Information Assurance & Security 2

Introduction to IA

Question

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

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
- 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?

"Information is data endowed with relevanc
Converting data into information thus requ
Knowledge by definition is specialized."(Bly

And what characteristics should informa l? It should be: accurate, timely, complete, v ailable.

What is Information?

According to Raggad, 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?

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?

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.

Which of these are the most important? How would you decide?

Information Assurance & Security 2

Information Security Careers

Surveying Information Security Careers and the Security + Certification

- Today, businesses and organizations require employees and even prospective applicants
  - To demonstrate that they are familiar with computer security practices
- Many organizations use the CompTIA Security+certification to verify security competency

Types of Information Security Jobs

Information Assurance (IA)

- A superset of information security including security issues that do not involve computers
- Covers a broader area than just basic technology defense tools and tactics
- Also includes reliability, strategic risk management, and corporate governance issues such as privacy, compliance, audits, business continuity, and disaster recovery
- Is interdisciplinary; individuals who are employed in it may come from different fields of study

Types of Information Security Jobs (continued)

Information security, also called computer security

- Involves the tools and tactics to defend against computer attacks
- Does not include security issues that do not involve computers

Two broad categories of information security positions

- Information security managerial position
- Information security technical position

Title	Position in Organization	Responsibilities	Average Salary
Chief Information Security Officer (CISO)	Reports directly to the CIO (large organizations may have more layers of management between); other titles "Manager for Security" and "Security Administrator"	The assessment, management, and implementation of security	$140,000
Security manager	Reports to CISO and supervises technicians, administrators, and staff	Work on tasks identified by CISO and resolves issues identified by technicians; requires understanding of configuration and operation but not necessarily technical mastery	$75,000
Security administrator	Between security manager and security technician	Has both technical knowledge and managerial skills; manages daily operations of security technology; may analyze and design security solutions within a specific entity; identifies users' needs	$64,000
Security technician	Generally entry-level position with technical skills	Provide technical support to configure security hardware, implement security software, diagnose and troubleshoot problems; focus on major security technology group	$40,000

Types of Information Security Jobs (continued)

Information security, also called computer security

- Involves the tools and tactics to defend against computer attacks
- Does not include security issues that do not involve computers

Two broad categories of information security positions

- Information security managerial position
- Information security technical position

Information Assurance & Security 2

Digital Security and Concepts of Cryptography

Objectives

- Understand the basics of digital security and the general concepts of cryptography in preparation for application and implementation
- Understand the different kinds of cryptographic protocols and the founding concepts that builds them

Objectives (minor)

- Describe the challenges of securing information
- Define information security and explain why it is important
- Identify the types of attackers that are common today
- List the basic steps of an attack
- Describe the five steps in a defense
- Explain the different types of information security careers

Challenges of Securing Information

- There is no simple solution to securing information
- This can be seen through the different types of attacks that users face today
    - As well as the difficulties in defending against these attacks

Today's Security Attacks

- Typical warnings:
  - A malicious program was introduced at some point in the manufacturing process of a popular brand of digital photo frames
  - Nigerian e-mail scam claimed to be sent from the U.N.
  - "Booby-trapped" Web pages are growing at an increasing rate
  - A new worm disables Microsoft Windows Automatic Updating and the Task Manager
  - Apple has issued an update to address 25 security flaws in its operating system OS X

Today's Security Attacks (continued)

- Typical warnings:
  - The Anti-Phishing Working Group (APWG) reports that the number of unique phishing sites continues to increase
  - Researchers at the University of Maryland attached four computers equipped with weak passwords to the Internet for 24 days to see what would happen
    - These computer were hit by an intrusion attempt on average once every 39 seconds

Today's Security Attacks (continued)

- Security statistics bear witness to the continual success of attackers:
  - TJX Companies, Inc. reported that over 45 million customer credit card and debit card numbers were stolen by attacker over an 18 month period from 2005 to 2007
  - The major security breaches that occurred during a three-month period
  - The total average cost of a data breach in 2007 was $197 per record compromised
  - A recent report revealed that of 24 federal government agencies, the overall grade was only "C-"

