Introduction

2016-08-29

What is security?

”Security is about preventing adverse consequences from the intentional and unwarranted actions of others.”

A security system is designed to prevent adverse consequences.
i.e. a lock prevents, pin-code prevents.

Some systems such as financial audits don’t stop access / doing stuff they should not do. The intention is to lessen the loss/impact and acts as a deterrent which has a preventive effect.

Prevention

Security systems are not just a technical system but everything that is put in place to aid prevention.

- Technology -> metal detector, spyware
- People -> military, guards, police
- Training -> How to safely use a computer, how to behave in case of fire, military training.
- Procedures -> Security check at the airport, procedure for online banking authentication. Steps to follow to guarantee security.
- Etc.

Note that like any system these can be attacked themselves, can have flaws, (design, implementation, usage), can fail etc.

Safety vs Security

This is an important distinction, protection against unintentional acts is safety - not security.

Unfortunately the Swedish word for both is ”säkerhet” which leads to a lot of confusion.
Often, but far from always, the mechanisms of protection are similar.

Unintentional vs Intentional actions

Safety is often more important - ”don’t attribute to malice that which can be adequately explained by stupidity”. Unintentional.

There are a lot more unintentional acts (accidents, thoughtlessness etc.) than there are intentional ones. I.e.

- Weak password or password on a post-it
- Recent train collision in southern Italy - an evaluation error that gave the authorization to the wrong train. Caused death and large financial loss. Human error.
- Costa Concordia disaster - captain sunk the ship, caused death and large financial loss. A stupid action that escalated.

Even the intentional acts are often that thought through - can escalated as well.
The effect can escalate and produce more disasters.

- A robbery can turn into an murder
- Script kiddies and newbies can be really dangerous

Unwarranted

- Unwarranted = not justified, not authorized (that is from the point of the defender of course)
- Not necessarily illegal per se, might be immoral, in bad taste etc but doesn't have to be even that.
- DRM (Digital Rights Management) is one example, I might have the legal right to make copies for myself byt the RIAA still view me as an attacker.

Attacker

We need someone to be behind the attack, this is someone is called an attacker.
Note that this is value neutral, the attacker can be both a good or a bad guy. Some hackers are good guys, some are bad guys (white hat / blue hat vs. black hat). Good guy hackers might hack to test security.

Attacks are specific ways to break the security of the system or a component of the system.
The term can be abstract (”You can attack the house by breaking a window” or refer to a specific incident (”The 9/11) attack against the world trade center.
The object of attacks are assets; your CC number and pin, a diamond, the Swedish electrical grid and so on.

What is the problem?

There are no easy fixes for security problems .. and thats not what people want to hear. If you are worried about an attack you don't want to hear that there are no solutions for a particular problem. Research should continue to find security solutions.

Technology in and of itself won't solve anything. As a general rule, technology enables things, we're trying to prevent things from happening, that's not quite the same thing.
technology can solve a lot of other problems so it's tempting to address security problems with technology as well.
That means that technology often doesn't do what we expect (or want) when applied to security.

Poor security is worse tan no security.
Time and money could have been better spent on security that works, or the ”improvement” might make us ”less secure” or less safe, (bars on windows vs fire).

The five step program

Schneier uses the following five questions to help evaluate a security system, technologies or practices.

They might seem trivial and they are, but the answers are often far from trivial. The questions help identify all the possible solutions.

1. What are assets you trying to protect
2. What are the risk to those assets
3. Howe well does the security solution mitigate those risks
4. What other risks the solution cause (may introduce other things)
5. What costs and trade-offs does the security solution impose

Step 1. What assets?

An asset is the object of the attack

We must ask ourselves / our customer
- what assets do you have?
- what are they worth?
  - To you?
  - To the attacker?
  - Note that these values are often different and can lead to attacks; expensive to you, cheap to the attacker
  - Example pictures on cellphone (high value for us, no one else cares -> ”cryptolockers” / ransomware)

We must set the scope of the problem -
It’s just as important to make clear what you don’t protect as well as what you protect.

Step 2. What are the risk to these assets?

This is about the need for security. What is being defended? Who is potentially an attacker of our assets? Could be a private human being, a company, the government.
What are the motives? To make money, region, politic, ethics…
What are their resources?
How much money and how much time do the attackers have?
How many people are involved in the attack, a single attacker? an organization?
What are the consequences of an successful attack? What is the loss for the attacked?

