Threat Models

by Steven M. Bellovin

Jonathan Brewer
Network Startup Resource Center
jon@nsrc.org

Threat Modeling

What are you trying to protect?

Against whom?

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?

Who Are Your Enemies?

Amateur Hackers

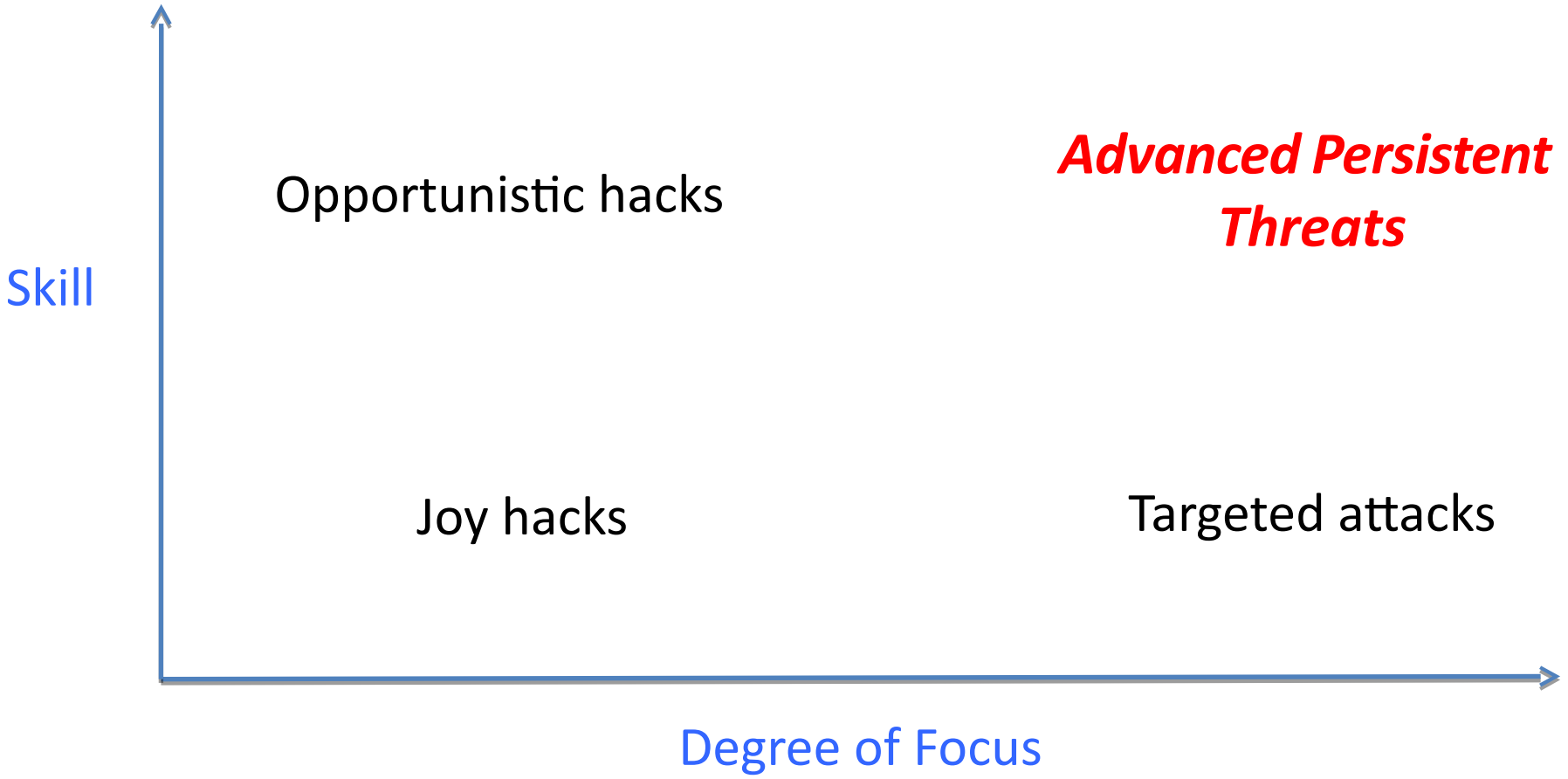
Unhappy Employees

Competitor Companies

Professional Criminals

Government or Military

The Threat Matrix



Joy Hacks

- Hacks done for fun, sometimes with little skill
- Some chance for damage, especially on un-patched 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

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: unhappy 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 abilities?"

What Really Counts

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

Allan Schiffman, 2004