Assets / Threats Pragmatics

BhutanNOG / Thimphu

2017.06.05-9

Just an Example

What is a BotNet?

1. Bot Maker infects thousands of machines using malware, fishing, …
2. Bot Maker has Command and Control
3. Bad Guy pays Bot Maker to attack
4. Bot Army attacks the Bad Guy's victims

By Tom-b - Own work, CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=9084453

We're Talking About Tens of GigaBytes per Second

We will describe many kinds of attacks and defenses

This was just to give you an idea

Overview

- Assets – What are we protecting?
- Attackers – From whom?
- Attacks – Common Attacks
- Defenses - Defenses

What are we Protecting

Many sorts of targets:

- Network infrastructure
- Network services
- Application services (money!)
- Data
- User machines

What is at risk?

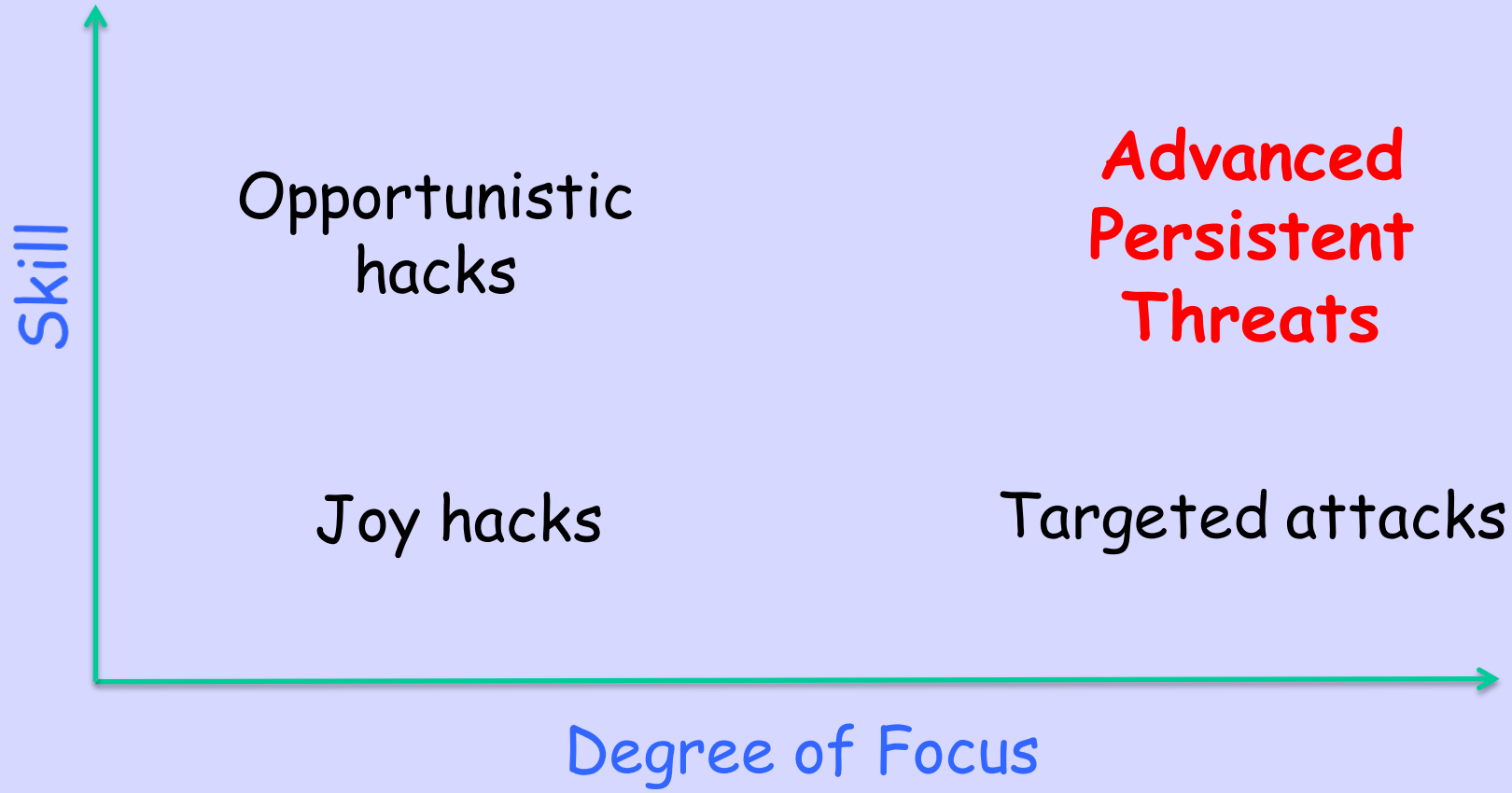
Who Are the Enemies?