Step 3. How well does the solution mitigate those risks?

A simple enough question but often overlooked by someone that has something to sell - the power of the solution. How well does the security solution work, not only in isolation but as a piece of the bigger puzzle. It doesn’t make sense to have bullet proof glass with a weak door and no alarm system. Also, not only how it works but also how it fails. For example, in computer security we have attack prevention and response systems. The second enters in action if the attack succeed. An additional system. A response mechanism. ”Detection and response”.

Step 4. What other risks does the security solution cause?

Address the problem of unintended consequences.
Most security solutions have ripple effects and most cause new security problems. Understand these problems and make sure they are smaller than the old ones. I.e. if you hire a security company to watch your house (perhaps via an alarm) but now you have a guard that have access to your house, what’s to say they’re not crooked? This is a question you must have an answer to.

Step 5. What costs and trade-offs does the security solution impose?

Everything costs something, if not money, then:
Convenience, time, comfort, loss of personal privacy.

Five steps: summing up

Note that these five steps don’t lead to the answer but rather provide the mechanism to provide the answer. The main question: is the added security worth it? Are the benefits of mitigation worth the cost, additional risks and trade-offs? This can be very hard to quantify, in fact we often can’t even begin to quantify it.
Note that these questions are easy to state but hard to answer. I.e. what are the risks? Can we even in theory know about all of them? The unknown unknown, that which we do not know and do not now we do not know. This could generate disasters.

Security trade-offs are subjective

Subjectivity

Security tradeoffs are subjective we accept different risks (in different situations).
How do we protect against air plane hijackings?
Easy, just ground all air craft?
Pretty extreme and we normally don't think the trade off is worth it.
However, within 2.5 hours after 9/11 the FAA grounded all commercial flights within the USA.
This was arguably a reasonable response given the circumstances - the FAA didn't know what was going on, the rule book had just been changed, grounding all aircraft, while extreme, could be justified.
Another example is the Air travel disruption after the 2010 Eyjafjallajökull eruption in Iceland. No one would take the risk. The decision was taken because in theory the ashes could destroy the engines. Could lead to potential disaster - so they were shut down.

However, extreme trade offs are easy
Scared about credit card fraud?
Don't own a credit card
Scared about your car being stolen?
Don't own a car
Scared of being mugged?
Live on a deserted island.

That extreme measures are not a workable solution. This is often forgotten when we're dealing with (new) technology.

Trade-offs. There is of course also a cultural component. In Sweden it's not believable to have credit card system that allows people to steal (fraud). Prevent anti social behaviour. In the USA - aah, never mind, we'll make more money accepting a 3% loss than we'll save by preventing it, just accept the loss and move on. Refund the money - let it happen.

The trade offs aren't up to you.
Laws and regulations might mandate a certain level of security - air port security is one example.

Laws and regulations might forbid certain security techniques - tear gas spray in Sweden (but not in the US).
If not laws then e.g, insurance companies might mandate a certain level o security or certain measures - if you have valuable paintings you can't get insurance without an alarm system.

Trade offs aren't worth it.
It's not lack of security methods, procedures and technology, it's that it's often not worth it.
Strip search all passengers - no-one flies. Remove all fitting rooms from shops - customers go elsewhere etc.

How do you evaluate and make sensible trade-off about security in your life? Locking your bike, etc. Write down a list of your ”security problems etc.”.

Risk vs threat

In security we men something special when we say ”threat” and ”risk”
That are overloaded terms and not all people mean the same things.

For security experts a that is a potential way an attacker can attack a system - theft, robbery, fraud.

Risk takes bot the likelihood of the threat and it's consequences into account. It is formulated as the product of likelihood and consequences. R = F * C.
If you suffer a theft of 500kr once every two years, your risk is R = 500 * 0.5 = 250kr. A security measure might cost more and wouldn't make sense.

This means that even though the threat carries grave consequences, but most often the likelihood is so remote that the risk is still negligible. I.e. an attack on your home by a paramilitary group - not likely to happen and might therefore not be worth to protect against.

However, we're not that good at evaluating events that don't happen relatively often. I.e. what's the likelihood of nuclear meltdown? 1 in 1000000 per year? How do we know that? What did TMI (Three Mile Island) and Chernobyl do to your assumptions? If there are a lot of samples, an estimation of probability can be made.

