Asset & Threats Models

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

Thanks

Most contents were provided by:

- Steven M. Bellovin
- Randy Bush

Starting Off

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

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

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)

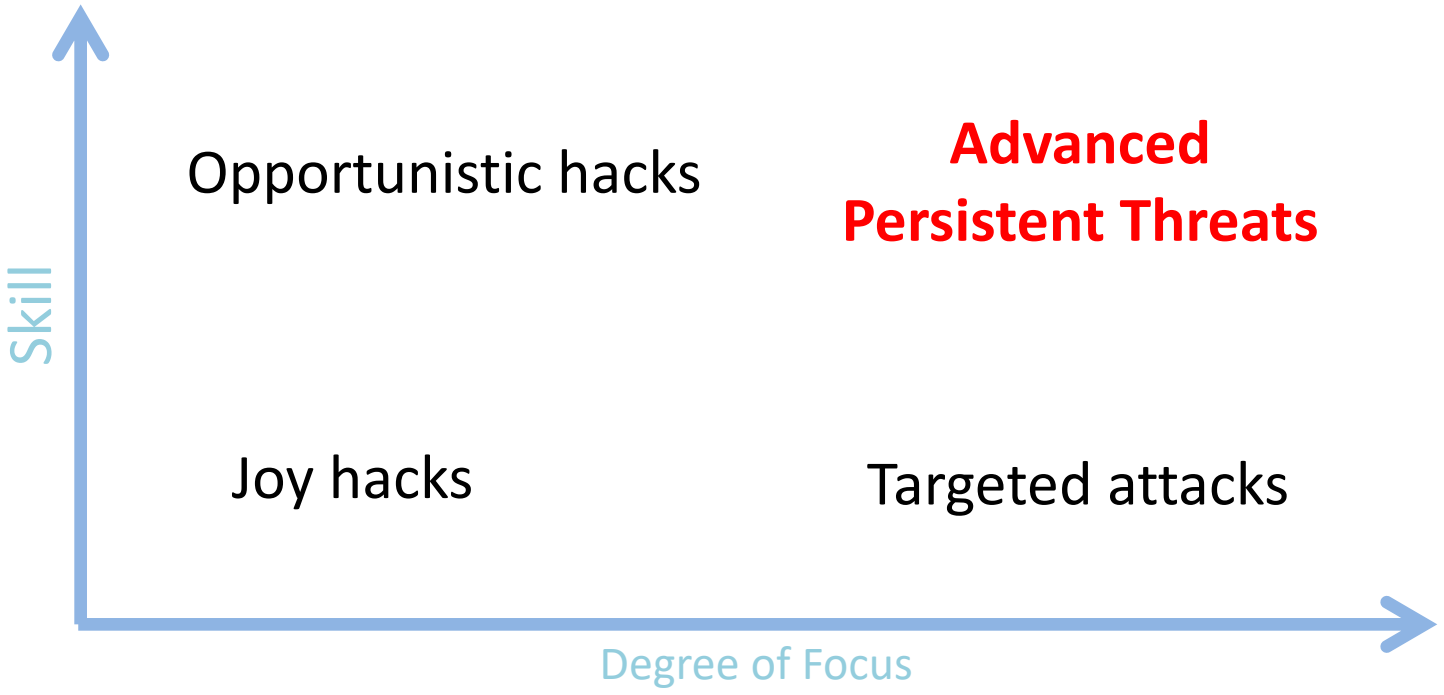
Your Asset

- $money and $valuables
- Credentials and accounts information
- Services itself
- CPU power/bandwidth
- Secret contents
- Software
- Data

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



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

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

Cost

- Is the value of the asset worth the cost of the Defense?