Organization	Description of Security Breach	Number of Identities Exposed
Safe Ride Services, Phoenix	Employee personal information as well as patient demographic and insurance information was exposed.	42,000
American Express Travel	Credit and debit card numbers from American Express, Visa, MasterCard, and Discover were in a man's possession and came from breaking into the computer systems of a restaurant and a restaurant supply business in the Seattle area.	27,257
Yahoo! Voices	Attackers accessed passwords of over 450,000 Yahoo! Voices users and the information was posted online.	453,492
Formspring, San Francisco	Attackers accessed Formspring's development server and posted the passwords of its users online.	28,000,000
University of Texas M.D. Anderson Cancer Center, Houston	A laptop with sensitive patient information was stolen from the home of a faculty member. It contained unencrypted patient names, medical record numbers, treatment and/or research information, and in some instances Social Security numbers.	30,000
The Public Employees Retirement Association (PERA) of New Mexico Albuquerque	A computer containing PERA information was stolen from a consulting agency.	100,000
Bethpage Federal Credit Union, Bethpage, NY	An employee accidentally posted data onto a file transfer protocol site that was not secure. The data contained customer Visa debit card names, addresses, dates of birth, card expiration dates, and checking and savings account numbers.	86,000
University of North Florida (UNF), Jacksonville	Multiple servers exposed Social Security numbers and other sensitive information. Students who submitted housing contracts since 1997 were affected.	23,246

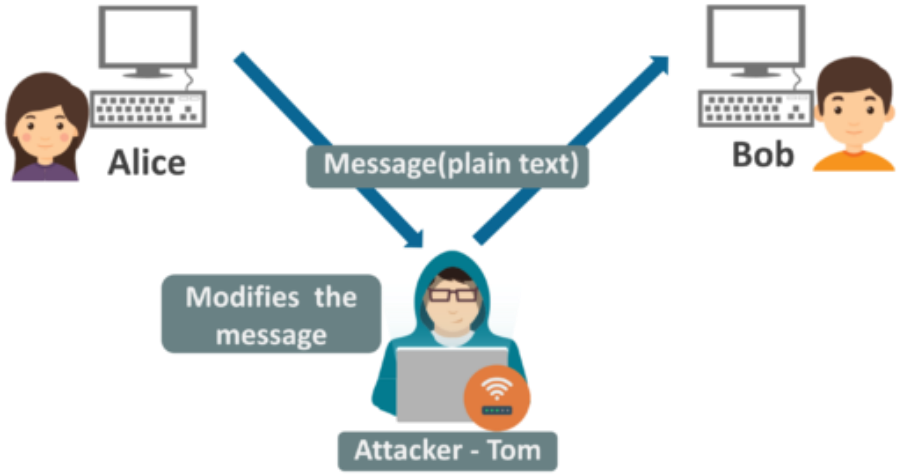
Selected Security Breaches Involving Personal Information In A Three Month Period

Information Assurance & Security 2

Importance of Information Security

What is Security?

- Security is about
  - Honest user
  - Dishonest Attacker
  - How the Attacker
    - Disrupts honest user's use of the system (Integrity, Availability)

