

Applied Networks & Security

Security

<http://condor.depaul.edu/~jkristof/it263/>

John Kristoff
jtk@depaul.edu

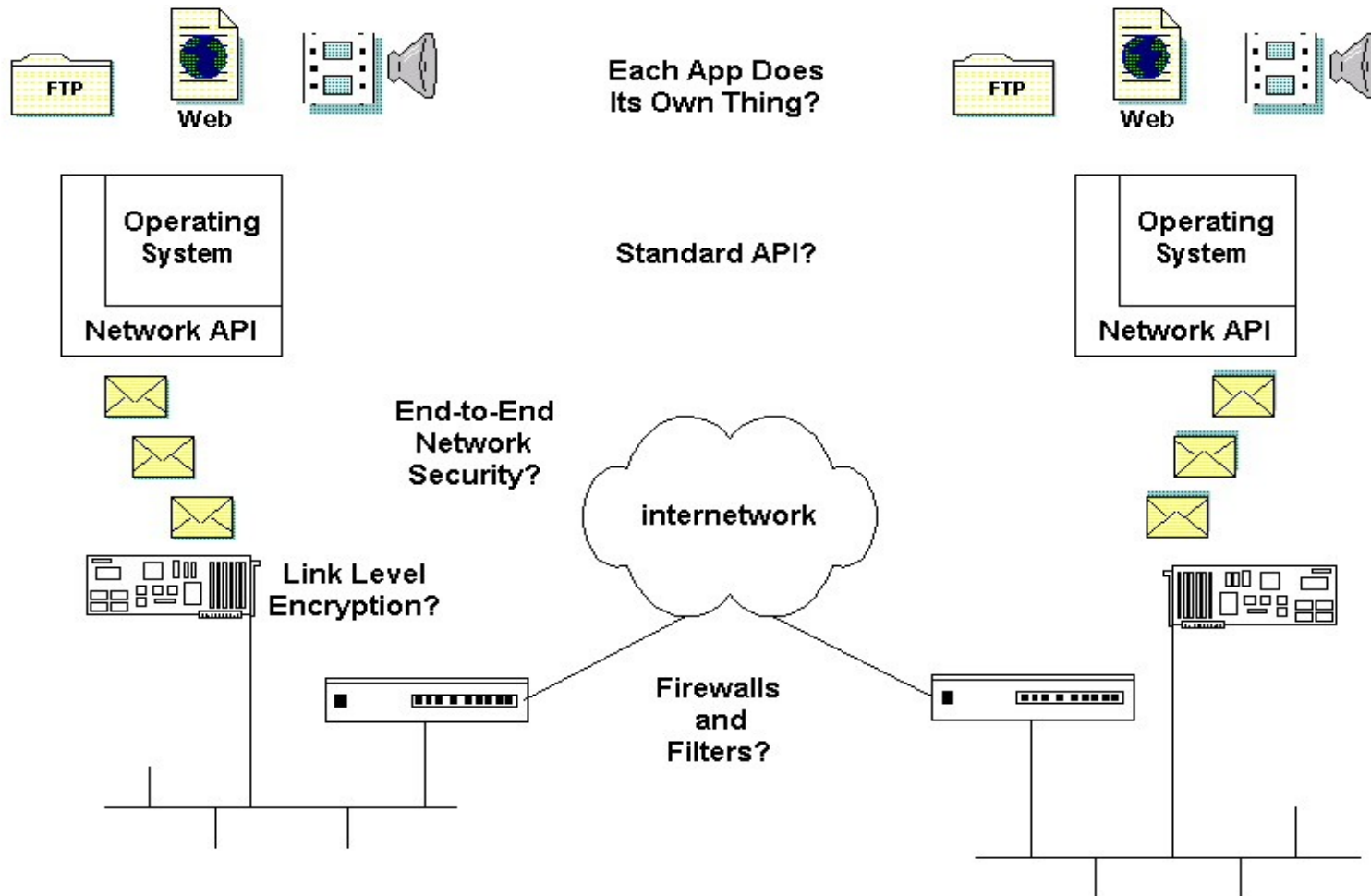
Internet security is hard to do!

- Lots of things need securing
- There is a lot more to it than just the *packets*
 - And fools rely on the filtering of magic bit patterns
- Software tends to be buggy and poorly designed
 - There is a LOT of software in widespread use
- Vendors ship systems with poor defaults
- Each user has to be a *system administrator*
- Few people are truly good at doing Internet security
- One person's security problem is also another's

Compare Internet Model to Telephone Network Model

- Telephone network
 - Centralized control
 - Functionality inside
 - Lightweight ends
 - Fixed parameters
 - Predictable usage
 - Innovation by a few
 - Regulated
- Internet
 - Distributed control
 - Functionality outside
 - Lightweight middle
 - Loose parameters
 - Unpredictable usage
 - Innovation by any
 - Unregulated

Where do you apply security?