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

Shouldn’t be *easier* targets

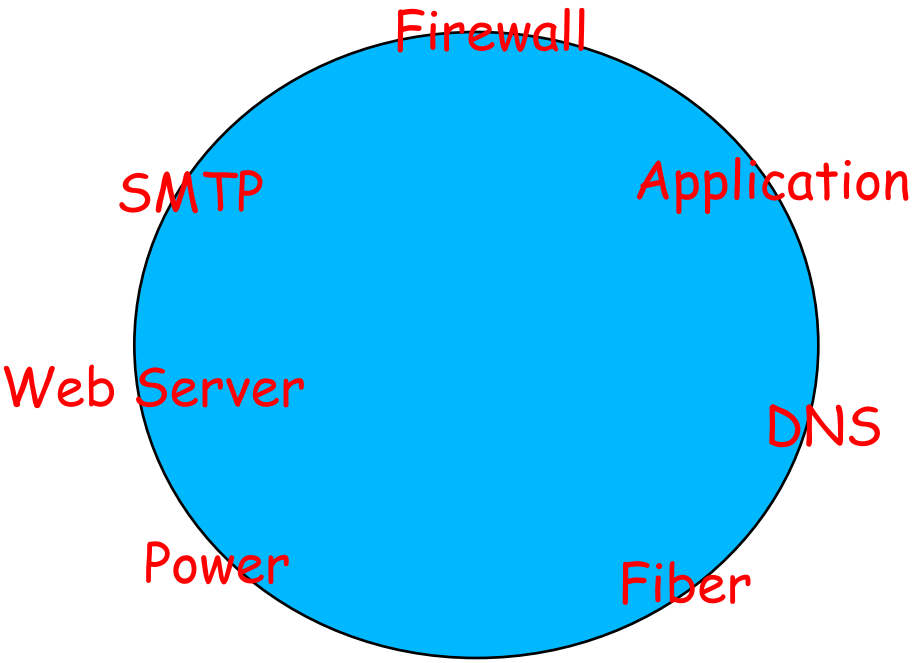
- Values
  - Higher is better for attackers
- Defense
  - Weaker is better for attackers
- If he values are the same, attacker may want to target weaker systems
  - You are weaker when others get safer
- Conclusion: follow Best Current Practices and revise your procedures to keep them up to date

