Security design and goal

Matsuzaki ‘maz’ Yoshinobu

<maz@iij.ad.jp>

Thanks

Most contents were provided by:

Steven M. Bellovin

- https://www.cs.columbia.edu/~smb

Starting Off

- What are you trying to protect?
- Against whom?

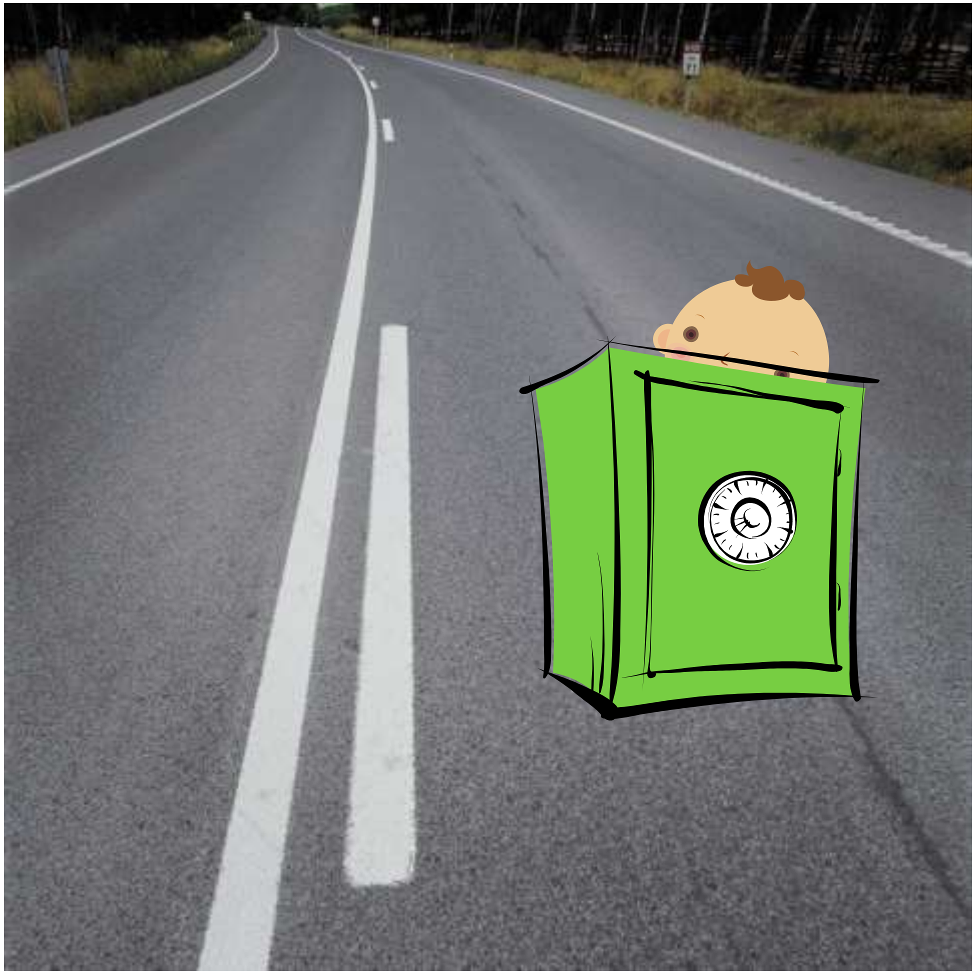
- All security system designs should start by answering those two questions.

Baby on Road

- Risk
  - traffic accident
  - rain and wind
  - kidnapping

Putting the Baby in a Strong box

- wrong solution
  - a bit safer, but
  - too ad-hoc
  - too local optimum
  - unreasonable
- baby may cry ☹



Baby at Home

- More secure
  - roof and wall
  - family
- Baby is happier ☺

Threats Modeling

Threat: An adversary that is motivated and capable of exploiting a vulnerability

- What vulnerabilities do you have?
- Who might attack them?
- Are they capable of exploiting those vulnerabilities?

