Thinking Security

Steven M. Bellovin
Federal Trade Commission/
Columbia University

Security's Progress

1. There is good research on a new defense
2. Using this defense becomes a recognized "best practice"
3. It is inscribed on assorted auditors' checklists
4. A change in technology or the threat model renders it all but useless
5. It stays on the checklists… (Do you still shred your old punch cards and paper tapes?)

Technology Changes

- Single-job batch systems
- Multi-user timesharing systems
  - Mainframes; Unix; “superminis”
- Stand-alone microcomputers
  - DOS (no OS protection)
- Dial-up PCs
- Networked PCs running full-blown OSes
- Smartphones, tablets, etc
- The “Internet of things”?

I’ve used all except, perhaps, the last…

Threat Model Changes

- Joy hackers
  - "Pursuit of knowledge"
  - Manual hacking, often via stepping stones
  - Annoying viruses and worms
  - Random spread; most did little damage
- The spammer/hacker alliance
  - Worms that don't shut down the Internet; bots as payloads
- Cyberespionage
- Cyberattacks (Stuxnet, Flame, Shamoon)
- "Preparing the battlefield"?

Security Advice

- Pick strong passwords
- Use a firewall
- Run current antivirus software
- Stay up to date on patches

Security Advice

- Pick strong passwords
  - *The Morris-Thompson paper is from 1979, an era of electromechanical terminals and few logins*
- Use a firewall
  - *Smartphones, tablets, and laptops move around*
- Run current antivirus software
  - *It's increasingly ineffective*
- Stay up to date on patches
  - *What about 0-day attacks?*

Passwords (1979)

- Password strength rationale is from the days of electromechanical terminals
- No local computational capability
- No keystroke loggers or user malware
- Moore's Law change since 1978: about 4,000,000× improvement

(Picture courtesy Perry Metzger)

Passwords

- Old scenario: hacker steals hashed system password file from timesharing machine
- New scenarios:
  - Hacker steals application—not system—password file from web server
  - May be plaintext, for password recovery
  - Secondary authentication questions are jokes
  - Malware plants keystroke loggers
  - Users are lured to phishing websites

Firewalls

- Firewalls are topological barriers
  - They work best if they themselves are small and simple, and enforce a limited security policy
- A large company will have hundreds of *authorized* links that go through or around the firewall

Foresight?

"The advent of mobile computing will also stress traditional security architectures... It will be more important in the future. How does one create a firewall that can protect a portable computer, one that talks to its home network via a public IP network? Certainly, all communication can be encrypted, but how is the portable machine itself to be protected from network-based attacks? What services *must* it offer, in order to function as a mobile host? What about interactions with local facilities, such as printers or disk space?"

Firewalls and Internet Security, Cheswick and Bellovin (1994)

Antivirus

- "The antivirus industry has a dirty little secret: its products are often not very good at stopping viruses."(*NY Times, 1/1/2013)*
- Most A/V programs are *reactive*; they work by looking for signatures of known malware
- The new stuff can spread quite widely before the vendors update their signature databases
- Tailored viruses may not be widespread enough to make it into some A/V programs

Patches

- Patches are necessary, to fix known vulnerabilities
- It can take a long time produce a high-quality patch
- Despite that, production software is incompatible with new patches; testing is needed
- But—"Patch Tuesday" is followed by "Exploit Wednesday"; the bad guys reverse-engineer the patches

Where Did We Go Wrong?

- Static advice
- Static advice to use static defenses
- Dynamic, adaptive adversaries in a world of rapidly changing technology

"Life is a dynamic process and can't be made static. '—and they all lived happily ever after' is fairy-tale stu—" (Robert Heinlein, *Sixth Column* (1941))

How Do We Improve?

- We cannot predict important new applications
- We cannot predict radically new devices, e.g., smartphones
- We cannot predict new classes of attacks
- We can make decent projections of improvements in CPU power, storage capacity, and price
- Is that enough?

Sometimes, Raw Power is the Threat

- One major threat to DES was brute force; this has been known since 1979
- It happened, though later than forecast by Diffie and Hellman
  - Their analysis said $20,000,000; straight-line Moore's Law would make that about $5K in 1997
  - The actual cost was about $250K
- But—we cannot predict cryptanalytic (or any other) *breakthroughs*

What Are Our *Assumptions*?