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

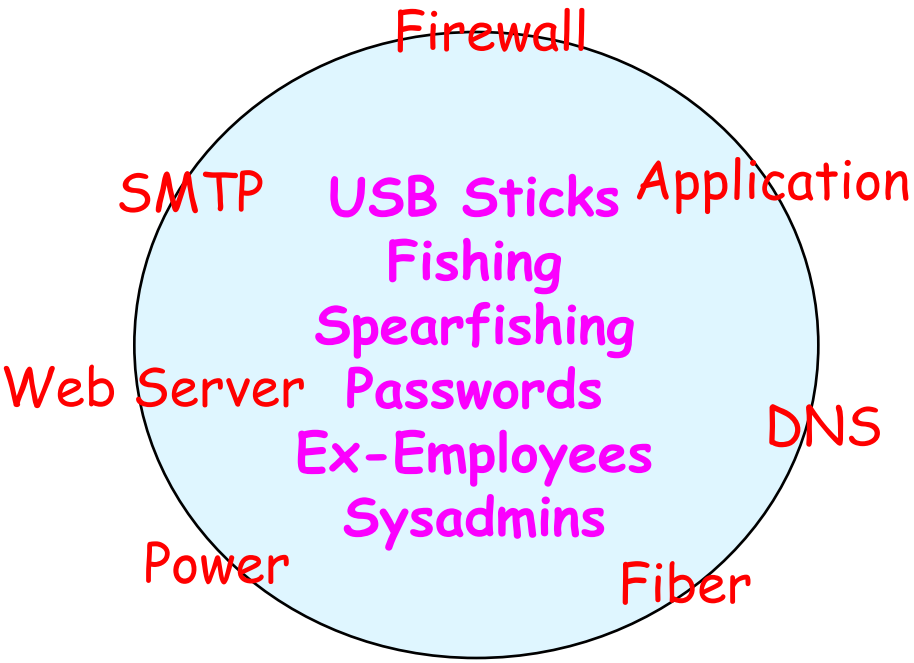
Attack Surface

- Entire Perimeter you have to Defend



Soft Gooey Inside

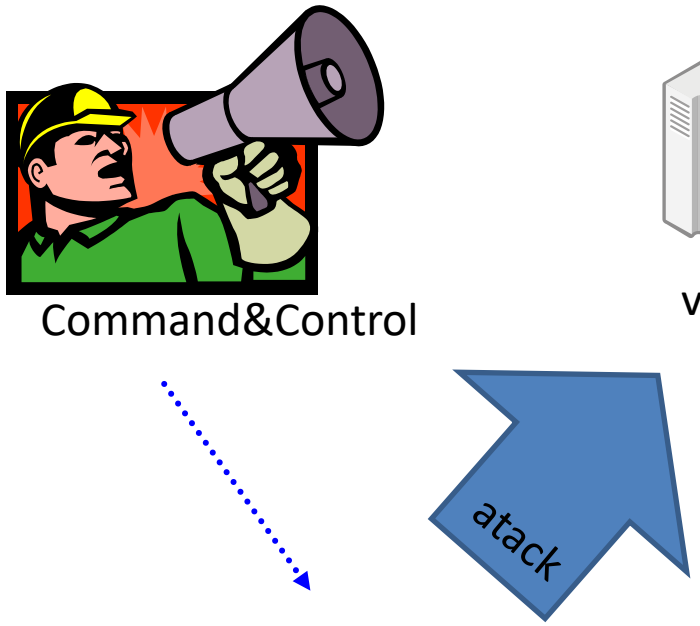
- But it is not just the perimeter!



Common Denial of Services Attacks

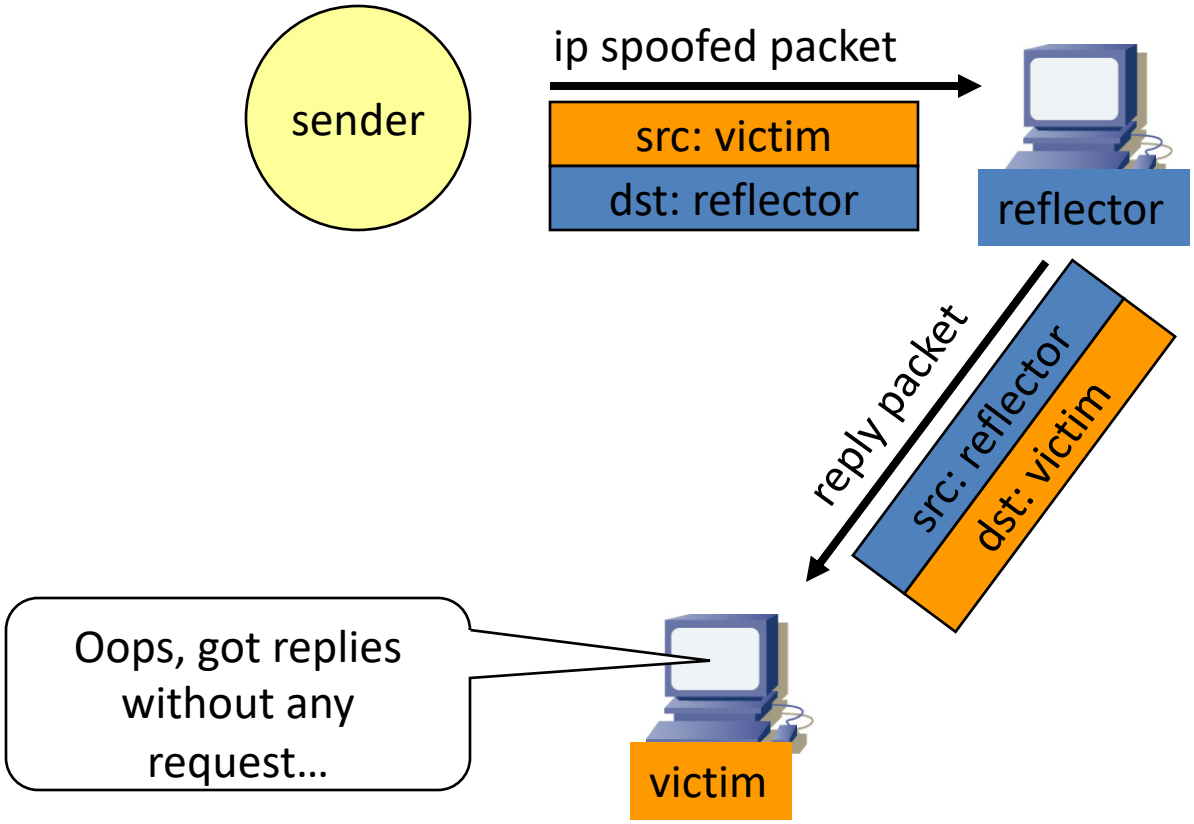
- Server resources
  - IP fragment flooding
  - SYN/FIN/ACK flooding
  - Connection flooding
- Network capacity
  - Traffic flooding
- Computer resources required to launch attacks

