the data captive until a payment is made
  - **Scareware** - persuade the user to take a specific action based on fear.

Initial Code Red Worm Infection

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Types of Malware (Cont.)

- Types of Malware (Cont.)
  - **Rootkit** - modify the operating system to create a backdoor
  - **Virus** - malicious executable code that is attached to other executable files
  - **Trojan horse** - carries out malicious operations under the guise of a desired operation
  - **Worm** - replicate themselves by independently exploiting vulnerabilities in networks
  - **Man-in-The-Middle** or **Man-in-The-Mobile** – take control over a device without the user's knowledge

Code Red Worm Infection 19 Hours Later

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Symptoms of Malware

- There is an increase in CPU usage.
- There is a decrease in computer speed.
- The computer freezes or crashes often.
- There is a decrease in Web browsing speed.
- There are unexplainable problems with network connections.
- Files are modified.
- Files are deleted.
- There is a presence of unknown files, programs, or desktop icons.
- There are unknown processes running.
- Programs are turning off or reconfiguring themselves.
- Email is being sent without the user's knowledge or consent.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Social Engineering

- Social Engineering – manipulation of individual into performing actions or divulging confidential information
  - **Pretexting** - an attacker calls an individual and lies to them in an attempt to gain access to privileged data.
  - **Tailgating** - an attacker quickly follows an authorized person into a secure location.
  - **Something for something (Quid pro quo)** - an attacker requests personal information from a party in exchange for something

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Wi-Fi Password Cracking

- Wi-Fi Password Cracking – Password discovery
  - **Social engineering** - The attacker manipulates a person who knows the password into providing it.
  - **Brute-force attacks** - The attacker tries several possible passwords in an attempt to guess the password.
  - **Network sniffing** - The password maybe discovered by listening and capturing packets send on the network.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Phishing

- Phishing
  - malicious party sends a fraudulent email disguised as being from a legitimate, trusted source
  - trick the recipient into installing malware on their device or sharing personal or financial information
- Spear phishing
  - a highly targeted phishing attack

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Vulnerability Exploitation

- Vulnerability Exploitation – scan to find vulnerability to exploit
  - **Step 1** - Gather information about the target system using port scanner or social engineering
  - **Step 2** - Determine learned information from step 1
  - **Step 3** - Look for vulnerability
  - **Step 4** - Use a known exploit or write a new exploit
- Advanced Persistent Threats – a multi-phase, long term, stealthy and advanced operation against a specific target
  - usually well-funded
  - deploy customized malware

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

DoS

- DoS is a disruption of network services
  - **Overwhelming quantity of traffic** - a network, host, or application is sent an enormous quantity of data at a rate which it cannot handle
  - **Maliciously formatted packets** - maliciously formatted packet is sent to a host or application and the receiver is unable to handle it

ates. All rights reserved. Cisco Confidential

DDoS

- Similar to DoS, from multiple, coordinated sources
- Botnet - a network of infected hosts
- Zombie - infected hosts
- The zombies are controlled by handler systems.
- The zombies continues to infect more hosts, creating more zombies.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

SEO Poisoning

- SEO
  - Search Engine Optimization
  - Techniques to improve a website's ranking by a search engine
- SEO Poisoning
  - Increase traffic to malicious websites
  - Force malicious sites to rank higher

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.2 The Cybersecurity Landscape

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is a Blended Attack?

- Uses multiple techniques to compromise a target
- Uses a hybrid of worms, Trojan horses, spyware, keyloggers, spam and phishing schemes
- Common blended attack example
  - spam email messages, instant messages or legitimate websites to distribute links
  - DDoS combined with phishing emails
- Examples: Nimbda, CodeRed, BugBear, Klez, Slammer, Zeus/LICAT, and Conficker

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

What is Impact Reduction?

- Communicate the issue
- Be sincere and accountable
- Provide details
- Understand the cause of the breach
- Take steps to avoid another similar breach in the future
- Ensure all systems are clean
- Educate employees, partners and customers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

2.3 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary

- Identify examples of security vulnerabilities.
- Explain how a security vulnerability is exploited.
- Describe types of malware and their symptoms, methods of infiltration, methods used to deny service.
- Describe a blended attack and the importance of impact reduction.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO

Chapter 3: Protecting Your Data and Privacy

Instructor Materials

Introduction to Cybersecurity v2.1

Chapter 3: Protecting Your Data and Privacy

Introduction to Cybersecurity v2.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 3: Protecting Your Data and Privacy