- Most security mechanisms rest on *assumptions*
- Often, these are implicit, and are not recognized even by the architects
- When our hardware, software, or usage patterns change, our assumptions can be invalidated
- But—since we never wrote them down, we don't know to look out for danger

Password Assumptions

- Attacker computing power
  - PDP 11/70?
  - Ratio of attacker/defender CPU power?
- Threat model
  - Theft of hashed password file
  - Serious limits to online guessing rate
- Limited number of passwords to be remembered
- Iterated cryptographic function can't be inverted

Only the last has held up!

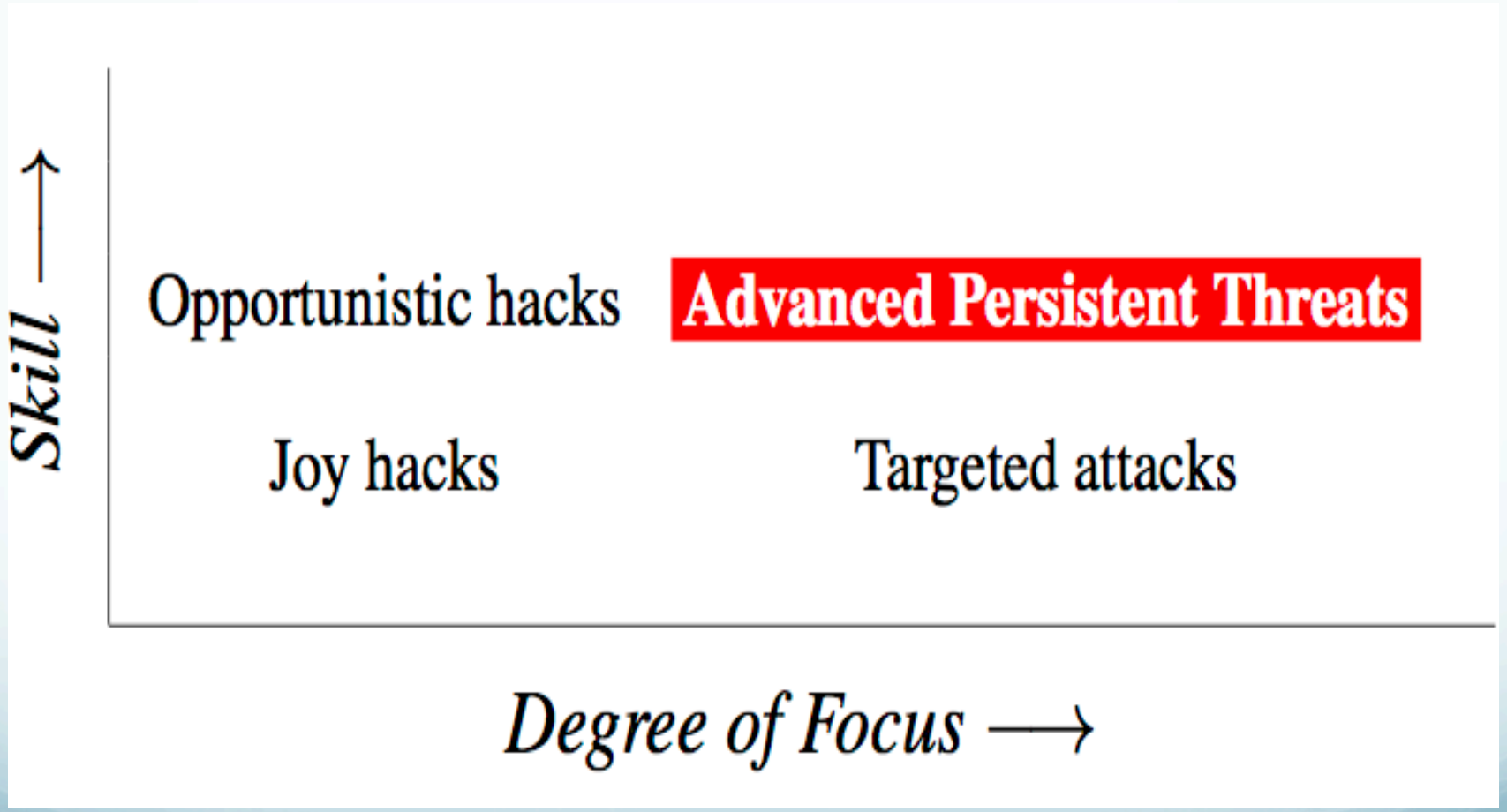
When Did These Fail?