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, AKA Nation State Adversaries

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

The OPM Hack

- US **O**ffice of **P**ersonnel **M**anagement
- Records of 21.5m USG employees and security clearance applicants
- Started March 2014 discovered April 2015, data of all USG employees
- Included theft of detailed security-clearance background information
- Think blackmail of USG empls & agents

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?
  - USBs in the parking lot
- 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 (see Stuxnet)
- Pay special attention to procedures
- Investigate *all* oddities

Varying Defenses

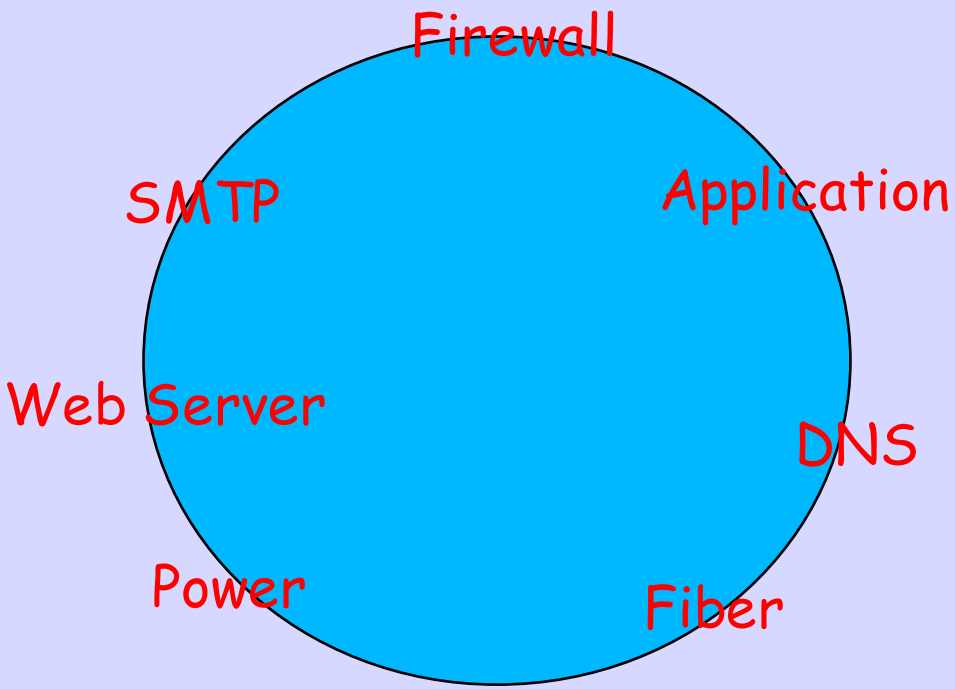
- Don't use the same defenses for everything
- Layer them; protect valuable systems more carefully
- Maybe you can't afford to encrypt everything—but you probably can encrypt all communications among and to/from your high-value machines

Uneven Playing Field

- The defender has to think about the entire perimeter, all the weakness
- The attacker has to find only one weakness
- This is not good news for defenders