Risk management

This is an area and industry all to itself and one that s well known in banking, insurance etc.
Note that we can never eliminate the risk, and even if we could, that would be too expensive, we're trying to reduce the risk to manageable levels. A door lock doesn't eliminate burglaries, but it makes them somewhat less likely.

Insurance is a interesting risk management tool. It allows a business to take a risk and, for a fee, pass it off to someone else (insurance company)

It's a great tool in many other situations. Mainly security situations where the odds are easy to come by and we can give a value to the asets and the consequences of the attack. If the problem is hard to solve - a risk that cannot be predicted - insurance won't cover it (force majure).

It's just not much of a tools for us in computer security - since we can't tell what the risks are or how likely they are.

Security must balance the risk

Adequate security at a reasonable cost. In general, Business want to maximize their profits - a problem. They want to earn more money.

Balancing the risk and trade-off are the point of the five-step process
Step 2 determinerisk
Steps 3 and 4 find possible solutions
Step 5 evaluates the trade-off. We try to balande pros and cons.

Is the added security worth the trade-off?
This is risk management and tell us what countermeasures are reasonable.

Risk evaluation is subjective.
We're not rational when we talk of risk
Some risks are not worth it to some people no matter what
Nuclear Power
Terrorist attacks
Torture
Death penalty.

Perceived risks vs actual risks

We exaggerate spectacular but rare events and downplay common risks
Earthquakes but not slipping in the bathroom.

Terrorism not street crime - latter claims far more lives.
Poisoned candy at Halloween (no recorded instance).

We have trouble estimating risk for situations that aren't exactly like our normal situation.
Foreign city is perceived as more insecure than home. Europeans perceive US as full of guns. Men underestimate risk for unaccompanied woman.

Personified risks are perceived as greater than anonymous risks.
"A single death is a tragedy, a million is a statistic"
News always chase the human interest story, we will identify with that - 9 people trapped in a mine
Osama bin Laden was the face of Al Queda - and valuable to te opposition as such.

When people voluntary take a risk they tend to under estimate it, when they have no choice but to take the risk (and no control) the tend to overestimate it.

Eg.g Airplane vs car -Pilot vs you driving (even though pilot is probably better at flying than you at driving).

Terrorism is scary because it is a bolt out of the blue.

Domestic violence.

We overestimate risks that are being talked about (availability heuristic - recent events are overestimated - the perception).
News media skews our perception. Every air plane crash is headline news. Automobile accidents not so much. In US equivalent to a ful 727 crash every day and a half.
In Sweden, every single rape assault is reported in the news. These are probably only 1/10 of date rapes and 1/100 domestic rapes.

We tend to have more fear to what is an anomaly.

2016-08-31

Security trade-offs depend on power and agenda

Security is not always the first priority - subjectivity. When more actors are involved in the security decision there'll be someone with more power then the rest.

Many players with their own agenda

If the problem is complex many actors will be in on decision-making. Each one has a subjective perception of risk, tolerance for living with risk and willingness to make various trade-offs.

Security decisions are taken considering the players' agenda. Making trade-offs, personal analysis of the security problem, internal and external non-security considerations.

Agenda does not always contemplate security
Why wasn't lighters and cigarettes banned from flying when tweets were? The tobacco lobby is much stronger than the tweezer lobby.

Show you do something for increase security - will you reelect government official doing nothing to improve security?

Don’t influence too much flight schedule
Airlines companies are not willing to reduce the number of flights and number of passengers. Therefore security check must be done in a reasonable time. Cannot take too long - be too secure (trade-off)

Example of Post 9/11 in the airline security problem:
Government, airlines, tobacco corporations/lobby, public/consumers, food/drink corporations/lobby, pilots union, flight attendant union.

Food/drink corporations had a chance to earn more money (don’t allow drinks) - need to buy
Pilots union, increased risk - higher pay?
Everyone has their own agenda.

Security policy

When you set up a system, you set up a policy.

Who is authorized to do what?

The policy will be aimed at ”preventing adverse consequences from the intentional and unwarranted actions of people”

Someone has to set it and decide what an unwarranted action is (what is allowed and what is not) - often it is the asset owner who decides. Everyone else is obligated to go along with the definition.