- Attacker computing power has been increasing gradually
  - Sharp increase after 2000, with the rise of botnets
  - More recent jump with the use of GPUs
- Threat model changed around 2003, with the rise of for-profit hacking
- Number of logins has been going up since the rise of the web—hard to pinpoint a number, but it was obviously an issue 10 years ago
- But—our password policies remain about the same

Why is Threat Model Important?

- More precisely, why is it an *assumption*?
- We implicitly assume certain limits to the behavior of our enemies
  - Is someone going to break into your house to bug your keyboard?
- "Amateurs worry about algorithms; pros worry about economics" (Allan Schiffman, 2004)
- A stronger threat means the attacker has more resources

The Threat Matrix



Attacker Resources

- Joy hackers: few; primarily downloaded scripts and exploits
  - *The 1990s threat model*
- Targetiers: considerable knowledge about your systems and procedures; possibly inside access
- Opportunistic attackers: sophisticated tools; often, plenty of money
- APTs: everything, up to and including "the 3 Bs" (burglary, bribery, and blackmail)
  - We see this—*to some extent*—today

Assumptions Behind Firewalls

- Obvious: topological nature
- Less obvious: simple—i.e., comprehensible and correct—security policy
- Less obvious: all interesting protocols are efficiently protectable by a firewall
- Crucial but often ignored today: assumption that the firewall's implementation of a protocol is itself correct and secure

To some extent, *all* of these are now false

Are Firewalls Themselves Secure?

- There are far more protocols in use today
- To function, the firewall must understand all of these
- This implies a lot of code; often, a lot of very complex code
- Why should we think this code is correct?

Firewalls and Threat Models

- Joy hackers are probably stopped
- Opportunistic hackers can get through, especially with worms, phishing, and drive-by downloads
- Targetiers have detailed knowledge of topology and behavior; they may or may not be blocked
- To APTs, firewalls are just a speed-bump

Flow Monitoring Assumptions

- What are the assumptions?
- Why *should* it work?
- We assume:
  - We can capture “enough” flows
  - We will capture the evil ones
  - We will be able to spot the flows of interest

Flow Rate

- Assume actual traffic of *P* packets per second and *F* flows/second
  - Implies *P*/*F* packets per flow
- Assume maximum capture rate of *C* flows/sec
- What is the relationship of *F* and *C*?
- If *F*>>*C*, we must down-sample and will miss important flows. Ultimate success may depend on technology changes: relative growth of *F* and *C*
- Statistical sampling may mean we'll something—and with an intelligent adversary, we may miss what the attackers want us to miss
  - Assumption: the attacker can't manage that. True?

Limits to Flow Monitoring

- Size of the traffic matrix—it goes up as the *square* of the number of endpoints
- Memory bandwidth has only been increasing slowly
  - Number of endpoints and bandwidth have both increased far more quickly
  - Memory speeds haven't kept up
- Conclusion: sampling is *necessary*—but does it hurt us?
- That it doesn't is another assumption

Packets per Flow

- What is the behavior of the monitoring system for low *P/F*?
  - Is there considerable overhead for creating state for a flow?
  - Can the attacker use that to evade detection?
- Underlying assumption: behavior at low *P/F* just affects the random percentage picked up. Is this a way to hide?

Spotting Evil Flows

- Suppose the percentage of evil flows is very low—can we spot them?
- Can the attacker create enough benign-looking flows to hide amongst?
- Another assumption: evil flows have certain characteristics—size, destination, etc.—that we can spot. Can the attacker hide, via proxies and the like?
  - Attack: compromise legitimate web site your users visit; serve malware from there
- "Low and slow" attacks?

Spotting Exfiltration

- Underlying assumption: all traffic to a given destination is equivalent
  - But—sites like gmail, Facebook, etc., are multipurpose
- Second assumption: looking more deeply at flows can show anomalies
  - Can the attacker mimic them?

"And by the way, we are belittling our opponents and building up a disastrous overconfidence in ourselves by calling them pirates. They are not—they can't be. Boskonia must be more than a race or a system—it is very probably a galaxy-wide culture. It is an absolute despotism, holding its authority by means of a rigid system of rewards and punishments. In our eyes it is fundamentally wrong, but it works—*how it works*! It is organized just as we are, and is apparently as strong in bases, vessels, and personnel."

E.E. "Doc" Smith, *Galactic Patrol* (1950)

Final Thoughts

- Our defenses are built for a given threat and a given set of technologies
- Neither of these are static—and we can't be, either