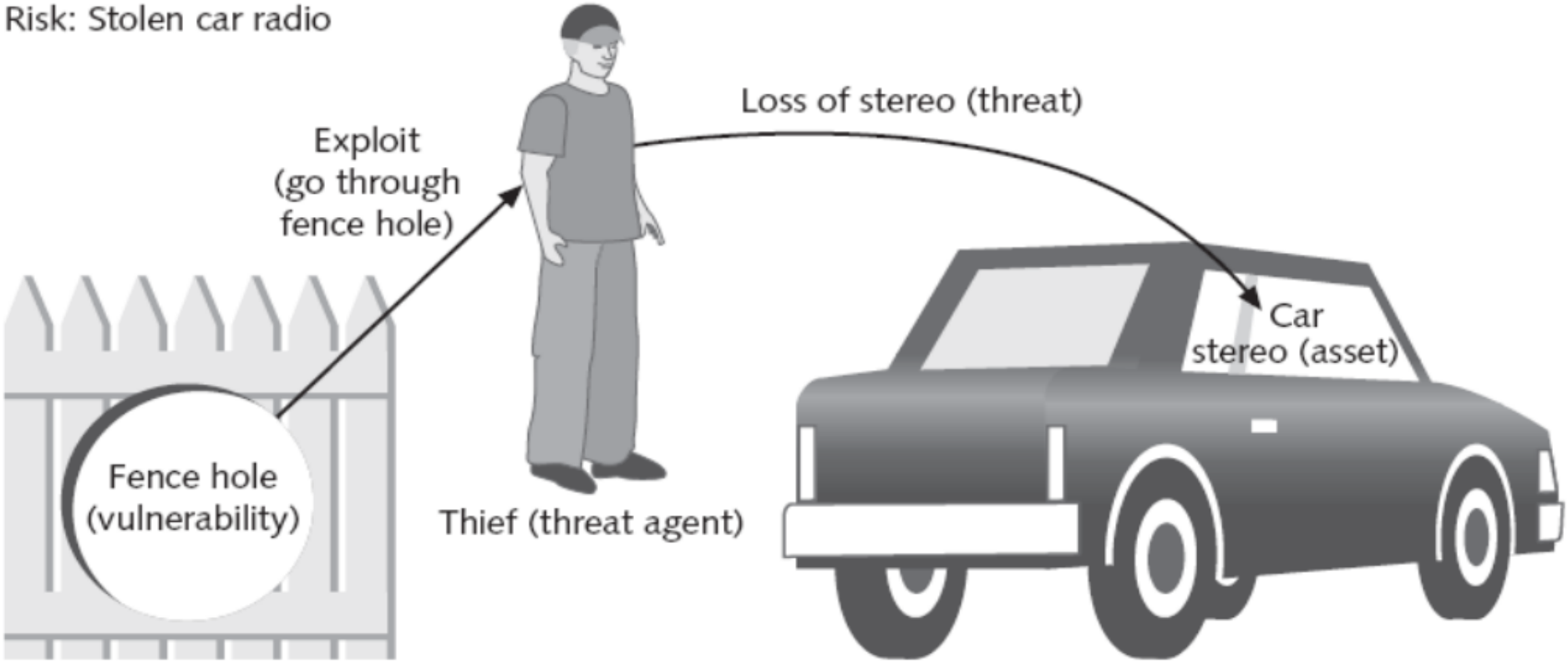


Network Attacker – Intercepts and controls network communication

Web Attacker – Sets up malicious site visited by victim; no control of network

OS Attacker – Controls malicious files and applications

Information Security Terminology (continued)



Information Security Terminology (continued)

Term	Example in Amanda's Scenario	Example in Information Security
Asset	Car stereo	Employee database
Threat	Steal stereo from car	Steal data
Threat agent	Thief	Attacker, virus, flood
Vulnerability	Hole in fence	Software defect
Exploit	Climb through hole in fence	Send virus to unprotected e-mail server
Risk	The likelihood that a thief will exploit the hole	The likelihood that an attacker will exploit the software bug

Importance of Information Security

- Preventing data theft
  - Security is often associated with theft prevention
  - The theft of data is one of the largest causes of financial loss due to an attack
  - Individuals are often victims of data thievery
- Thwarting identity theft
  - Identity theft involves using someone's personal information to establish bank or credit card accounts
    - Cards are then left unpaid, leaving the victim with the debts and ruining their credit rating

Importance of Information Security

- Avoiding legal consequences
  - A number of federal and state laws have been enacted to protect the privacy of electronic data
    - The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
    - The Sarbanes-Oxley Act of 2002 (Sarbox)
    - The Gramm-Leach-Bliley Act (GLBA)
    - USA Patriot Act (2001)
    - The California Database Security Breach Act (2003)
    - Children's Online Privacy Protection Act of 1998 (COPPA)

Importance of Information Security

- Maintaining Productivity
  - Cleaning up after an attack diverts resources such as time and money away from normal activities