All security need to be studied in term of two facts:
Agendas defining policy (who will make money - who wants what)
Players will gain and lose (some will have more or less power)

Complexity of security policies

A policy can be straightforward (a simple security policy):
You can control the basic security policy to your house
You can control the basic security policy of your computer / cellphone
A company can control who is enable to access buildings and offices, who has power to sign, who keep the company’s books etc.

A complex policy:
When no sole player has control over the system.
The credit card system; it involves customers, merchants, banks (issuer, customer, merchant), the credit card company and the government. No player has full control over the system and there is not only one system - many systems.

A cloud provider; it involves customers and their assets, the provider assets, the credit card system (or other payment system), the government etc.

No one have the full control of the system.

Proxies

A player who act in the interest of other players.
Neither you nor the airline nor any of the other players of airline security get to decide about security. But a government proxy is supposed to take every player’s agenda in account and should make the decision.

Proxies are necessary, we can't all master everything all the time, we are a specialized society - this is never more true than when computers are involved.
Government rely on consultans companies that made risk analysis's and propose security solutions.
You probably will rely on an agent to evaluate the structural integrity of a house you are going to buy - someone who is used to solve a problem.

The problem: the proxy has an agenda and own priorities.

Proxies almost never make the same decisions that you would, the have the most profound impact on security choices, greater than technology: the proxy has its own agenda, priorities and goals.

Security is complex because it includes subjectivity, agenda, power.

The security theater

Security measures should provide the feeling of security in addition to the reality

If there is a security problem (i.e. terrorism or malmware) - you want to feel that there is security put in place to solve the problem. It doesn't have to be aligned with the real security need.

Some countermeasures provide the feeling of security rather than actual security itself.

The theatre can be pu in place because the player's agenda does not contemplate real security. And sometimes it's more expensive to have a theatre than to solve the actual security problem.

Examples:
Air port security to a large extent is security theatre. You are "safe" when you fly - but terrorism is not solved.
The agenda of the proxy that decides includes being seen to do something (doesn't matter what). Come up with a solution ever though it doesn't really solve the problem.
Some form of antiterrorism that now are put in place in big cities - military walking around with guns and rifles. They might not have bullets (are useless) - a theatre.

It's not completely useless, it can relieve anxiety but you have to believe in it.

Externality and security

"Externality" is borrow from economics

An externality is when security doesn't make economic sense for you, since someone else will have to bear the cost of failure. Most of our environmental problems stem from this, it doesn't pay for the company to clean up their act since the consequences of pollution is suffered by someone else (or at least shared between everyone, including the company).

If you want to make a security system that works - make sure there ar no externalities.
The ones that are interested in the consequences and have to bear the cost are also the ones who can affect the likelihood. If you do then, economic and other interests will align.

Security is a state of mind, security is a process , it is not a product. All security involve trade-offs, trade-offs are subjective. Risk = likelihood * consequences. Everybody makes those trade-offs differently (proxies).

Covered:

Chapter 1-3 in the course book.

Computer security

Chapter 1 of the book (security in computing - available online at BTH library)

Check slides!

Historically security has been about the protection of physical assets from real physical enemies or bad guys. Traditionally security deals wit these actions:

Prevention (locks, doors)
Detection (burglar alarms)
Response / recovery (dial 911, replace locks - what happens after)

During recent years, information security has gained a lot of space and attention. It's an important area of R&D (research and development)

Why is it important?

There are many reasons:
Our society seamlessly rely on computer and digital communication systems (internet)
Computer systems get more complex
More and more systems interrelate with each other
Critical infrastructures (energy, control of water quality, railway, airway) are computer-dependent
Information as an asset increasingly important - the laptop might be stolen or destroyed but we care about the data on the laptop
Financial and government interests
Rising terrorist threats

Definition

"Computer security is the protection of the items you value, called the assets of a computer or computer system"

There are many types of assets, involving hardware, software, data, people, processes, or combinations of these. To determine what to protect, we must first identify what has value and to whom.

"Computer security deals with the prevention and detection of unauthorized actions by users of a computer system"

Don't forget the wise words: "Security is a process, not a product". An anti-virus

What does it mean to protect a computer / information?

Preserve and mention the following system properties:
Confidentiality (Data - not all data should be accessed by everybody, read/write access)

Integrity (Data, systems and services (applications))
Availability (Data, systems and services (applications))
Accountability (Actions - identify who did what - who was responsible of the attack?)
Nonrepudiation (No one should be able to deny what they did)
Reliability (Systems, services)

The properties must be maintained both in case of intentional or unwarranted actions

CIA triad - or security triad

The three most important terms.