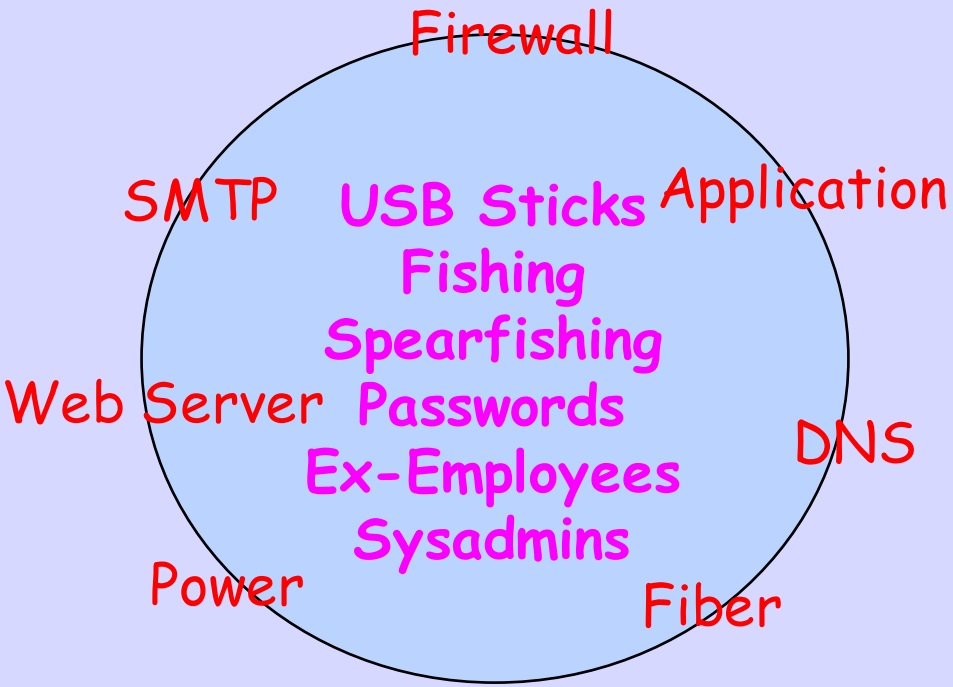
Attack Surface

Entire Perimeter you have to Defend



Soft Gooey Inside

But it is not just the perimeter!



Layers of Protection

- Firewalls (though there are laptops on the inside)
- Intrusion Detection Systems
- Logging Systems and Analysis
- Protecting the Firewalls, IDSs, and Logging Systems

And what do you have?

A Much Bigger Attack Surface

US DoD data shows on average 1/3 of vulnerabilities in government systems are in the security software

It's the Software!

"Instead of focusing on the impact of the hacks, we should dig for the reasons these systems were so vulnerable in the first place. Almost without fail, the root cause is bad software."

-- Gary McGraw

But We Have to Defend the Entire Attack Surface

Network Infrastructure

- Routers (and routing protocols)
- Switches and other network elements
- Infrastructure Services: DNS, DHCP, LDAP, Microsoft stuff

Links

- Primary risk is wiretapping
- Easily defeated by encryption—but are people using it?
- Most encryption doesn't protect against traffic analysis—but that isn't in everyone's threat model
- Link-layer encryption protects against most traffic analysis, but it has to be done on every vulnerable link

Crypto is not the Weakness

- Commonly, the encryption technology is fine and is not broken
- As long as you have not invented your own
- The weakness is OpSec, Operational Security Practices
  - Key Management
  - Weak Keys and Antique Crypto Algorithms
  - Sending Cleartext

Traffic Analysis

- Looks at *external* characteristics of traffic: who talks to whom, size of messages, etc.
- *Very* valuable to intelligence agencies, police, etc.
- Who works with whom? Who gives orders to whom?
- Not generally useful for ordinary thieves, though sophisticated attackers could use it to find targets

Solutions

- Use VPNs or application-level encryption
- Use link encryption for high-risk links (e.g., WiFi)
- Also use link encryption for access control (especially WiFi)
- Don't worry about traffic analysis—unless your enemy is an intelligence agency. Of course it is!

(Is WiFi Safe?)

- Inside an organization, WiFi+WPA2 Enterprise is generally safe enough without further crypto
  - However, it's harder to trace an infected host that's doing address-spoofing
- For external WiFi, *always* use crypto above the link, preferably VPNs
  - Make sure you do mutual authentication
- There is some residual risk if your VPN doesn't drop unencrypted inbound traffic

Switches and the Like

- Compromised switches can be used for eavesdropping
- Special risk in some situations: reconfigured VLANs
  - VLANs provide good traffic separation between user groups
  - Especially useful against ARP- and MAC-spoofing attackers
- Other danger point: the monitoring port

ARP and MAC Spoofing

- ARP maps the IP address desired to a MAC address
- Switches learn what MAC addresses are on what ports, and route traffic accordingly
- If a malicious host sends out traffic with the wrong MAC address, the switch will send traffic to it
- If a malicious host replies to an ARP query for some other machine, the malicious host will receive the traffic, but this might be noticed

Address-Spoofing Happens

- A few years ago, someone spoofed the IP and MAC addresses of a university's FTP server
- The attacking machine was in another building but on the same VLAN
- No one had noticed the intermittent failures of the FTP service
- The machine had been penetrated 6 months earlier....
- Switches should log MAC and IP addresses changes, and keep those logs for a long time