Number Total Employees	Average Hourly Salary	Number of Employees to Combat Attack	Hours Required to Stop Attack and Clean Up	Total Lost Salaries	Total Lost Hours of Productivity
100	$25	1	48	$4,066	81
250	$25	3	72	$17,050	300
500	$30	5	80	$28,333	483
1000	$30	10	96	$220,000	1,293

Cost of attacks

Importance of Information Security

- Foiling cyberterrorism
  - **Cyberterrorism**
    - Attacks by terrorist groups using computer technology and the Internet
  - Utility telecommunications, and financial services companies are considered prime target of cyberterrorists

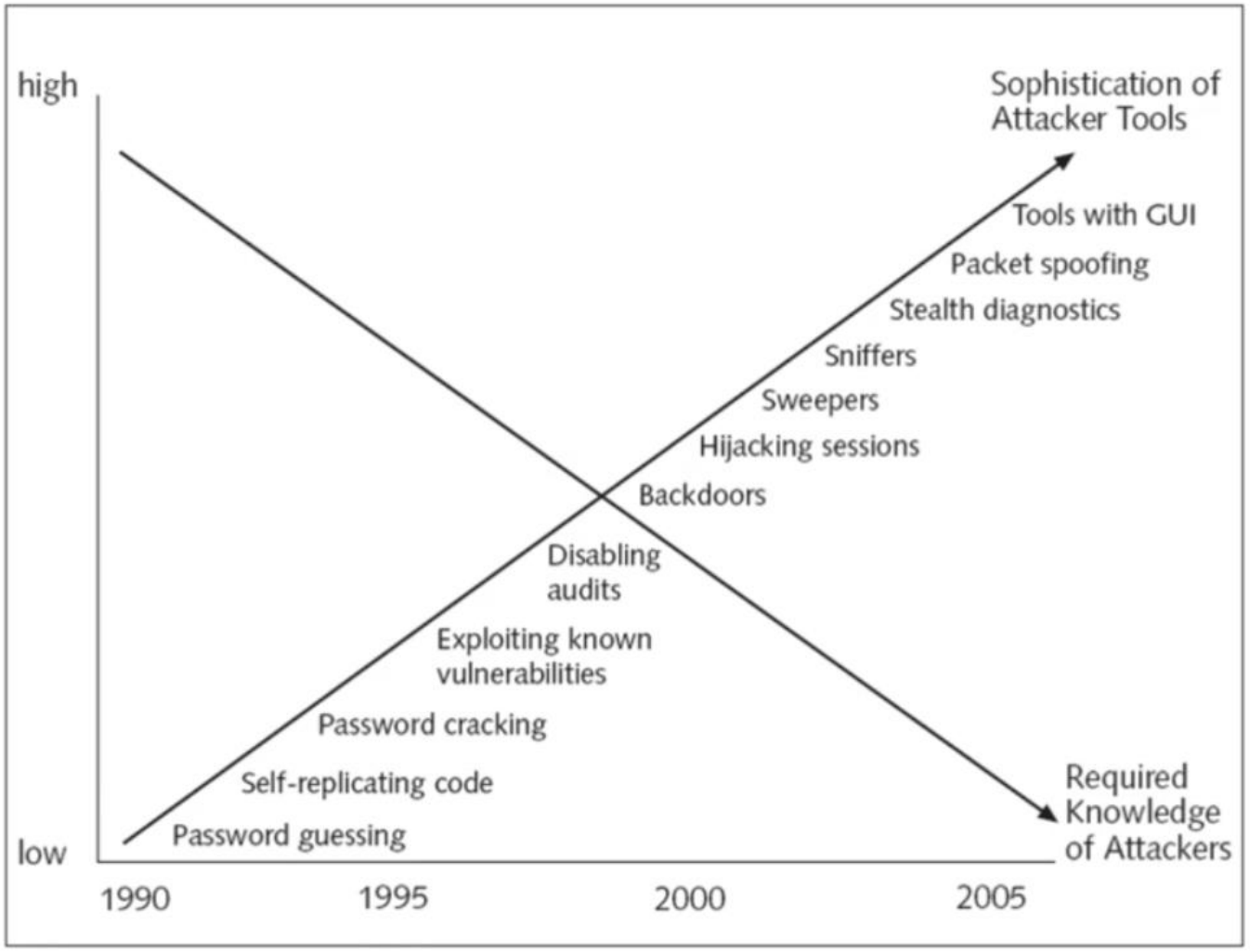
Information Assurance & Security 2

Difficulties in Defending Against Attacks

Difficulties in Defending Against Attacks

- Speed of attacks
- Greater sophistication of attacks
- Simplicity of attack tools
- Attackers can detect vulnerabilities more quickly and more readily exploit these vulnerabilities
- Delays in patching hardware and software products
- Most attacks are now distributed attacks, instead of coming from only one source
- User confusion

Increase sophistication of attack tools



Difficulties in Defending Against Attacks

Reason	Description
Speed of attacks	Attackers can launch attacks against millions of computers within minutes.
Greater sophistication of attacks	Attack tools vary their behavior so the same attack appears differently each time.
Simplicity of attack tools	Attacks no longer limited to highly skilled attackers.
Detect vulnerabilities more quickly	Attackers can discover security holes in hardware or software more quickly.
Delay in patching	Vendors are overwhelmed trying to keep pace by updating their products against attacks.
Distributed attacks	Attackers can use thousands of computers in an attack against a single computer or network.
User confusion	Users are required to make difficult security decisions with little or no instruction.

What is Information Security?

- Knowing why information security is important today and who the attackers are is beneficial.

- The tasks of guarding information that is in a digital format
- Ensures that protective measures are properly implemented
- Cannot completely prevent attacks or guarantee that a system is totally secure

What is Information Security?

- Information security is intended to protect information that has value to people and organizations
  - This value comes from the characteristics of the information:
    - Confidentiality
    - Integrity
    - Availability
- Information security is achieved through a combination of three entities

What is Security?

- System correctness

  - Good input ⟶ Good output

- Security

  - Bad input ⟶ Bad output

What is Security?