The end-to-end (e2e) argument

- Functionality is generally best placed at the ends
 - If it's redundant at each hop, maybe move it out
- Key concept to understanding Internet Architecture
- Most people never do e2e security, likely a key reason why Internet security is never any good
- e2e security is hard on a large (Internet) scale
- e2e may be the Internet's best and worst feature depending on your perspective

Thought exercises

- What does an e2e architecture enable?
- What sorts of thing does it disable?
- Should the Internet architecture change?
 - Has the Internet architecture changed already?
- If so, in what ways?
- Is there something beyond the telephone and the Internet architectures that should be explored?
- Would it help if we were at the pub?

Security by obscurity

- This is generally a very bad approach
- But it is a widespread approach
 - Interactive passwords are one form
- Secrets have a tendency not to be eventually
 - Guessing
 - Leaks
- Compromise can be catastrophic
- Force attackers to *have* something, not just know
 - e.g. physical access, two-factor authentication

Layered defenses

- The belt and suspenders approach
- Place security mechanisms throughout the system
- There may be a layer an attacker can't penetrate
- Multiple layers tend to slow an attacker down
- A failure at one layer can be better contained

Principle of least privilege

- Limit what a user/process can do by default
- Similar to default deny
- Popular systems are beginning to finally do this
- Do you use the admin/root account for routine work?

Default deny

- Just what it sounds like
- Limit all but that which is expressly permitted
- New or unknowns fail safe
- Limits the areas of concern to protect and monitor
- May be difficult to implement when explicit allow rules are extensive

Security by fiat

- Though shalt not do/use *X*
- Often implemented by organizational policy
 - Very often security geeks making these choices
- Usually supported by filters, firewalls and/or limited access to hosts and networks by users
- Can work reasonably well in some environments
 - Impractical in many environments
- Never underestimate the power of a determined user (especially if they rank higher than you), attacker or piece of malware

Black lists

- Maintain a list of known “bad sources”
- Widely used for spam and related packet senders
- Not without problems
 - False positives, transient addresses, political
- Security geeks often love black lists
- BL maintainers are frequently attacked, harassed

Address spoofing

- Using an unassigned source address
 - Usually done for malicious purposes
- Impersonation attacks
 - Source address-based authentication attacks
 - e.g. ARP spoofing
- Reflection attacks
 - e.g. SMURF attacks

Anti-spoofing

- Layer 2
 - e.g. bridge/LAN port detection and restrictions
 - Not widely deployed
- Layer 3
 - Source-based address filters
 - Unicast reverse path forwarding (uRPF) checks
 - Not widely deployed enough
- Can be difficult to deploy in complex environments

Bogon filtering

- For a current list of bogons see:
 - <http://www.cymru.com/Bogons/index.html>
- Where can bogon filters go?
- Should you actually do bogon filtering?
- In-class discussion

Packet probes and network scanning

- In essence door rattling, see what is out there
 - May provide valuable intel for an attacker
 - Often good for auditing and troubleshooting
- Tendency these days to remain as quiet as possible
 - NAT and RFC 1918 tend to be good at providing this feature in lieu of probes and scanning
- <http://insecure.org/nmap> is a nice tool for the toolbox
- Probing may be indirect
 - e.g. DNS queries, open resolver bouncing

Route hijacking

- Claiming you can forward packets to destination X
- May be a man-in-the-middle (MITM) attack
- May be a denial of service
- May be a transient impersonation attempt

Spam

- Do I really need to say much about this?
- Why is this problem so bad and hard to fix?
- It costs spammers very little to send lots of mail
- They actually get a return on it, success rate %-wise it's low, but high enough to make it profitable
- If you think you have the solution, there is a lot of wisdom that begins here:
 - <http://www.rhyolite.com/anti-spam/you-might-be.html>

Trojan horses, worms and viruses

- You don't want them :-)
- Malicious code often attempts to hide
- Often includes a back door for an intruder to access
- May collect data from the system (e.g. Keylogger, email address harvesting, packet capture)
- May send spam, packets (DoS), attempt to spread to other hosts, etc.
- Detection and removal can be difficult