Confidentiality: Prevention of unauthorized disclosure information
- Only authorized people or systems can access protected data
- Keeping data and resources hidden
- A good example is cryptography

Integrity: Prevention of unauthorized modification of information
- Data integrity (integrity)
- Origin integrity (authentication - who accessed the system)

Availability: Prevention of (unauthorised) withholding of information or resources
- Enabling access to data and resources
- In other computer science area this property relate to ”quality of service - QoS”

CIA is a common definition of security.

A security control in a computer system is the result of a balanced combination of the three terms.

Implying there are trade-offs between them.
- Trade-offs: cost: performance, usability, etc

Confidentiality

Some people feel that the main objective of computer security is to stop unauthorized people from accessing sensitive information.
This means that confidentiality deals with unauthorized reading.

Problem:
Who determines what people or systems are authorized to access the current system? By accessing data, do we mean that an authorized party can access a single bit? The whole collection? Pieces of data out of context?

The authorization to access the data / system is given by three elements:
Who can access, **how** can we access and **what** can we access?
Who, how and what defines an access policy.

Can you identify any confidentiality threats?

An unauthorized person can access a data item and reveal it: WikiLeaks.
Un unauthorized process or program access a data item: Spyware.

Integrity

Definition:

”The state that exists when computerized data is the same as that in the source document and has not been exposed to accidental or malicious alternation or destruction”

In other words, making sure that data is just as it is supposed to be.

This means that integrity deals with unauthorized writing of data.

Integrity is also a prerequisite for other security mechanisms, i.e. an attacker might try to circumvent an confidentiality control by modifying an OS - violate the integrity.

Preserving the integrity of an item may mean that the item is:
precies / accurate
unmodified
modified only in acceptable ways
modified only by authorized people
modified only by authorized processes
consistent
internally consistent
meaningful and usable
(or more)

Can you identify any integrity threats?

A malicious macro that change the content of a word document
A computer processor that in certain circumstances generate incorrect results when doing floating point operations.
When you type ”<space> 123” in a numeric excel cell, excel transform it in character and the spreadsheet generate an incorrect result.

Availability

”The property of being accessible and usable upon demand by an authorized entity”

In other words, ensuring that unauthorized users cannot prevent legitimate users from having access to their systems.

Check slide

There is a timely response to our request.

Resources are allocated fairly so that some requesters are not favored over others.

The service or system involved follows a philosophy of fault tolerance. Hardware or software faults lead to graceful cessation of service or to work-arounds rather than to crash and abrupt loss of information. Cessation does mean end; whether it is graceful or not. Ultimately the system is unavailable. However, with fair warning of the system’s stopping, the user may be able to move to another system and continue work

The service or system can be used easily and in the way it was intended to use. This is a characteristic of usability, but an unusable system may also cause an availability failure.

Can you identify availability threats?

A common threat to availability is a so called DDoS or DoS

CIA summary

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) and an availability. Check slide.

CIA - another perspective

The nature of the harm caused to assets
Security harm can be caused by four acts:
interception - access the medium used to transfer data
interruption - stop the flow of data (availability)
modification - modify data
fabrication - make completely fake information - look realistic

Confidentiality can suffer if someone intercepts data
Availability is lost if someone interrupts
Integrity can fail if someone modify or fabricate data

Thinking of these four kinds of acts can help what threats exists against the computers you are trying to protect

Accountability

We have to accept the fact that we hardly ever will be able to prevent all improper actions since:
some of our authorized actions can lead to a security violation - system admin who makes an error (knowingly or not)
Our security system might include flaws that allows an attacker to circumvent our controls

Therefore we introduce accountability, so that users can be responsible for their actions

Therefore the system has to identify and authenticate users and keep an audit-trail of security-relevant events.

Nonrepudiation

Nonrepudiation provides a way to tell if something really has occurred

Usually cryptographic signatures are used to handle this

Examples include nonrepudiation delivery (check slide)

Reliability

Specifies that a computer system must be able to function correctly even when it is executing in adverse environments

Mainly deal with accidental failures - safety not security

Safety = accidental failures
Security = intentional failures

The vulnerability - threat - control paradigm

Vulnerability: is a weakness that could be exploited to cause harm
Threat: is a set of circumstances that could cause loss or harm
Controls: prevent threats from exercising vulnerabilities.
Check slide

What is an asset?