- System correctness

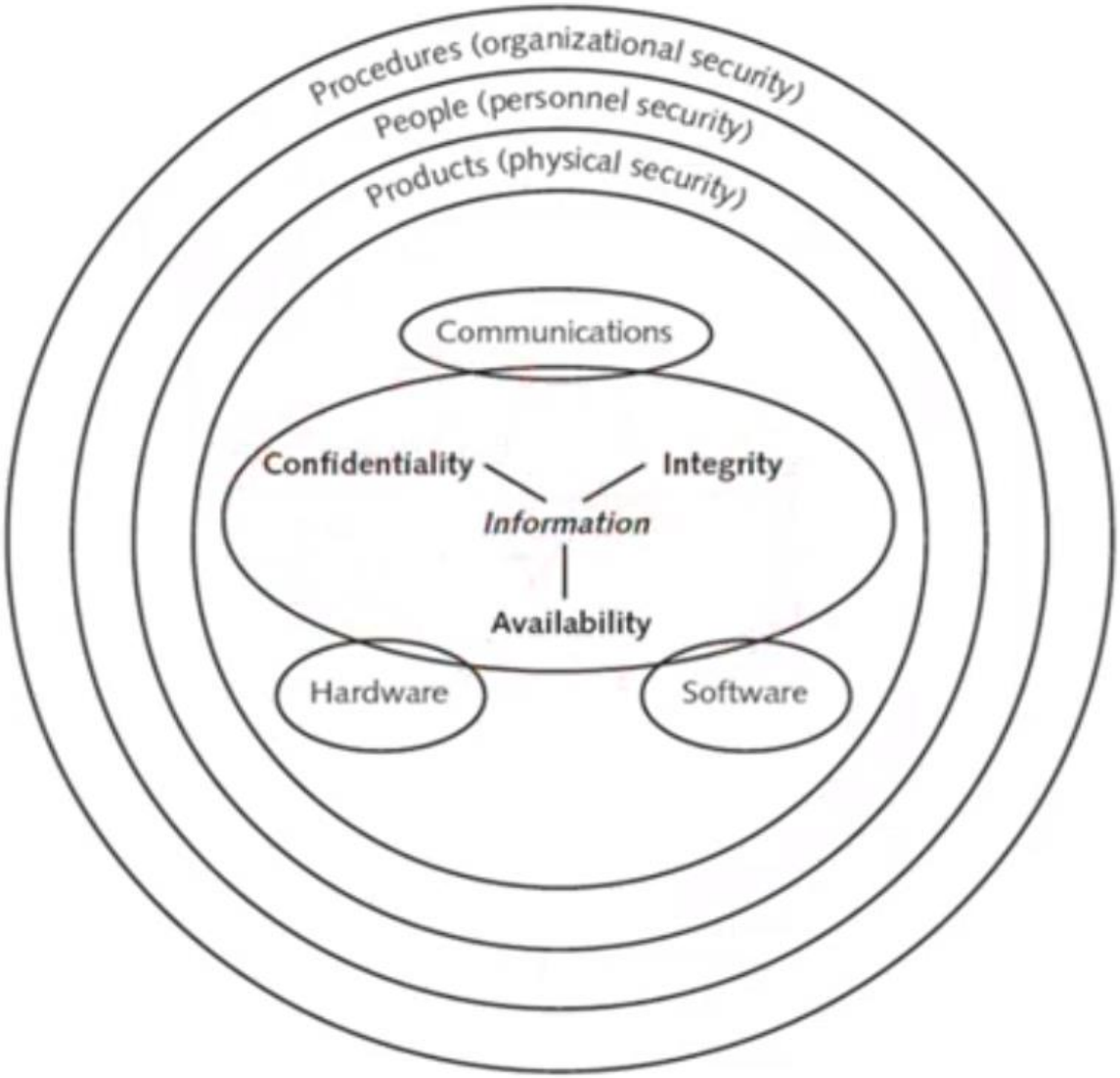
  -More features: better
- Security

  - More features: can be worse

Security Properties

- Confidentiality
  - Information about system or its users cannot be learned by an attacker
- Integrity
  - The system continues to operate properly, only reaching states that would occur if there were no attacker
- Availability
  - Actions by an attacker do not prevent users from having access to use of the system

Information Security Components



Defining Information Security

Layer	Description
Products	The physical security around the data. May be as basic as door locks or as complicated as intrusion-detection systems and firewalls.
People	Those who implement and properly use security products to protect data.
Procedures	Plans and policies established by an organization to ensure that people correctly use the products.

Information Security Layers

Defining Information Security

- A more comprehensive definition of information security is:
  - That which protects the integrity, confidentiality, and availability of information on the devices that store, manipulate, and transmit the information through products, people, and procedures

Information Security Terminology

- **Asset**
  - Something that has a value
- **Threat**
  - An event or object that may defeat the security measures in place and result in a loss
- **Threat agent**
  - A person or thing that has the power to carry out a threat

Information Security Terminology

- **Vulnerability**
  - Weakness that allows a threat agent to bypass security
- **Risk**
  - The likelihood that a threat agent will exploit a vulnerability
  - Realistically, risk cannot ever be entirely eliminated

Information Assurance & Security 2

Malware

Objectives

- Define malware
- List the different types of malware
- Identify payloads of malware

Attacks Using Malware

- Malicious software (malware)
  - Enters a computer system:
    - Without the owner's knowledge or consent
  - Uses a threat vector to deliver a malicious "payload" that performs a harmful function once it is invoked
- Malware is a general term that refers to a wide variety of damaging or annoying software

Attacks Using Malware

- Attackers can mask the presence of their malware by having it “mutate” or change
- Three types of mutating malware:
  - Oligomorphic malware – changes its internal code to a predefined mutation whenever executed
  - Polymorphic malware – completely changes from its original form whenever it is executed
  - Metamorphic malware – can rewrite its own code and thus appears different each time it is executed

Circulation/Infection

- Three types of malware have the primary traits of circulation and/or infections:
  - Viruses
  - Worms
  - Trojans