Introduction to Cybersecurity v2.1

Chapter 3 - Sections & Objectives

- 3.1 Protecting Your Data
  - Explain how to protect devices from threats.
    - Explain how to protect your devices and network.
    - Describe safe procedures for data maintenance.
- 3.2 Safeguarding Your Online Privacy
  - Explain how to safeguard your privacy.
    - Describe strong authentication methods.
    - Describe safe online behaviors.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.1 Protecting Your Data

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Your Computing Devices

- Keep the Firewall On
  - Prevent unauthorized access to your data or computing devices
  - Keep the firewall up to date
- Use Antivirus and Antispyware
  - Prevent unauthorized access to your data or computing devices
  - Only download software from trusted websites
  - Keep the software up to date
- Manage Your Operating System and Browser
  - Set the security settings at medium or higher
  - Update your computer's operating system and browser
  - Download and install the latest software patches and security updates
- Protect All Your Devices
  - Password protect
  - Encrypt the data
  - Only store necessary information
  - IoT devices

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Use Wireless Networks Safely

- Home Wireless Network
  - Change the pre-set SSID and default administrative password on your Wi-Fi router.
  - Disable SSID broadcast
  - Use WPA2 encryption feature
  - Be aware of WPA2 protocol security flaw – KRACK
    - Allows intruder to break the encryption between wireless router and clients
- Use caution when using public Wi-Fi hotspots
  - Avoid accessing or sending sensitive information
  - Use of VPN tunnel can prevent eavesdropping
- Turn off Bluetooth when not in use

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Use Unique Passwords for Each Online Account

- Prevents criminals from accessing all your online accounts using one stolen credentials
- Use password managers to help with remembering passwords
- Tips for choosing a good password:
  - Do not use dictionary words or names in any languages
  - Do not use common misspellings of dictionary words
  - Do not use computer names or account names
  - If possible use special characters, such as ! @ # $ % ^ & * ( )
  - Use a password with ten or more characters

OK	Good	Better
allwhitecat	a11whitecat	A11whi7ec@t
Fblogin	1FBLogin	1.FB.L0gin$
amazonpass	AmazonPa55	Am@z0nPa55
ilikemyschool	ILikeMySchool	!Lik3MySch00l
Hightidenow	HighTideNow	H1gh7id3Now

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Use Passphrase Rather Than a Password

- Tips in choosing a good passphrase:
  - Choose a meaningful statement to you
  - Add special characters, such as ! @ # $ % ^ & * ( )
  - The longer the better
  - Avoid common or famous statements, for example, lyrics from a popular song
- Summary of the new NIST guidelines:
  - 8 characters minimum in length, but no more than 64 characters
  - No common, easily guessed passwords, such as password, abc123
  - No composition rules, such as having to include lowercase and uppercase letters and numbers
  - No knowledge-based authentication, such as information from shared secret questions, marketing data, transaction history
  - Improve typing accuracy by allowing the user to see the password while typing
  - All printing characters and spaces are allowed
  - No password hints
  - No periodical or arbitrary password expiration

OK	Thisismypassphrase.
Good	Acatthatlovesdogs.
Better	Acat th@tlov3sd0gs.

Lab – Create and Store Strong Passwords

Networking Academy

Lab – Create and Store Strong Passwords

Objectives

Understand the concepts behind a strong password.

Part 1: Explore the concepts behind creating a strong password.

Part 2: Explore the concepts behind securely storing your passwords?

Background / Scenario

Passwords are widely used to enforce access to resources. Attackers will use many techniques to learn users' passwords and gain unauthorized access to a resource or data.

To better protect yourself, it is important to understand what makes a strong password and how to store it securely.

Required Resources

- PC or mobile device with Internet access

Part 1: Creating a Strong Password

Strong passwords have four main requirements listed in order of importance:

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Encrypt Your Data

- Encrypted data can only be read with the secret key or password
- Prevent unauthorized users from reading the content
- What is Encryption?
  - process of converting the information into a form where an unauthorized party cannot read it

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Back up Your Data

- Prevent the loss of irreplaceable data
- Need additional storage location for the data
- Copy the data to the backup location regularly and automatically
- Local Backup
  - NAS, external hard drive, CDs/DVDs, thumb drives, or tapes
  - Total control and responsible for the cost and maintenance
- Cloud Storage Service, such as AWS
  - Access to backup as long as you have access to your account
  - may need to be more selective about the data being backed up

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Back up Data to External Storage

Networking Academy

Lab – Backup Data to External Storage

Objectives

Backup user data.

Part 1: Use a local external disk to backup data

Part 2: Use a remote disk to backup data

Background / Scenario

It is important to establish a backup strategy that includes data recovery of personal files.

While many backup tools are available, this lab focuses on the Microsoft Backup Utility to perform backups to local external disks. In Part 2, this lab uses the Dropbox service to backup data to a remote or cloud-based drive.