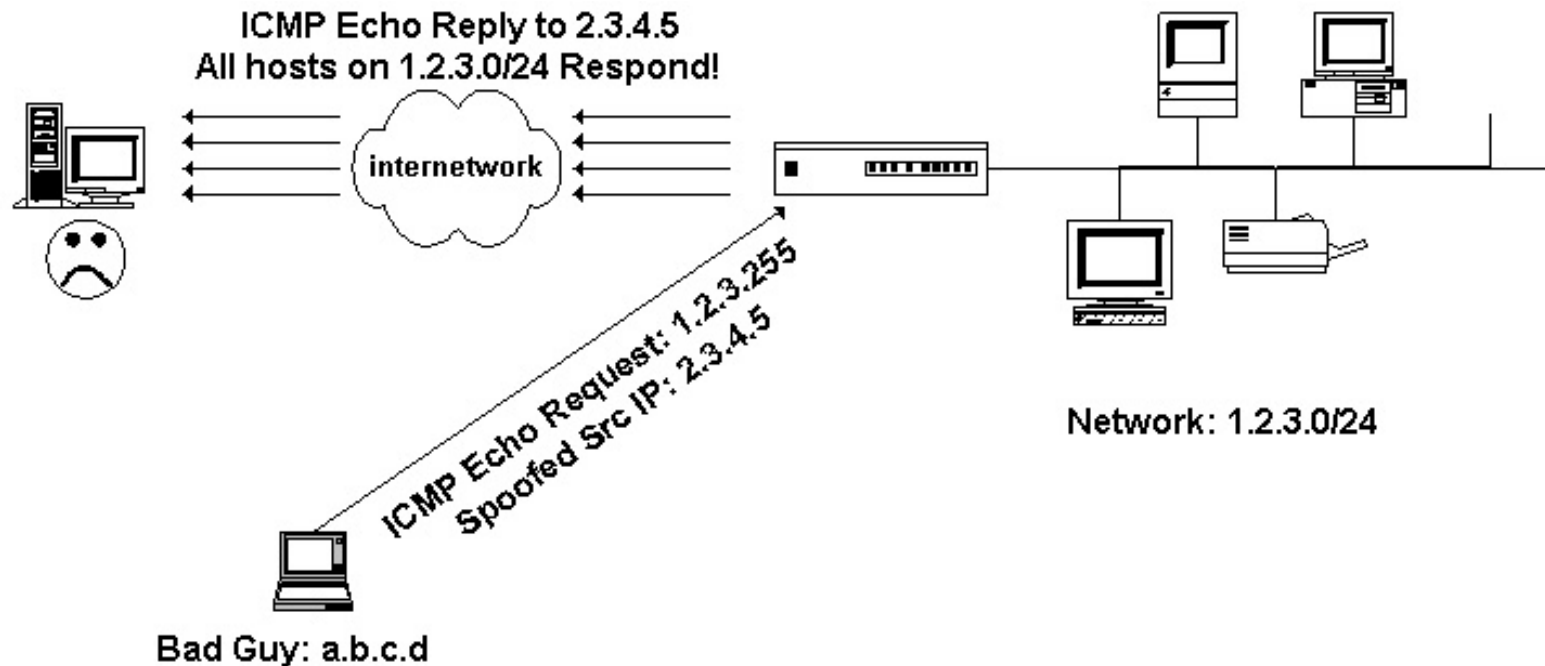
Buffer overflows

- Limited sized buffer is overrun with additional data
- That additional data can alter a running process
- In essence, a programming bug
- May be exploited for malicious intent
- Very common symptom for many vulnerabilities

