Threat Models

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.

Threat 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

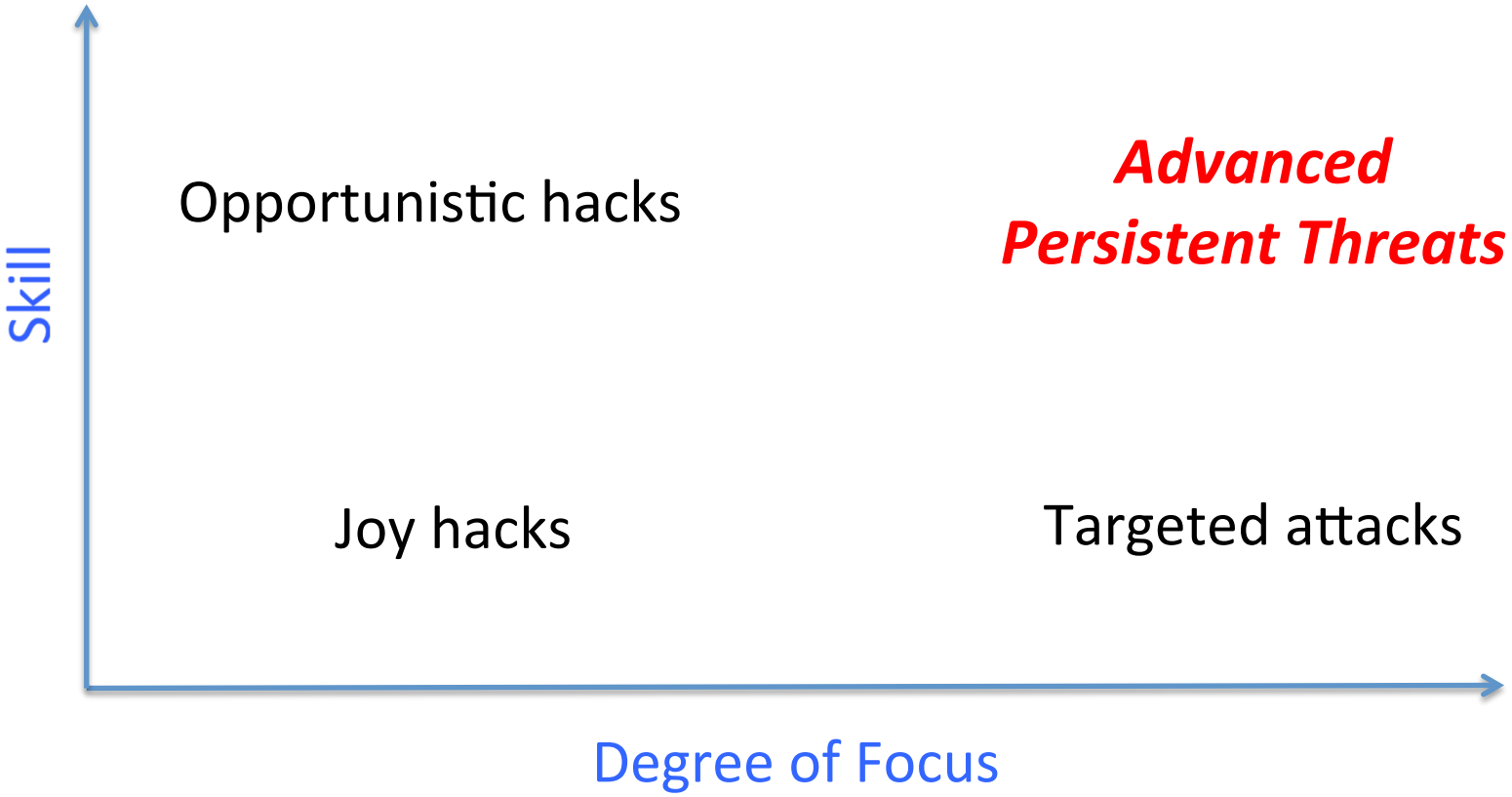
- My house has easily-breakable glass windows
- Banks store their money in vaults
- Banks have more money than I do…

(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 Threat Matrix



Joy Hacks

- Hacks done for fun, with little skill
- Some chance for damage, especially on unpatched machines
- 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, machines 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 fake 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

The Wrong Question

- “Is this system secure?”

The Right Questions

- "What would it cost to crack this system?"

or

- "What knowledge and resources would an attacker need"?

or

- "Is this system secure against an attacker with the following ablities?"

What Really Counts

"Amateurs worry about algorithms; pros worry about economics."

Allan Schiffman, 2004

Case Study: Alberto Gonzalez

- 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 systems will protect you
  - 0-days were used: patches and antivirus won't help
- Detected when someone *thoroughly* investigated some system crashes

The NSA

- Hacks into remote machines
- Hacks into remote routers and firewalls
- Intercepts mail-order systems and plants back doors
- Massive analysis of transactional data (phone call records, web logs, etc.)
- Sabotaged a cryptography-related pseudorandom number generator standard
  - Note, though, that they're better at *good* cryptography than just about anyone else—is your own design better?

Lessons

- *Ordinary commercial defenses will not suffice*
- Diversity is your friend: even an intelligence agency can't hack everything
- Home-built is not necessarily more secure; secure design and operation, of systems and components, is *difficult*
- Note carefully: it's not just the NSA and its friends; there are many other governments doing (or trying to do) the same thing