Defenses

- Harden switch access
  - ACLs
  - ssh-only access, and only using public/private key pairs; no passwords

Routers

- Routers can be used for the same sorts of attacks as switches
- Because routers inherently separate different networks, they always defend against certain kinds of address spoofing
  - This makes them targets
- Worse yet, routers can launch *routing protocol attacks*

Routing Protocol Attacks: Effects

- Traffic is diverted
  - Attacker can see the traffic and do traffic analysis
  - Attacker can modify packets
  - Attacker can drop packets
  - Attacker can hijack prefixes
- End-to-end crypto can protect the packets' contents, but can't stop traffic analysis or denial of service

Why is Routing Security Different?

- Most security failures are due to buggy code, buggy protocols, or buggy sysadmins
- Routing security problems happen when everything is working right, but some party decides to lie. The problem is a dishonest participant
- Most routers can lie via any routing protocols they're using

Defending Against Routing Attacks

- Must *know* authoritative owner of prefixes
- Generally done with a certificate signed by the address space owner
- Being rolled out today as RPKI
- All routing announcements must be digitally
- signed
- Each router needs a route-signing certificate
- All signatures must be over the full path; signatures are thus *nested*
- In the IETF process as BGPSEC

Network Services

- Certain core services are ubiquitous—and frequently attacked
  - DNS
  - DHCP
  - SMTP
  - Assorted local services: file servers, printers, LDAP, and more
- *These are the means, not the goals of the attackers*

DNS

- DNS responses are easily spoofed by attackers
  - Cache contamination
  - Query ID guessing
  - Deliberate tinkering by ISPs, nation-states, hotels, etc.
- Because responses are cached, client/server authentication can't solve it.
- Must have *digitally signed* records (DNSSEC)

SMTP

- Historically, a major attack target; principle implementations were very buggy
- Today, the big problem is spam; must keep attackers from spamming/fishing your users, and from using you to spread spam
- Spearfishing is the major penetration
- Secondary issue: separate inside and outside email systems—inside email often has sensitive information

Encrypted Email

- Email messages themselves can be encrypted: useful for end-to-end security
  - But S/MIME and PGP are hard to use, and their *absence* will not be noticed
- SMTP can be encrypted, too
  - Not that crucial for site-to-site relaying (but eavesdroppers do exist); *very* important for authenticated email submission
  - Your users *must* authenticate somehow—via IP address if inside; via credentials if roaming—before sending mail through your outbound SMTP server

Local Services

- Rarely directly accessible from the Internet; (ab)used after initial penetration
  - Virus spreading
  - File contents, in targeted attacks
  - Privilege escalation
- Quite often buggy, but there's little choice about running them; they're necessary for scalability and productivity

Application Services

- Data center-resident: deliver services to the outside world
- Obvious example: HTTP
- But—HTTP is generally a front end for a vital database
- A prime target

Targeting Application Services

- Generally exposed to the outside—and you can't firewall them, because they *must* be exposed to the outside
- The server can be used for the bad guys' content: phishing servers, "warez" sites, more
- The database often holds very valuable information, like credit cards
- There are usually connections from these servers back into the corporation

User Machines

Ordinary desktops are targets, too

- Plant keystroke loggers to steal passwords, especially for financial sites
- Turn into bots—bandwidth is what matters
- Turn into spam/spearfishing engines; use machine's privileges (generally based on network location) to send out spam through the authorized SMTP server

Users

- Users make mistakes
  - They click on things they shouldn't
  - They visit dangerous sites
  - They mistake phishing emails for the real thing
  - They don't keep their systems up to date
  - "PEBCAK": Problem Exists Between Chair and Keyboard
- (It's not even their fault; our systems are horribly designed)

Social Engineering

- Phishing and other 'clickbait' are the most common and most dangerous forms of Social Engineering
- Click on one bad URL and your computer is infected
- 'Spearphishing' is when phishing email seems to come from someone you know
- When my wife sends a URL or attaches a file, I ask in Signal or Skype if it is real

Social Engineering

- Try to trick people into doing things they shouldn't
- People *want* to help
  - Walk in the door dressed as a delivery or repair person
  - Call and sound like an insider: "Chris, could you reset my password on server #3 in rack 7? Its connection to the RADIUS server is hung."
- A very different skill than purely technical stuff— but *very* useful too