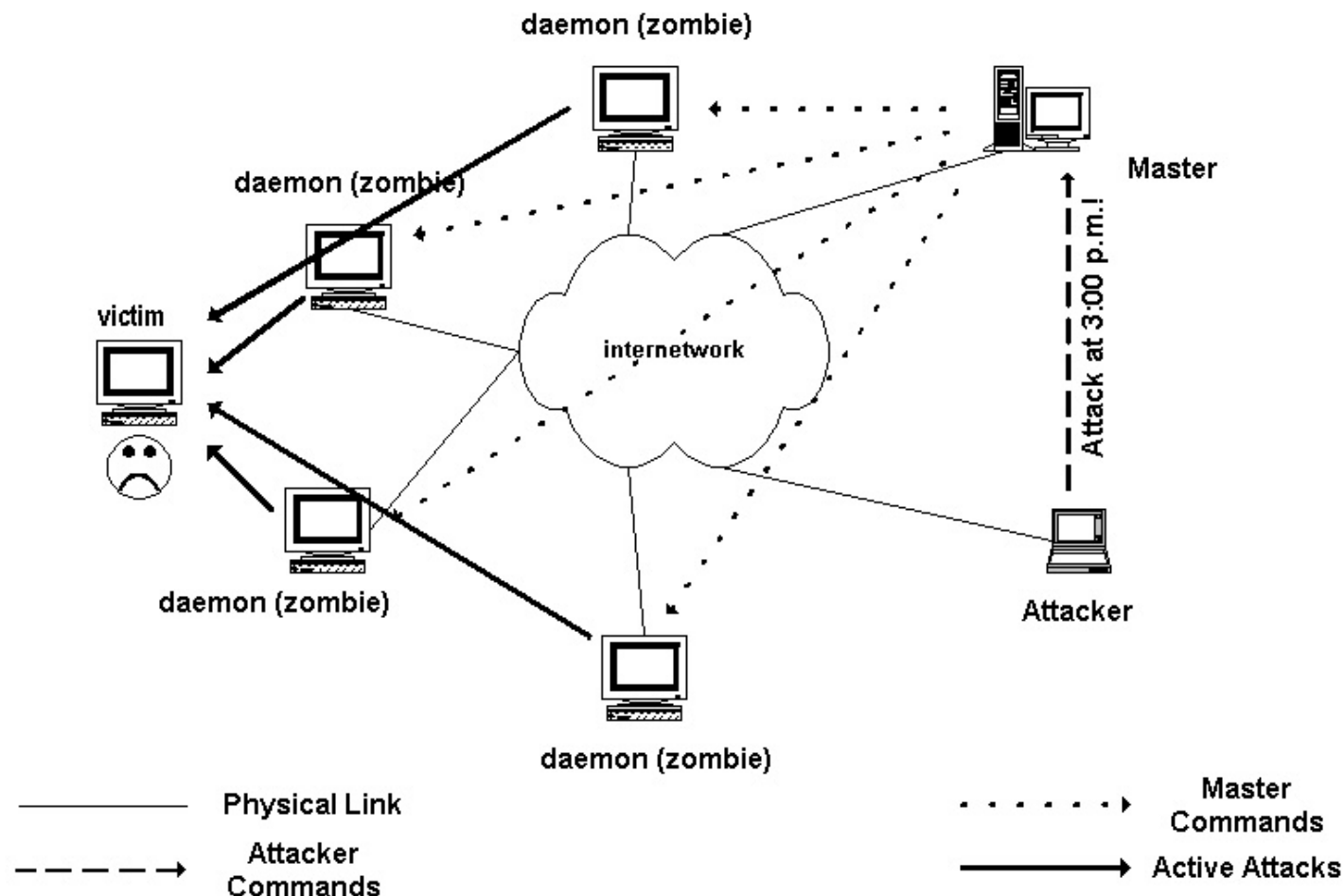
Privilege escalation

- Elevating privileges to perform otherwise denied operations
- Sometimes this is done on demand for certain operations (e.g. PING needs raw socket access)
- Attacks may attempt to elevate privileges in order to attack a protected system (e.g. buffer overflow attacks often do this)

Denial of Service (DoS) Amplification/reflection attack

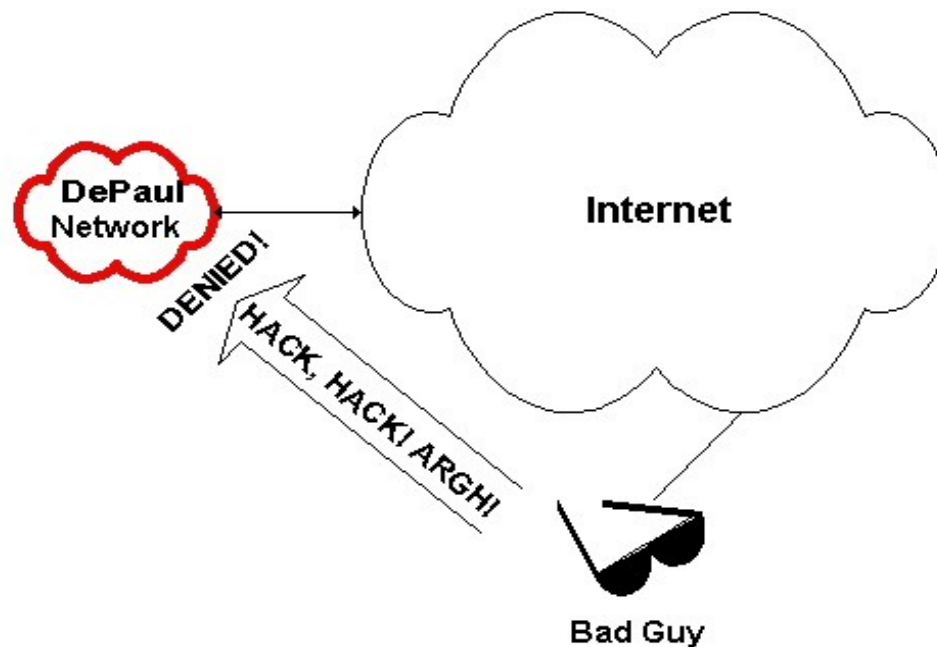


Distributed Denial of Service (DdoS) attacks - botnets



Perimeter security

- Define a boundary
- Separate a trusted inside from an untrusted outside
- Commonly people refer to “the network firewall”



An aside, backyard security stories

- Why is our DNS server emitting IRC traffic?
- You're hired security chief, now clean your system
- The misplaced Info Assurance exam
- 14,897,261 udp packets, let's take a packet capture
- What do these have in common?