Assets

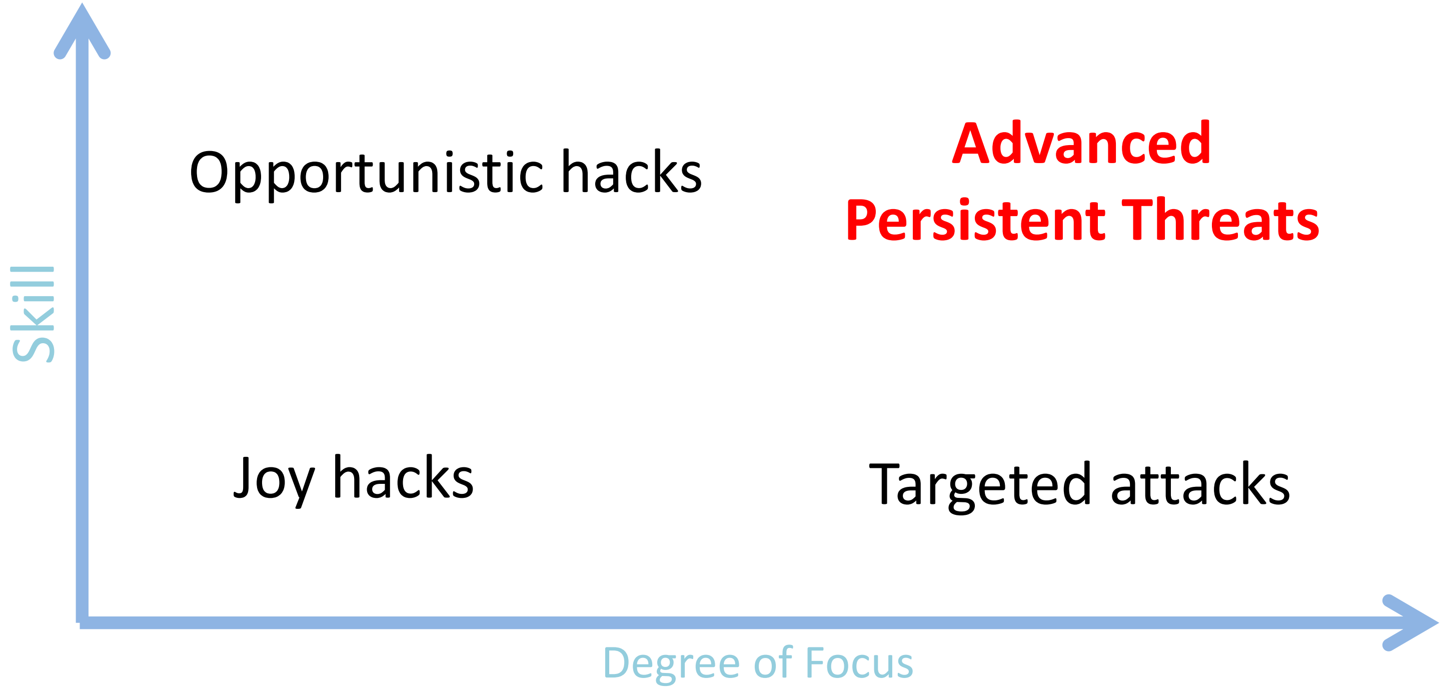
- My house has easily-breakable glass windows
- Banks store their money in vaults
- Banks have more money than I do…

(Creative Commons licensed by Flickr user mbrand)

Who Are Your Enemies?

- Script kiddies: little real ability, but can cause damage if you’re careless
- Money makers: hack into machines; turn them into spam engines; etc.
- Government intelligence agencies

The Treat Matric



Opportunistic hacks

Advanced Persistent Threats

Joy hacks

Targeted attacks

Skill

Degree of Focus

Joy Hacks

- Hacks done for fun, with little skill
- Some chance for damage, especially on unpatched computers
- Targets are random; no particular risk to your data (at least if it’s backed up)
- Ordinary care will suffice
- Most hackers start this way

Opportunistic Hacks

- Most phishers, virus writers, etc
- Often quite skilled, but don’t care much whom they hit
  - May have some “0-days” attacks
- The effects are random but can be serious
- Consequences: bank account theft, computers turned into bots, etc.

Targeted Attacks

- Attackers want *you*
  - Sometimes, you have something they want; other times, it’s someone with a grudge
- Background research -- learn a lot about the target
  - May do physical reconnaissance
- Watch for things like “spear-phishing” or other carefully-targeted attacks

Advanced Persistent Threats (APT)

- Very skillful attackers who are aiming at particular targets
- Sometimes -- though not always -- working for a nation-state
- Very, very hard to defend against them
- May use non-cyber means, including burglary, bribery, and blackmail
- Note: many lesser attacks blamed on APTs

Are You Targeted?