Check slide

There are loads of data. What data should be protected? How long could the business survive when the asset has been damaged?

Vulnerabilities

Simple passwords
Programs with unnecessary privileges
Programs with known flaws (bugs)
Weak configuration (easier to setup)

There are automatic vulnerability scanners that identify some vulnerabilities but only those known by the developer of the scanner.

Computer vulnerabilities (from 1970) - check slide.

What is a threat?

Threats are actions that are carried out by attackers who try to exploit vulnerabilities to damage assets.

Common threats in a computer include:
Spoofing (the attacker pretends to be somebody else)
Tampering: security settings are changed to give an attacker more privileges
Repudiation: a user denies having performed an attack
(Check slide)

Difference between threat and vulnerability

Check slide

Control (or countermeasure)

Is the means to counter threats
Harm occurs when a threat is realized against a vulnerability. To protect against harm, then:
neaturalize the threat
close the vulnerability
or both

We can deal with harm in several ways:
prevent it by blocking or fixing vulnerability
deter it by making the attack harder
deflect it by making it less attractive
mitigate it by making its impact less severe
detect it as it happens presume time after
recover from it

Effects of control

check slide

Public key encryption

2016-09-07

Chapter 2 section 3 in ”Security in computing”
Chapter 8 in introduction to security

Asymmetric, i.e. different keys for encryption and decryption

The public key is only used for encryption. Anyone who want to send you a message uses your public key. You decrypt using your private key.

One of the keys cannot be derived (retrieved) from the other.

Built on mathematical functions that are easy to compute in one direction and hard to compute in the other.

Integer factorization of probe numbers is one such example.

It solves the symmetric cryptography problem - it ensures that people can exchange keys without trusting the media.

Problem: MITM can replace public key with his own

Problem: Asymmetric cryptography is slow. Use it to exchange symmetric keys

Rivest and Shamir protocol (1984):
A -> public key -> B
A <- public key <- B
A -> symmetric key -> B’s public key -> half message -> B
A <- half message <- A’s public key <- random <- B
A -> other half -> B
B puts together both halves (decrypting with private key) and obtains the symmetric key.
A <- other half of number <- B
Amy puts together the random number, decrypts using private key. She can encrypt this number (that only bill can have created)
A -> sends encrypted number (using symmetric key) -> B
B compare the random number with the one he generated. Correct? Good connection

Examples: PGP (Pretty Good Privacy) S/MIME

RSA

Public key cipher

Invented by Raves Shamir & Adleman (1973)

Rests on the problem of factorizing large prime numbers

Is an exponentiation cipher and uses heavy modular arithmetics

Problem: be able to check the integrity.

Cryptographic checksums

Also called hash functions
Does not use any cryptographic keys
A one-way mathematical function
Mathematically irreversible
Outputs a hash

Problem: can collide

Digital signature

Chapter 2 section 3 in ”Security in computing”

”A digital signature is a construct that authenticates both the origin and the contents of a message in a manner that is provable to a disinterested this party.”

Example
A wants to send 100$ to B
Bank must be able to prove that A is the one who wants to send money. Non-repudiation - she cannot deny that she sent the message.
Bank wants to know that the message is entirely from A - not altered along the way. A will know that bank cannot change document (add more money). Authenticity - A wrote it.
Both A and Bank want to know that the message is new and that it is not reused.

A digital signature must be *unforgeable*. No one else should be able to replicate it.
It must be *authentic*. B must see that A is the only one who could have created the message.
It is *not alterable*. After transmitted, messaged could not be changed by anyone.
It is *not reusable*.

Use both public and private key but in a reverse order, i.e. encrypt with the private key and decrypt with corresponding public key. Only A could have created the message.

Check slide ”Putting it all together” & ”Putting all together: the process” & ”Tools Derived from Cryptography”

Monday: key management. Crypto analysis. Break the crypto. Chapter 8 in ”Introduction to Computer Security”

Read laboration 1. Lab 1 on Monday? Submit online. Write a report.

F4 - Systems, attackers & attacks

2016-09-19

Chapter 4-5-6 of book.

Systems

What they are and how they work, esp. security systems.