Encryption

- Make something readable, unreadable
- Generally requires some black art math
- Crypto strength relies on cipher and key length
- Plain text -> cipher text -> plain text
- The safe keeping of decryption keys is... key!

Shared key crypto

- AKA symmetric crypto
- Communicating parties share a common key
- This key is used to encrypt and decrypt
- The key must be kept secret!
- Safekeeping the key gets harder as parties increase
- How do the trusted parties agree on a key?
- Example:
 - Ciphertext: 7,23,4 52,32,6
 - Key: Ulysses, Page, Line, Word

Public key crypto

- Everyone has 2 keys, one public, one private
 - A 2-key pair are mathematically related
 - Should be difficult to deduce one from the other
- The public key can be widely publicized
 - Use key used to encrypt messages to key owner
- The private key must be kept a secret!
 - Owner uses this key to decrypt messages encrypted with the public key
- Digital signatures can be verified with the public key

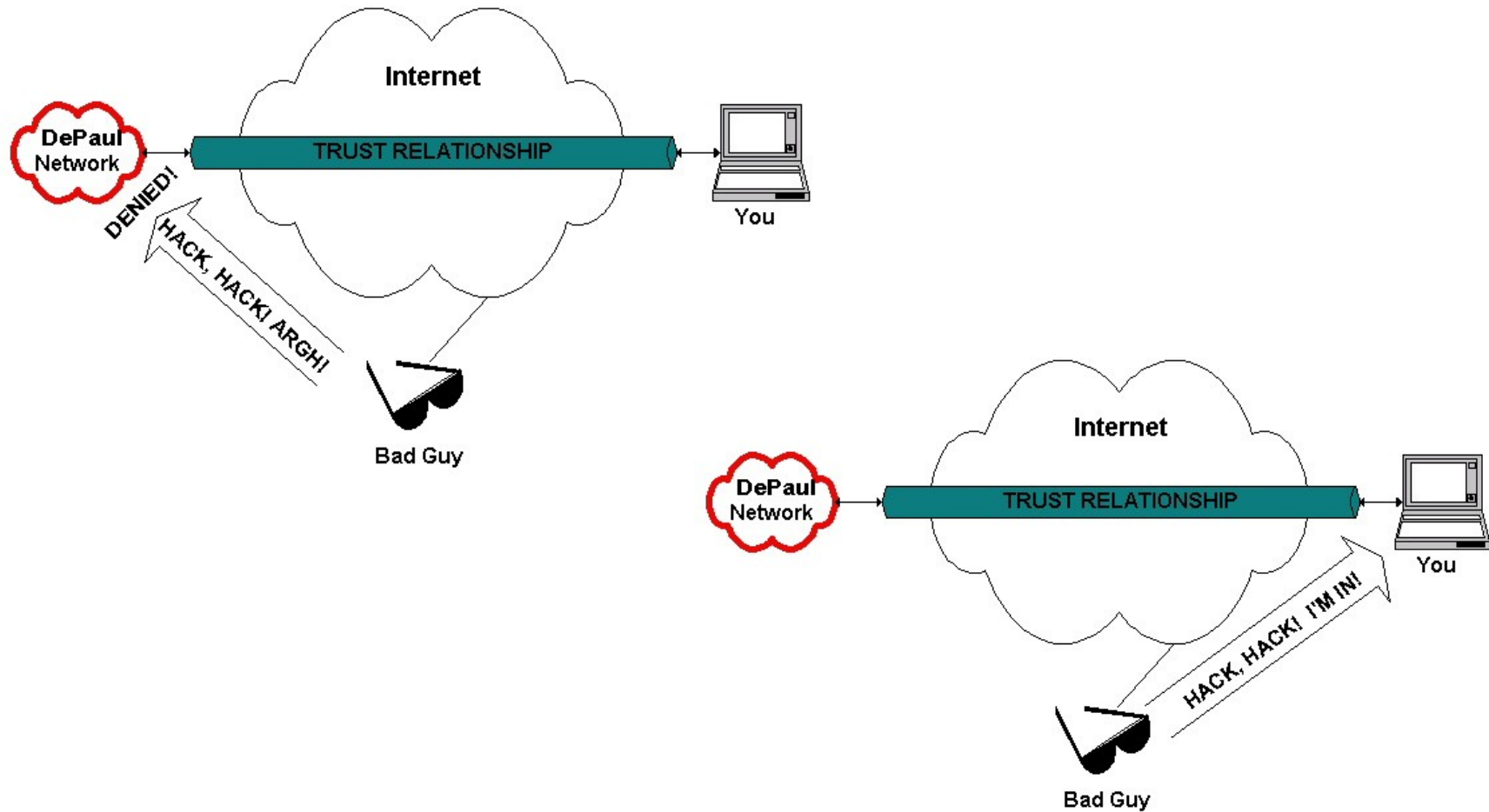
Crypto illustrated



Virtual Private Networks

- Using encryption, protects data between endpoints
- Used to help secure an un-secure public network
- IPSec/SSL/PPTP protocols are often used
- Often used to make host appear on a trusted net
- Usually only guards against network eavesdropping

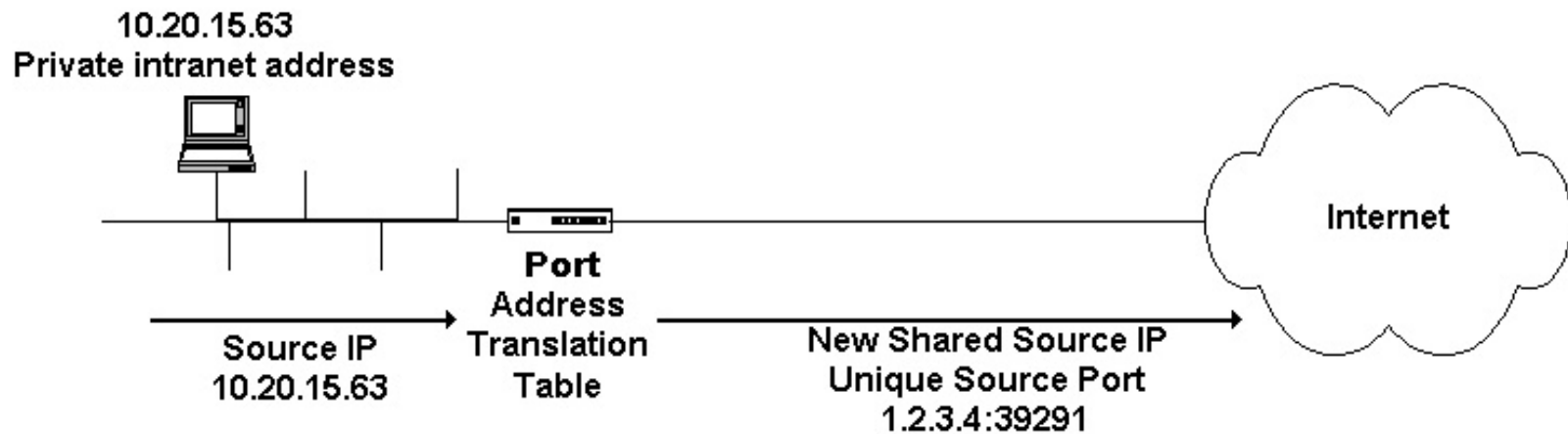
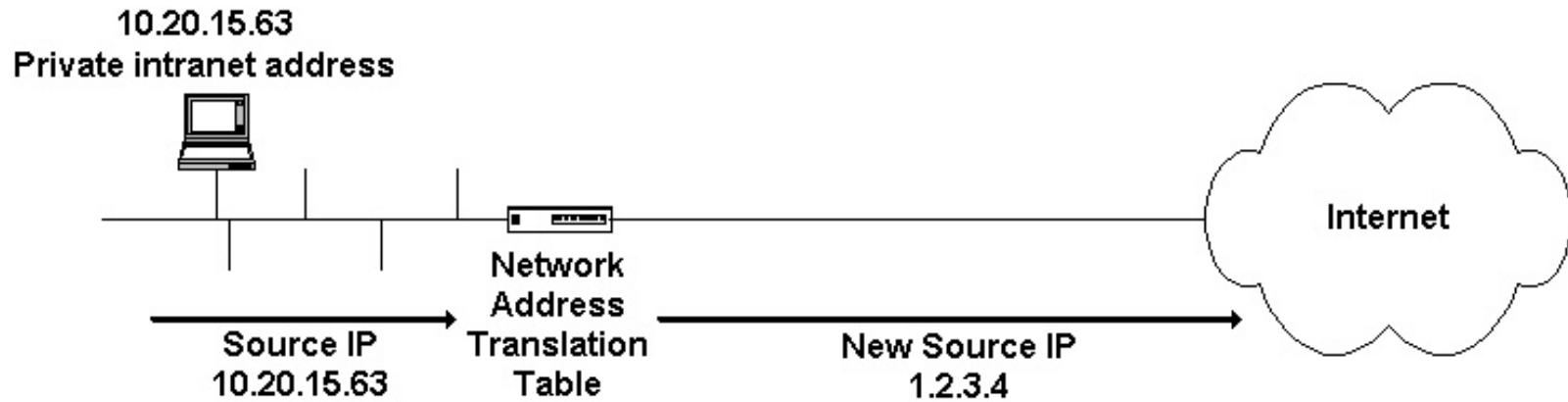
This would be bad