Required Resources

- PC or mobile device with Internet access

Part 1: Backing Up to a Local External Disk

Step 1: Getting Started With Backup Tools in Windows

Computer usage and organizational requirements determine how often data must be backed up and the type

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Deleting Your Data Permanently

- Use available tools to delete permanently: SDelete and Secure Empty Trash, for example
- Destroy the storage device to ensure that the data is unrecoverable
- Delete the online versions

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Who Owns Your Data

Networking Academy

Lab – Who Owns Your Data?

Objectives

Explore the ownership of your data when that data is not stored in a local system.

Part 1: Explore the Terms of Service Policy

Part 2: Do You Know What You Signed Up For?

Background / Scenario

Social media and online storage have become an integral part of many people's lives. Files, photos, and videos are shared between friends and family. Online collaboration and meetings are conducted in the workplace with people who are many miles from each other. The storage of data is no longer limited to just the devices you access locally. The geographical location of storage devices is no longer a limiting factor for storing or backing up data at remote locations.

In this lab, you will explore legal agreements required to use various online services. You will also explore some of the ways you can protect your data.

Required Resources

- PC or mobile device with Internet access

Part 1: Explore the Terms of Service Policy

If you are using online services to store data or communicate with your friends or family, you probably entered into an agreement with the provider. The Terms of Service, also known as Terms of Use or Terms and

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.2 Safeguarding Your Online Privacy

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Two Factor Authentication

- Popular online services use two factor authentication
- Need Username / password or PIN and a second token for access:
  - **Physical object** - credit card, ATM card, phone, or fob
  - **Biometric scan** - fingerprint, palm print, as well as facial or voice recognition

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

OAuth 2.0

- An open standard protocol that allows an end user's credentials to access third party applications without exposing the user's password
- Act as the middle man to decide whether to allow end users access to third party applications.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Sharing Too Much Information?

Do Not Share Too Much on Social Media

- Share as little information as possible on social media
- Do not share information such as:
  - Birth date
  - Email address
  - Phone number
- Check your social media settings

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Email and Web Browser Privacy

- Email is like sending a postcard.
- Copies of the email can be read by anyone with access.
- The email is passed among different servers
- Use the private browsing mode can prevent other from gathering information about your online activities.
- Private mode on popular browser
  - **Microsoft Internet Explorer**: InPrivate
  - **Google Chrome**: Incognito
  - **Mozilla Firefox**: Private tab / private window
  - **Safari**: Private: Private browsing

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Lab – Discover Your Own Risky Online Behavior

Networking Academy

Lab – Discover Your Own Risky Online Behavior

Objectives

Explore actions performed online that may compromise your safety or privacy.

Background / Scenario

The Internet is a hostile environment, and you must be vigilant to ensure your data is not compromised. Attackers are creative and will attempt many different techniques to trick users. This lab helps you identify risky online behavior and provide tips on how to become safer online.

Part 1: Explore the Terms of Service Policy

Answer the questions below with honesty and take note of how many points each answer gives you. Add all points to a total score and move on to Part 2 for an analysis of your online behavior.

a. What kind of information do you share with social media sites?

1) Everything; I rely on social media to keep in touch with friends and family. (3 points)
2) Articles and news I find or read (2 points)
3) It depends; I filter out what I share and with whom I share. (1 point)
4) Nothing; I do not use social media. (0 points)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

3.3 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Summary

- Explain how to protect your devices and network from threats.
- Describe safe procedures for data maintenance.
- Explain how to safeguard your privacy by using strong authentication methods and practicing safe online behaviors.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO

Chapter 4: Protecting the Organization

Instructor Materials

Introduction to Cybersecurity v2.1

Chapter 4: Protecting the Organization

Introduction to Cybersecurity v2.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 4: Protecting the Organization

Introduction to Cybersecurity v2.1

Chapter 4 - Sections & Objectives

- 4.1 Firewalls
  - Explain techniques to protect organizations from cyber attacks.
    - Describe the various types of firewalls.
    - Describe different types of security appliances.
    - Describe different methods of detecting attacks in real time.
    - Describe methods of detecting malware.
    - Describe security best practices for organizations.
- 4.2 Behavior Approach to Cybersecurity
  - Explain the behavior-based approach to cybersecurity.
    - Define the term botnet.
    - Define the term kill chain.
    - Define behavior-based security.
    - Explain how NetFlow helps to defend against cyberattacks.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 4 - Sections & Objectives (Cont.)