Botnet



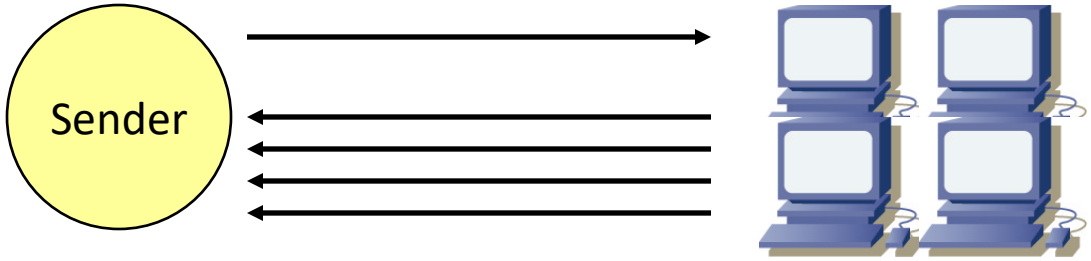
1. Bot Maker infects thousands of machines using malware, fishing, …
2. Bot Maker has Command and Control
3. Bad Guy pays Bot Maker to attack
4. Bot Army attacks the Bad Guy's victims

Reflections



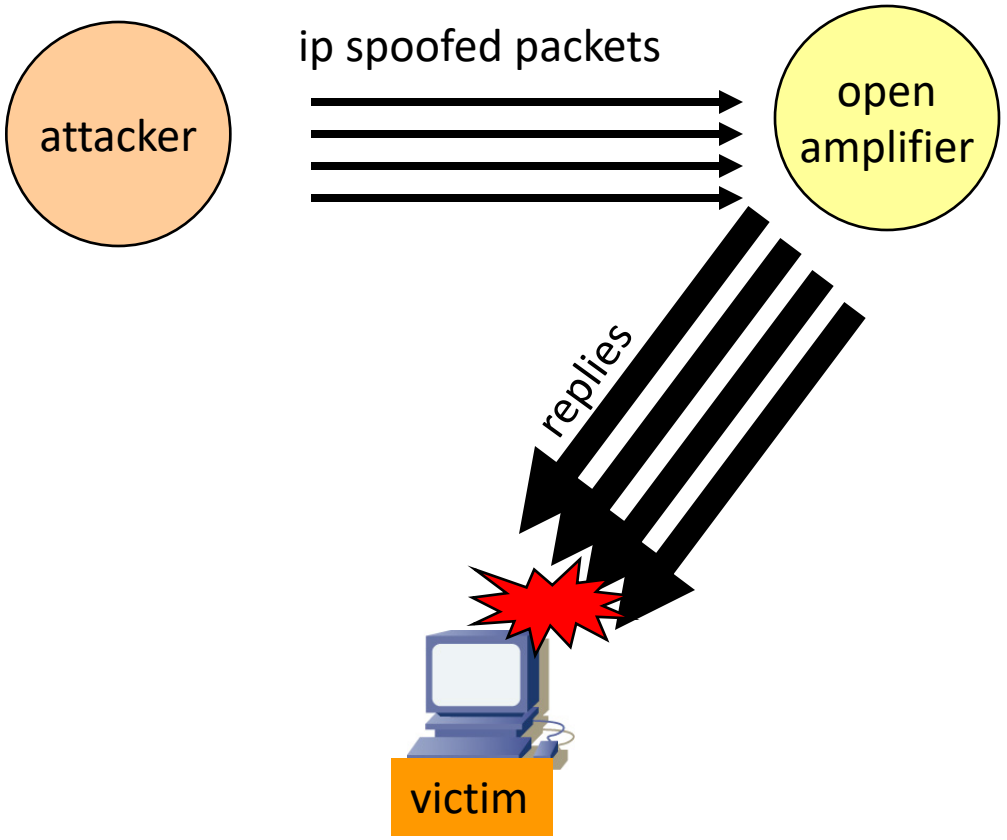
Amplification

1. multiple replies

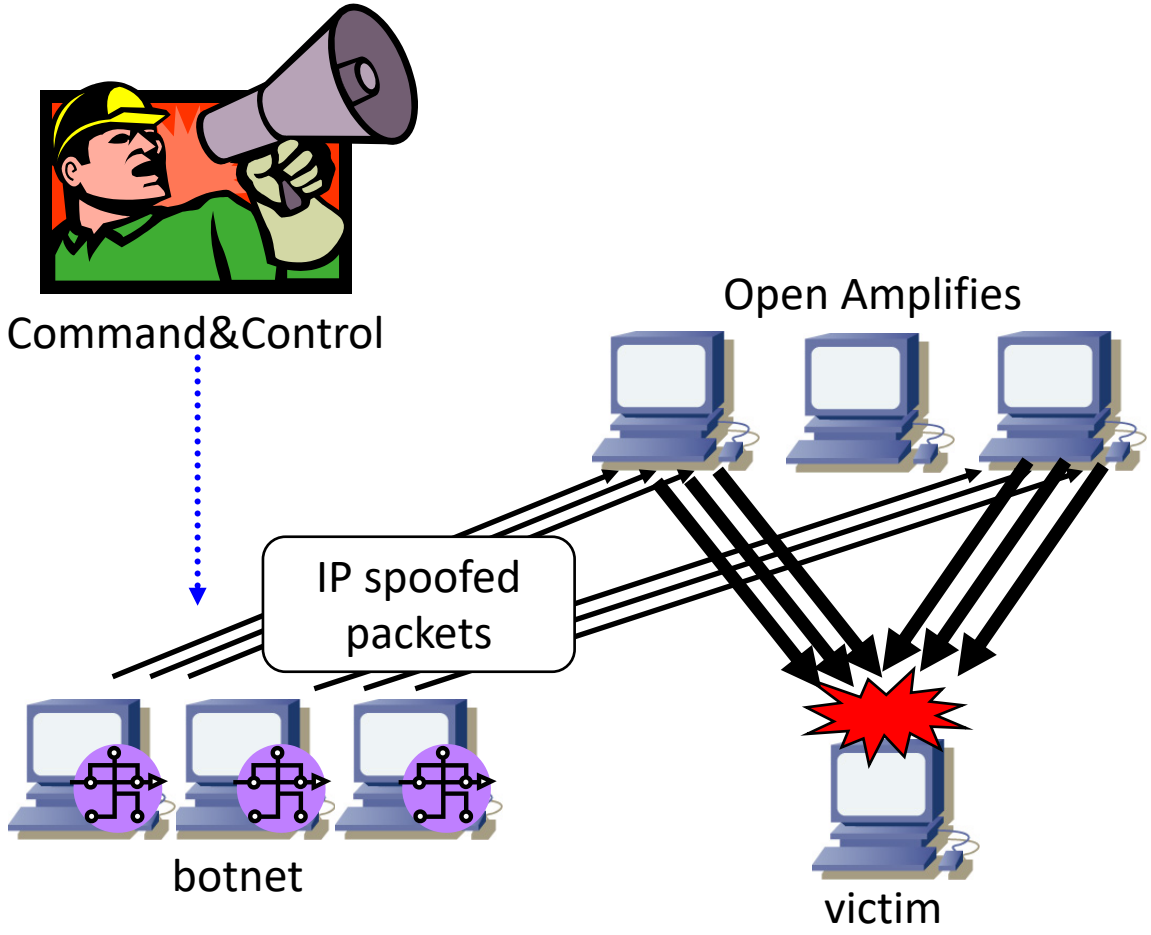


2. bigger reply

IP reflection attacks



Botnet and reflection attack



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

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

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
- Then owner says what AS may announce the address space
- Being rolled out today as RPKI-based Route Origin Validation

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/phishing 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 their fault!
- Today's systems are horribly designed

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

Summary

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

And again

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