Network Address Translation (NAT)

- A solution designed for an address space problem
- Why am I talking about NAT now?
- Map internal address to one used externally
 - People usually use NAT w/ port translation
 - Port/network address translation
- Significant complexity, state and fate issues
- NAT really sucks IMNSHO!

NAT/NAT-PT illustrated



Honeypot, honeynet and darknets

- Honeypot/net system(s) setup to lure attackers
- Darknet AKA sinkhole
 - Packets to unused addresses
 - Packets go in, nothing comes out
 - Basically collecting the random garbage
- Used to track, monitor and analyze attacks
- Can be educational
- Miscreants sometimes learn what to avoid

Flows and logs

- Flows record a summary of network traffic
 - (e.g. NetFlow)
- Logs can be most anything (e.g. DNS queries)
 - (e.g. syslog)
- Widely used for trending and alerting
- Often a useful audit trail for investigations

Firewalls

- What most people think of when they think security
- Retrofitting centralized control into the network
- Examine packets in flight, possibly *keep state*
 - Use state for decision making on future packets
- Often perpetuates the neglect of other problems
- Inspection on a per-packet basis can be problematic

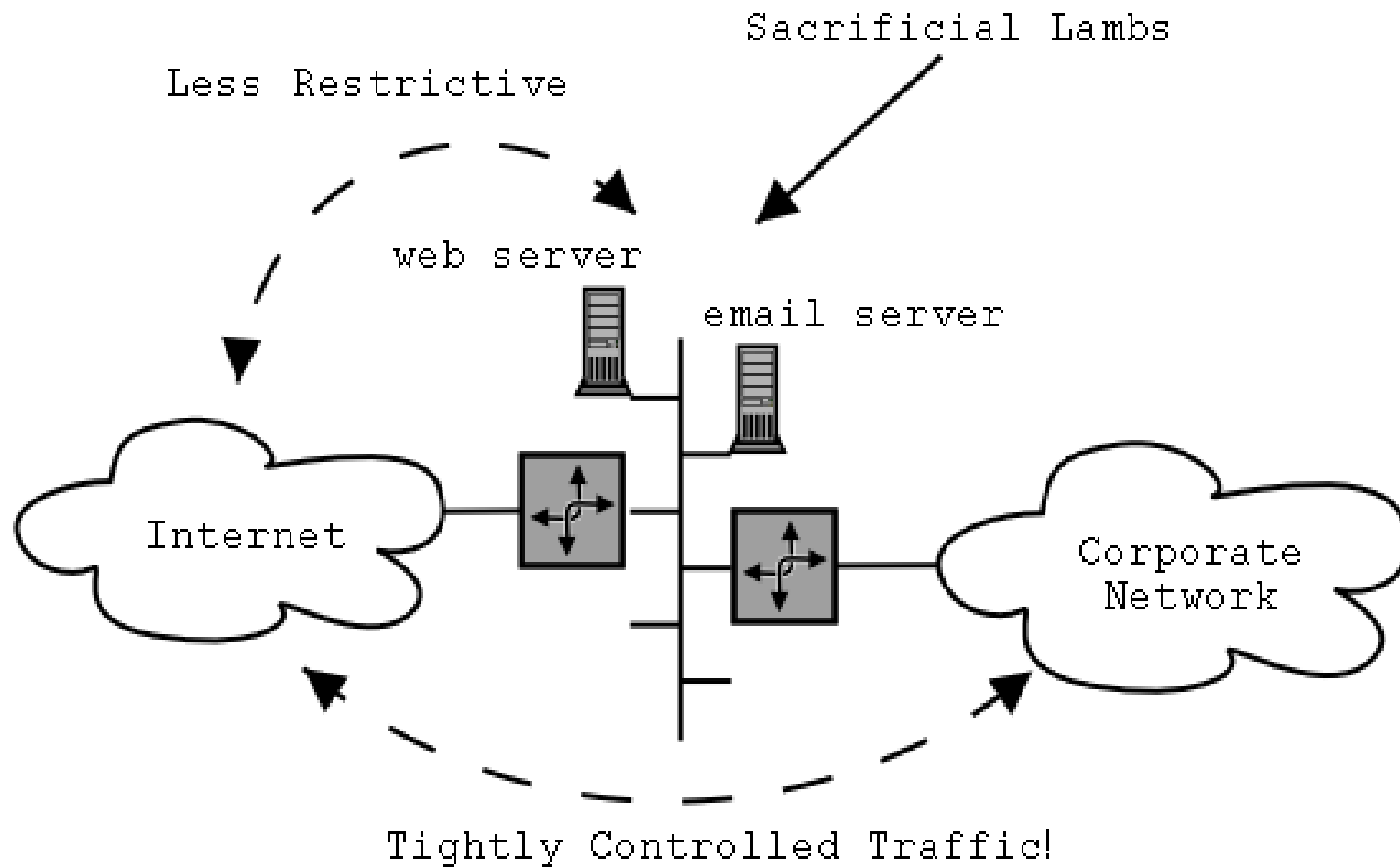
Per-packet filtering

- Stateless packet filtering