- 4.3 Cisco's Approach to Cybersecurity
  - Explain the Cisco approach to providing cybersecurity.
    - Identify the function of CSIRT within Cisco.
    - Explain the purpose of a security playbook.
    - Identify tools used for incident prevention and detection.
    - Define IDS and IPS.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.1 Firewalls

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Firewall Types

- Control or filter incoming or outgoing communications on a network or device
- Common firewall types
  - **Network Layer Firewall** – source and destination IP addresses
  - **Transport Layer Firewall** – source and destination data ports, connection states
  - **Application Layer Firewall** – application, program or service
  - **Context Aware Application Firewall** – user, device, role, application type, and threat profile
  - **Proxy Server** –web content requests
  - **Reverse Proxy Server** – protect, hide, offload, and distribute access to web servers
  - **Network Address Translation (NAT) Firewall** – hides or masquerades the private addresses of network hosts
  - **Host-based Firewall** – filtering of ports and system service calls on a single computer operating system

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Port Scanning

- Process of probing a computer, server or other network host for open ports
- Port numbers are assigned to each running application on a device.
- Reconnaissance tool to identify running OS and services
  - Nmap – A port scanning tool
- Common responses:
  - **Open or Accepted** - a service is listening on the port.
  - **Closed, Denied, or Not Listening** – connections will be denied to the port.
  - **Filtered, Dropped, or Blocked** – no reply from the host.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Appliances

- Security appliances fall into these general categories:
  - **Routers** - can have many firewall capabilities: traffic filtering, IPS, encryption, and VPN.
  - **Firewalls** – may also have router capability, advanced network management and analytics.
  - **IPS** - dedicated to intrusion prevention.
  - **VPN** - designed for secure encrypted tunneling.
  - **Malware/Antivirus** - Cisco Advanced Malware Protection (AMP) comes in next generation Cisco routers, firewalls, IPS devices, Web and Email Security Appliances and can also be installed as software in host computers.
  - **Other Security Devices** – includes web and email security appliances, decryption devices, client access control servers, and security management systems.

Detecting Attacks in Real Time

- Zero-day attack
  - A hacker exploits a flaw in a piece of software before the creator can fix it.
- **Real Time Scanning from Edge to Endpoint**
  - Actively scanning for attacks using firewall and IDS/IPS network device
  - detection with connections to online global threat centers
  - detect network anomalies using context-based analysis and behavior detection
- **DDoS Attacks and Real Time Response**
  - DDoS, one of the biggest attack threats, can cripple Internet servers and network availability.
  - DDoS originates from hundreds, or thousands of zombie hosts, and the attacks appear as legitimate traffic.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Protecting Against Malware

Cisco AMP Threat Grid benefits security functions across the organization

Secure Operations Center Team	Incidence Response Team	Threat Intelligence Team	Security Infrastructure Engineering Team
Get more accurate, actionable data	Use forensically sound information to understand suspicious behavior faster	Proactively improve security infrastructure	Consume and act on threat information faster, and in an automated manner

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Best Practices

- **Some published Security Best Practices:**
  - **Perform Risk Assessment** – Knowing the value of what you are protecting will help in justifying security expenditures.
  - **Create a Security Policy** – Create a policy that clearly outlines company rules, job duties, and expectations.
  - **Physical Security Measures** – Restrict access to networking closets, server locations, as well as fire suppression.
  - **Human Resource Security Measures** – Employees should be properly researched with background checks.
  - **Perform and Test Backups** – Perform regular backups and test data recovery from backups.
  - **Maintain Security Patches and Updates** – Regularly update server, client, and network device operating systems and programs.
  - **Employ Access Controls** – Configure user roles and privilege levels as well as strong user authentication.
  - **Regularly Test Incident Response** – Employ an incident response team and test emergency response scenarios.
  - **Implement a Network Monitoring, Analytics and Management Tool** - Choose a security monitoring solution that integrates with other technologies.
  - **Implement Network Security Devices** – Use next generation routers, firewalls, and other security appliances.
  - **Implement a Comprehensive Endpoint Security Solution** – Use enterprise level antimalware and antivirus software.
  - **Educate Users** – Educate users and employees in secure procedures.
  - **Encrypt data** – Encrypt all sensitive company data including email.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.2 Behavior Approach to Cybersecurity

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Botnet

- Botnet
  - A group of bots connect through the Internet
  - Controlled by malicious individuals or groups
- Bot
  - Typically infected by visiting a website, opening an email attachment, or opening an infected media file

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

The Kill Chain in Cyberdefense

Kill Chain is the stages of an information systems attack.