Security questions escalate

An example of a bank that want to protect money. To protect the money - install a vault to make it more secure.

Problem: protect money in the bank.
Solution: vault.

Problems:
Who knows the combination?
What if they quit or get sick or die?
Who puts money into, or takes money out of the vault?
How much money is there in the vault?
Who checks the vault?
Who keeps track of the money?
Are there safety deposit boxes in the vault?
Can customers access these boxes all by themselves?
Can they put what they like into them?
Who installed the vault?
Do the installer know the combination?
Is there an alarm system?
Who responds to the alarm?
Who gets to decide if it's a false alarm or real one?
-Questions that generate more questions.

Security is a system itself - not only about the asset or threat.

Security is complex

Security is a complex system that interact with itself, the asset being protected, and the surrounding environment. There are weak points - usually the interaction between systems. Interaction with asset and so on. An attacker usually targets these interaction points. I.e. when you move gold from the vault to another vault. The attacker attacks the truck transporting the gold -> when two bank systems interact.

Systems

A system is a collection of simple components that interact to form a collective whole. The single component of the system itself is meaningless - but when they interact with one another they make the system.

There are several complications:
Systems can become very large and complex.
They interact with each other in mysterious and unforeseen ways.
Even with other types of systems, political, economic, social etc. A security (software) system that interacts with physical systems like a social system.
Adding security to anything require a system.
If you want to understand security, you have to think in term of systems.

Security systems

Security is a system of individual countermeasures and the interactions between them. It shares the traits of other systems.

Not the bank vault, for example, the lock is a complex technical system, the handling of the money is a complex economical and financial system and the vault interacts with it etc.

Interactions are inevitable
There are intentional, unwanted and unforeseen interactions.
Prevent unwanted interactions - they are not desired. By design they should be prevented.
Unforeseen interactions are things no expected - they are the most critical. In the analysis of the system these interactions were not considered - the system can fail (electricity and so on).
Interactions produce so called emergent properties, or unintended consequences. For example bank vaults. They led to robbers taking bank managers families' hostage and force the manager to give to combination - which led to time locks.

Security systems are different

We want to protect a system. Typically a system is designed to do something (data center provides computational power and storage, power grid provides electricity). Security systems are designed to prevent somethings. It's not about what gets done, but about what gets prevented. Security systems are useful for what they don't allow to be done. Security engineering involves making sure systems don't fail. Security engineering care more about failure than correct operation. Interesting failure - real ATMs contain many ways to make sure you can't steal card numbers or pins. So attackers installed a fake ATM instead. They didn't think someone would create a fake ATM - failure.

Safety and reliability engineering ensure performance in face of failures. Safety systems only have to take random occurrences into account (that can be, at least, statistically modelled) we have to take intentional malicious occurrences into account (these cannot be statistically modelled).

Main difference:
Security systems account of the presence of an intelligent and malicious adversary (user) who force faults at precisely the most opportune (gaining) time and in precisely the most opportune (best for them) way.

Difference among safety and security

1. Fire stations
    1. Safety: set the proper number of fire stations in a town
    2. Security: a pyromaniac set more fires than fire stations can handle. He knows where to start a fire and how many he should light for the stations to be unable to cover all.
2. Knives
    1. Safety: accidentally left knives in a luggage. It is easily recognizable and they will remove the knife.
    2. Security: an attacker try to sneak a knife fabricated in am material that is hard to detect. It can be assembled in many parts and be reassembled later. An intelligent mind that wants to break the system.
3. Fire exits
    1. Safety: calculate the right number of fire exits.
    2. Security: attackers barricade fire exits

Main difference:
It's the presence of an adversary that make the difference

Cascading failure

Producing failures that potentially is very far from your target, but it allows you to reach in a sequence of attacks, the target system.

Security: Systems usually don't fail all at once but failures can often (be made to) cascade.
An attacker targets a component of the security system and try to use a small failure to break the entire system. Burglar uses generic garage door opener to get access to garage and goes on into the house via the unlocked door between garage and house. Or, disable the alarm, break into the bank, then break into the vault, then break into the safe-deposit boxes.

Compare with air plane accidents, there's often a long chain of seemingly minor problems that in the end compound to a major catastrophe.

The best way to attack is i n the seams between systems. High security prisons don't change guards on a fixed easily predicted schedule. It's easier to bribe a clerk to get a "real" fake ID than forge one.