- If you’re big, someone is probably targeting you, especially if you’re unpopular
- If you have something someone wants -- including money -- you can be targeted
- Or it could be random chance

A Crazy Neighbor

- A family told police about a neighbor’s (serious) misbehavior
- The neighbor retaliated: he hacked into their WiFi, stole their passwords, created face pornographic MySpace pages, sent threatening and harassing letters “from” them, etc.
- Eventually, the FBI was called in because of the threats, but they found who was really doing it
- Conclusion: A family was targeted, for no rational reason

A Paint Company

- A paint manufacturer was targeted, apparently for purposes of industrial espionage
- There were hints -- or claims-- of foreign government involvement

Defense Strategies

- Defense strategies depend on the class of attacker, and what you’re trying to protect
- Tactics that keep out teenagers won’t keep out an intelligence agency
- But stronger defenses are often much more expensive, and cause great inconvenience

Joy Hackers

- By definition, joy hackers use existing tools that target known holes
- Patches exist for most of these holes; the tools are known to A/V companies
  - *The best defense is staying up to date with patches*
  - *Also, keep antivirus software up to date*
- Ordinary enterprise-grade firewalls will also repel them

Opportunistic Hackers

- Sophisticated techniques used
  - Possibly even some 0-days
- You need multiple layers of defense
  - Up-to-date patches and anti-virus
  - Multiple firewalls
  - Intrusion detection
  - Lots of attention to logfiles
- Goal: *contain* the attack

Targeted Attacks

- Targeted attacks exploit knowledge; try to block or detect the reconnaissance
  - Security procedures matters a lot
  - How do you respond to phone callers?
  - What do people do with unexpected attachments?
- Hardest case: disgruntled employee or ex-employee

Advanced Persistent Threats

- Very, very hard problem!
- Use all of the previous defenses
- There are no sure answers -- even air gaps aren’t sufficient
- Pay special attention to procedures
- Investigate *all* oddities

Varying Defenses

- Don’t use the same defenses for everything
- Layer them; protect valuable systems more carefully
- Maybe you can’t afford to encrypt everything -- but you probably can encrypt all communications among and to/from your high-value machines

All Machines Are Valuable

- Even machines with no intrinsic value can be turned into bots
  - Send spam, launch DDoS, host phishing site, etc.
  - Spy on your local traffic
  - Defense: watch outbound traffic from your site

Comparison among Targets

- Values
  - Higher is better for attackers
- Defense
  - Weaker is better for attackers
- If he values are the same, attacker may want to target weaker systems
  - You are weaker when others get safer
- Conclusion: follow BCPs and revise your procedures to keep it up to date

Case Study: Alberto Gonzales

- Penetrated major American corporations, starting with unprotected WiFi reachable from the parking lot
  - Stole passwords from login sessions
  - Used SQL injection attacks
- Stole 180 million credit card numbers
- Total damages claimed to exceed US$400 million

Lessons

- Use proper crypto
- Don’t use plaintext passwords when logging in
- Don’t make simple programming mistakes
- There generally weren’t multiple lines of defense
- No one was watching for data exfiltration

Case Study: Stuxnet

- Targeted Iranian nuclear centrifuge plant
- Used four 0-days; targeted SCADA systems as well as Windows
- Started with infected USB drive -- but unknown how that drive got into the plant
- Attackers had detailed knowledge of the plant’s equipment
- Generally attributed to the US and/or Israel

Lessons

- Someone plugged in an infected flash drive
  - An agent? (Better personnel security)
  - A few infected drives in a parking lot? (Better procedures)
- Don’t assume that air gaps and obscure system will protect you
  - 0-days were used: patches and antivirus won’t help
- Detected when someone *thoroughly* investigated some system crashes

Computer Security Incident

Any real or suspected adverse event

examples:

- Attacks to/from your network
- Compromised Host
- Account/Information theft
- Spam or IT policy violation

Needs for Response

- To limit the damage
- To reduce the cost of recovery

- An effective response benefits for organizations
  - motivation to have a specialized team to response incidents in your organization

CSIRT

- Computer Security Incident Response Team(CSIRT) provides the incident handling service for its constituency
  – may offer other related services as well

- The first CSIRT - CERT/CC was created in 1998 in response to the Morris worm incident