- Filtering decision based on *magic* bit combinations
- Examples:
 - IP protocol type (ICMP, UDP, TCP, other)
 - Source/destination addresses
 - Protocol control fields (TCP SYN flag set)
 - Pattern match (“/bin/sh” on odd port numbers)

Stateful inspection

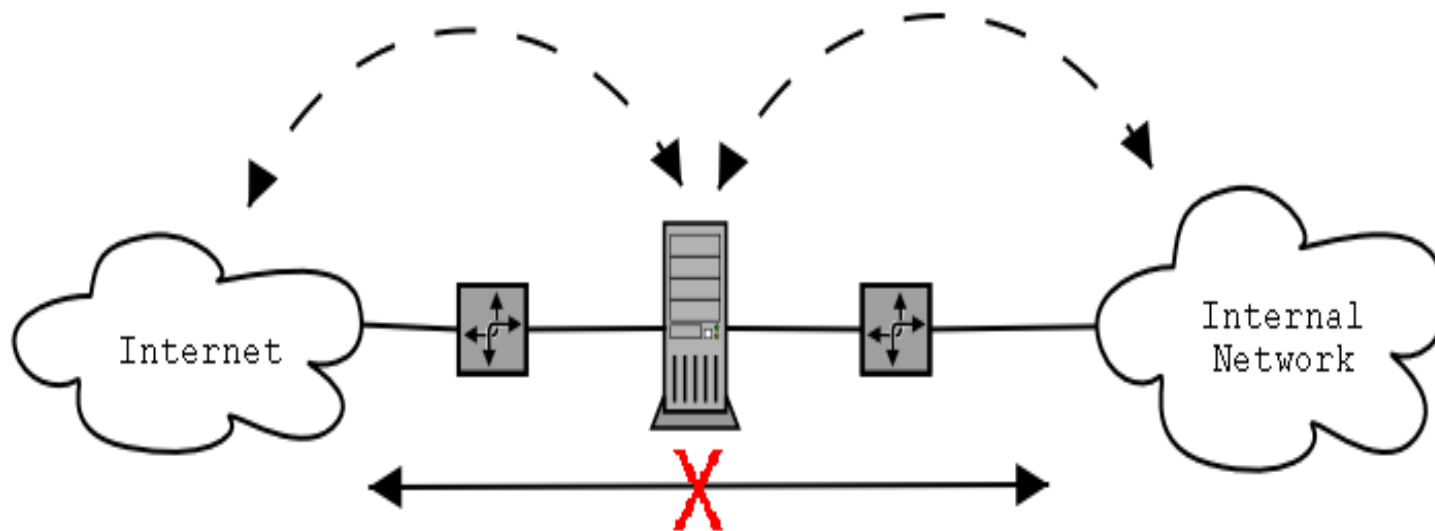
- Keep track of communications between hosts
- Significant improvement over simple packet filter
- Often used to limit connections to be made in one direction only
- Increases the complexity of the system
 - Complexity is the enemy of reliability/robustness
 - Communications fail if network state goes away

The screened subnet



Application layer gateway (proxy)

- No direction communications across boundary
- Results in total fair bit of state, fate and complexity
- Usable apps must be supported by the proxy



Intrusion Detection and Prevention Systems (IDS/IPS)

- Examine packets unobtrusively (usually)
- Maybe keep state
 - Fate of communications may not rely on it
 - If state goes away, things could keep working
- Report, or react on anomalies
 - Automated reaction could be used against you
- Difficult to minimize false positives/negatives

Security scenarios

- Half of you come up with a list of defenses
- Half of you come up with a list of attacks
- If you're just looking at these slides outside of class with no video, well, you should have been here