Two types of failure

Most security systems can fail in two ways.

Passive failure
    When they fail to prevent the unwanted action
        The lock is successfully picked
Active failure - the most dangerous one
    When they activate and stop wanted action
        The lock jams and now you can't get in even though you have the key

Active vs passive

Hence, passive failures are not as problematic as active failures.
Many more people are locked out by faulty locks than are picked by burglars.

Systems with many active failures, i.e. false alarms are almost always more problem than they are worth.

A system that shoots half of all terrorists, i.e. a passive failure rate of 50% is still useful - but one that shoots one in 1000 innocent passengers is bad. etc.

False alarms

Not just random occurrences.

Attackers can and do make systems give false alarm to make us even more sceptic of their performance.

"Boy who cried wolf"

Oldie; DoS a firewall to make the sysadmin turn it off as it was clearly broken

Throw rabbit over the fence of a Soviet army base in Afghanistan.

Ground motion (anti tunneling devices) detector alarms in banks rarely work - guards are tired of alarm before the tunnel is finished.

SUgar pellets against embassy window to set of alarm during thunderstorms.

All systems break sooner or later

Be prepared for it.
”When a thing that cannot possibly go wrong goes wrong it usually turns out to be impossible to get at or repair”.
Happened with the computers in the Space shuttle, but the astronauts managed to dismantle a wall and get to the computers anyway.
Practice what to do when (rare) security event occur.
Fire drills, safety demonstrations on aircraft, military exercises etc.
Shit happens, but not that often, you must train and practice.

Both training and practice are essential because real […] see presentation.

Attackers

Who they are and what they can do.

Attackers come in many shapes and have different characteristics. Motivations (anger, ideology, money).
Objectives (target asset)
Expertise (pro, non-pro)
Access (outsider, insider)
Resources (how much money and time)
Risk aversion (what the attacker is willing to lose)
Lone or part of group
etc.

Step 2 of the process for understanding security system: what are the risk of the assets you are defending?

Understanding the potential attackers is an integral part of the process for answering this question.

The one to look out for is the well funded one
He can trade money for almost anything
buy experts, bribe insiders

(see presentation).

In computer security and everyday language, a hacker is someone who breaks into computers and computer networks.

Hackers may be motivated by many different reasons.

Types of hackers.

White hat
Black hat
Grey hat
Script kiddie

so on..

White hat

A white hat hacker breaks security for non-malicious reasons, for instance to test their own security systems. Can be paid for pen-testing.

Black hat

Violates computer security for little reason beyond maliciousness or for personal gain. Destroy data, gain data, gain money

Grey hat

They might do it for fun.

Script kiddie

Non-expert who breaks into computer systems by using pre-packaged systems.

Neophyte

Starting to learn.

Blue hat

Someone outside computer security consulting firms who is used to bug test a system prior to its launch.

Hacktivist

Utilize technology to announce a social, ideological or religious thing.

Criminals

They don't have access, unless they're insiders. An employee, spouse supplier, contractor, consultant and so on. They're dangerous because they have knowledge and access. In order to stab someone in the back you frist hav etc gain their trust.

Insiders

Rare criminals but being many (most) high loss situations.
Armored car drivers and bank guards who let themselves be robbed with the help of friends etc.
Most security measures don't work against them.

And so on…

Attacks

There are no new themes, but there are new implementations

Murder, theft, impersonation, counterfeiting, terrorism, biological attacks.

The types are the same, the nature of attacks however changes.

Fraud

See presentation.

Phishing

A social engineering attack that aims at exploiting the weakness found in system processes as caused by system users. For example a system can be secure enough against passwords, but users may leak their passwords through phishing attacks.

Destructive attacks

Burnings, tagging…

Privacy

Lots to talk about. Traffic analysis

Even if you can't read the message, the fact that it was sent is sometimes bad enough.
The name of the rented video can leak enough information that you don't have to have seen it.
Nazi Germany used phone records to round up people who had talked to people they had already rounded up. Columbian drug cartels execute those in their ranks that have called the government too often.

Big problem:
Data aggregation a substantial risk. These databases will be misused by attackers or well intentioned do gooders. Government employees, outsiders breaking in, lobbyists. Note that the law is different in the US and Europe.

Progress is slow

Some attackers invent new attacks. Computers made this worse.

Cloud computing security

2016-10-17