1. **Reconnaissance** – Gathers information
2. **Weaponization** - Creates targeted exploit and malicious payload
3. **Delivery** - Sends the exploit and malicious payload to the target
4. **Exploitation** – Executes the exploit
5. **Installation** - Installs malware and backdoors
6. **Command and Control** - Remote control from a command and control channel or server.
7. **Action** – Performs malicious actions or additional attacks on other devices

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Behavior-Based Security

- Honeypots
  - Lures the attacker by appealing to the attackers' predictable behavior
  - Captures, logs and analyze the attackers' behavior
  - Administrator can gain more knowledge and build better defense
- Cisco's Cyber Threat Defense Solution Architecture
  - Uses behavior-based detection and indicators
  - Provide greater visibility, context and control

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Netflow

- Gather information about data flowing through a network
- Important components in behavior-based detection and analysis
- Establish baseline behaviors

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.3 Cisco’s Approach to Cybersecurity

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CSIRT

- Computer Security Incident Response Team
  - help ensure company, system, and data preservation by performing comprehensive investigations into computer security incidents
  - provides proactive threat assessment, mitigation planning, incident trend analysis, and security architecture review

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

APCERT

FIRST
Improving Security Together

computer emergency response team
CERT-EU
for the EU institutions, bodies and agencies

Software Engineering Institute | Carnegie Mellon University

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Security Playbook

- Collection of repeatable queries against security event data sources that lead to incident detection and response
- What does it need to accomplish?
  - Detect malware infected machines.
  - Detect suspicious network activity.
  - Detect irregular authentication attempts.
  - Describe and understand inbound and outbound traffic.
  - Provide summary information including trends, statistics, and counts.
  - Provide usable and quick access to statistics and metrics.
  - Correlate events across all relevant data sources.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Tools for Incident Prevention and Detection

- SIEM – Security Information and Event Management
  - Software that collects and analyzes security alerts, logs and other real time and historical data from security devices on the network
- DLP – Data Loss Prevention
  - Stops sensitive data from being stolen or escaped from the network
  - Designs to monitor and protect data in three different states
- Cisco Identity Services Engine (Cisco ISE) and TrustSec
  - Uses role-based access control policies

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

IDS and IPS

- IDS – Intrusion Detection System
  - Usually placed offline
  - Does not prevent attacks
  - Detect, log, and report
- IPS – Intrusion Prevention System
  - Ability to block or deny traffic based on a positive rule or signature match
- IDS/IPS system
  - Snort
  - Sourcefire (Cisco)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

4.4 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter Summary

- Describe the various types of firewalls and security appliances.
- Describe different methods of detecting malware and attacks in real time.
- Describe security best practices for organizations.
- Define botnet, kill chain, and behavior-based security.
- Explain how Netflow can help defend against cyberattacks.
- Identify the function of CSIRT within Cisco.
- Explain the purpose of a security playbook.
- Identify tools used for incident prevention and detection.
- Define IDS and IPS.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO

Chapter 5: Will Your Future Be in Cybersecurity?

Instructor Materials

Introduction to Cybersecurity v2.1

Chapter 5: Will Your Future Be in Cybersecurity?

Introduction to Cybersecurity v2.1
Planning Guide

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter 5: Will Your Future Be in Cybersecurity?

Introduction to Cybersecurity v2.1

Chapter 5 - Sections & Objectives

- 5.1 Cybersecurity Education and Careers
  - Explain the legal and ethical issues facing cybersecurity professionals
    - Describe the legal and ethical issues facing a cybersecurity professional.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5.1 Cybersecurity Education and Careers

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Legal Issues in Cybersecurity

- Personal Legal Issues
  - Be responsible with your skills
- Corporate Legal Issues
  - Businesses are required to abide by the cybersecurity laws.
  - Break the law, you could lose your job and your company could be punished.
  - When you are not sure, you should consult legal department.
- International Law and Cybersecurity
  - IMPACT
    - global partnership of world governments, industries and academia
    - Improving global capabilities when dealing with cyber threats

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Ethical Issues in Cybersecurity

- Personal Ethical Issues
  - Legal behavior may still be unethical.
- Corporate Ethical Issues
  - Ethics are codes of behavior that are sometimes enforced by laws.
  - Organizations with Published Codes of Ethics:
    - The CyberSecurity Institute (CSI)
    - The Information Systems Security Association (ISSA)
    - The Association of Information Technology Professionals (AITP)

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Cybersecurity Jobs

- Some online job search engine
  - ITJobMatch
  - Monster
  - CareerBuilder
- Different types of cybersecurity jobs
  - Penetration testing / ethical hacker
  - Security administrator
  - Network administrator
  - System administrator

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

5.1 Chapter Summary

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Chapter Summary

- Describe the legal and ethical issues.

© 2016 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

CISCO