The Incident handling service

- a single point of contact to receive incident reports
- provides response and support to the report
- announcement to disclose information about specific attack/incident
- feedback to the report/request

building your CSIRT

- mission statement
  - what/how to do
- constituency
  - for whom
- structure
  - budget, position within organization
- relationship with other CSIRTs

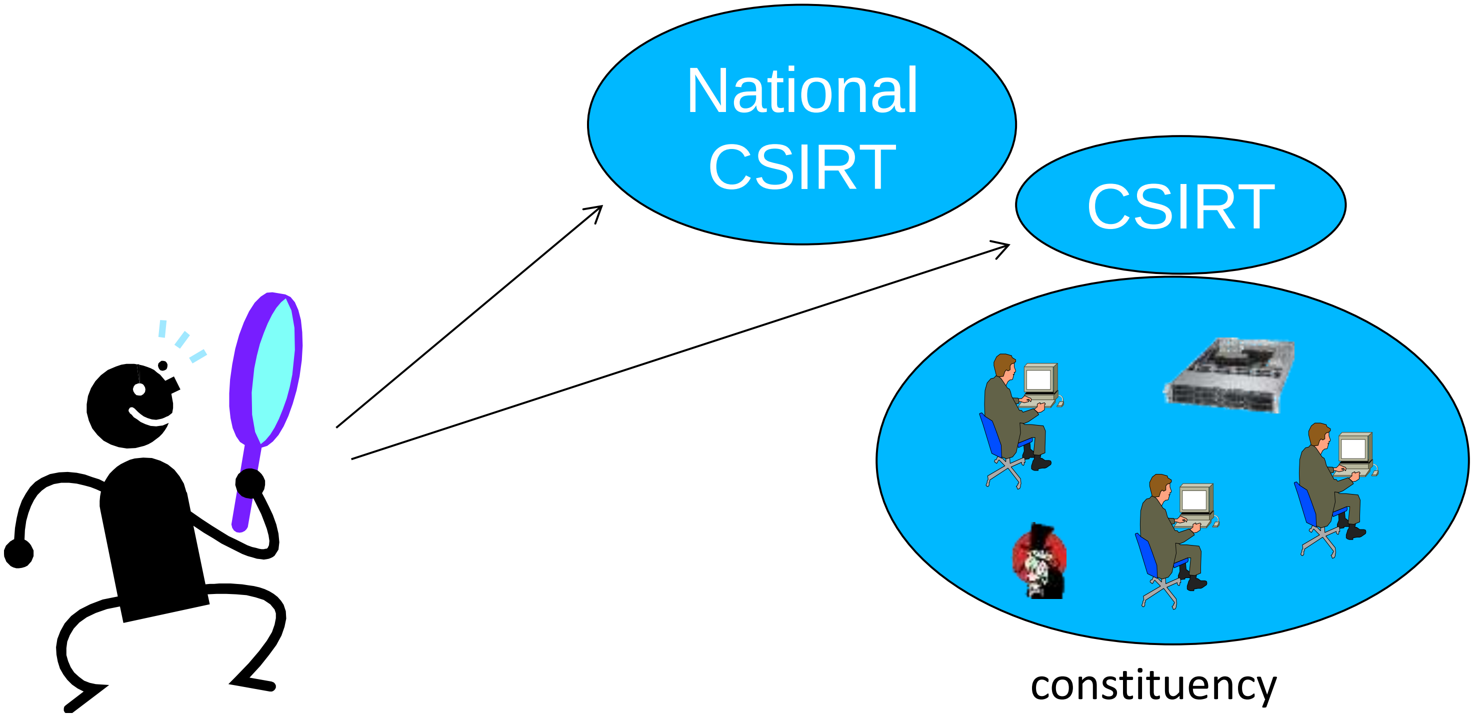
CSIRT types

- National CSIRTs
  - a national point of contact to coordinate an incident handling, reduce the number of security incidents in that country
- ISP/xSP CSIRTs
  - provide a secure environment for their customer, and provide response to their customers for security incidents

CSIRT types

- Vendors CSIRTs
  - improve the security of their products
- Enterprise CSIRTs
  - improve the security of their corporation’s infrastructure, and provide on-site response for security incidents

Point of Contact



Summary

- Use proper crypto
- Use multi layer security
  - Up-to-date patches and anti-virus
  - firewall
  - IDS and anomaly detection
- Revise security procedure
- Be ready for incidents

And again

- What are you trying to protect?
- Against whom?