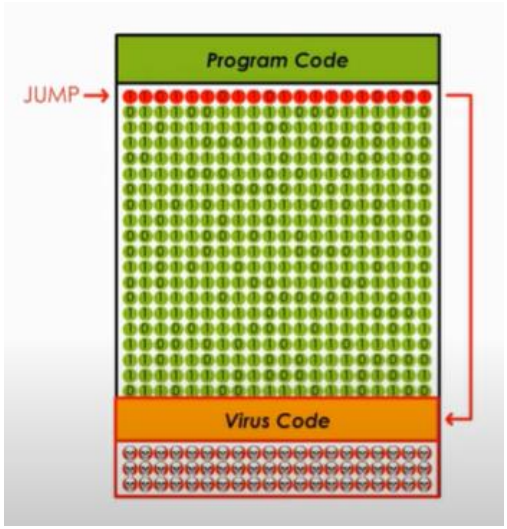
Viruses

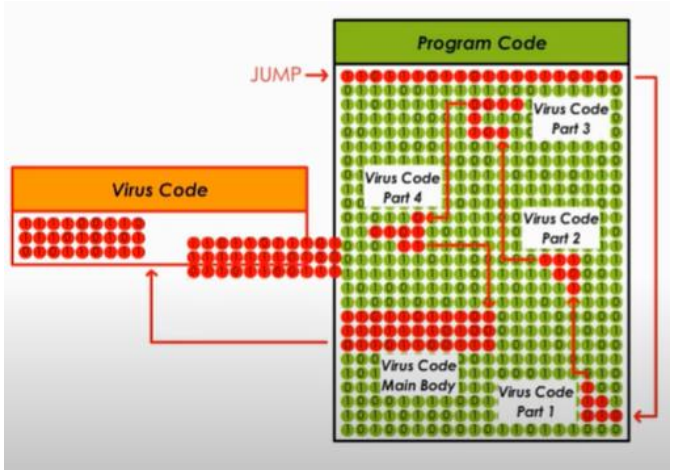
- **Computer virus –** malicious computer code that reproduces itself on the same computer
- **Program virus –** infects an executable program file
- **Macro –** a series of instructions that can be grouped together as a single command
  - Common data file virus is a **macro virus** that is written in a script known as a macro

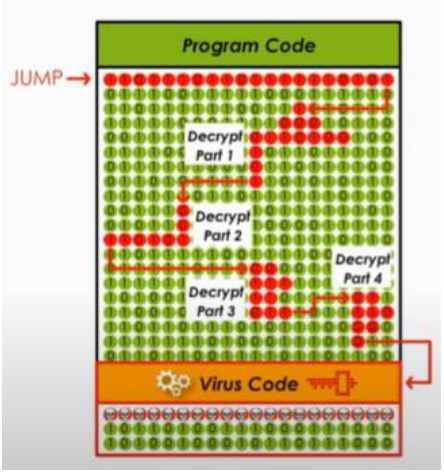
Virus Infection Methods

- Appender infection – virus appends itself to end of a file
    - Easily detected by virus scanners
- Swiss cheese infection – viruses inject themselves into executable code
  - Virus code is “scrambled” to make it more difficult to detect
- Split infection – virus splits into several parts
  - Parts placed at random positions in host program
  - The parts may contain unnecessary “garbage” doe to mask their true purpose

Viruses


Program Code
JUMP
Virus Code


Program Code
JUMP
Virus Code
Virus Code Part 3
Virus Code Part 4
Virus Code Part 2
Virus Code Main Body
Virus Code Part 1


Program Code
JUMP
Decrypt Part 1
Decrypt Part 2
Decrypt Part 4
Decrypt Part 3
Virus Code

Worms

- A malicious program that uses a computer network to replicate
  - Send copies of itself to other network devices
- Worms may:
  - Consume resources or Leave behind a payload to harm infected systems

Examples of worm actions

- Deleting computer files
- Allowing remote control of a computer by an attacker

Trojans

- An executable program that does something other than advertised
  - Contain hidden code that launches an attack
  - Sometimes made to appear as data file

Example

- User downloads “free calendar program”
  - Program scans system for credit card numbers and passwords
  - Transmits information to attacker through network