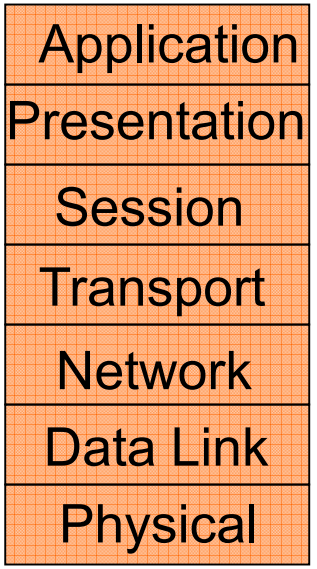
Network Security II

- Focus
  - How do we secure network systems?
- Topics
  - Example systems
  - Systems security issues at all levels



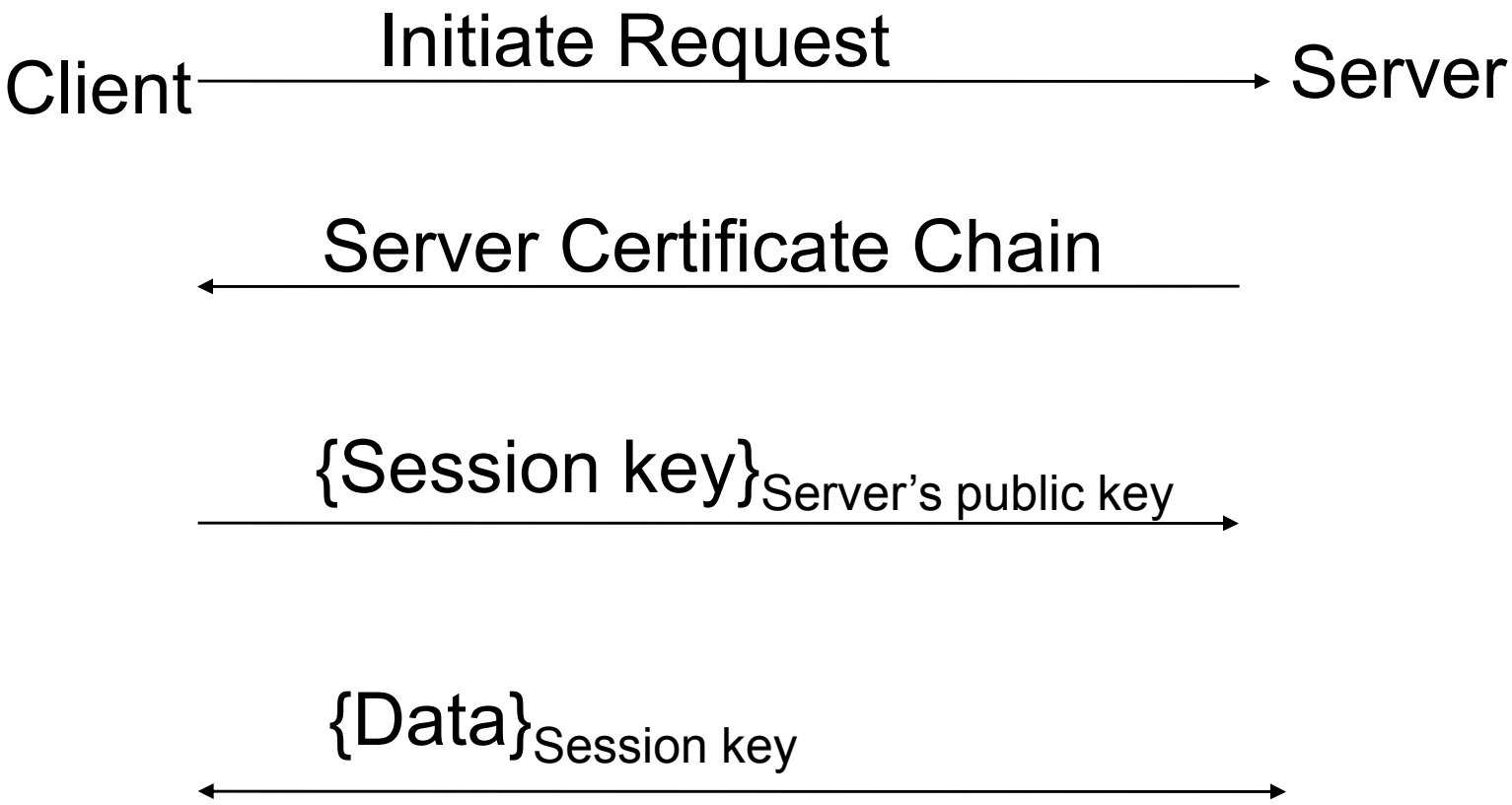
Example Systems

- Cryptography can be applied at multiple layers
- Secure Sockets (SSL) and Secure HTTP (HTTPS)
  - For secure Web transactions
- IP Security (IPSEC)
  - Framework for encrypting/authenticating IP packets
- Secure Shell (ssh)
  - Remote connection with encryption etc.
- 802.11i / WPA2
  - Protection at the 802.11 link layer

SSL/TLS and HTTPS

- Secure transport layer targeted at Web transactions
  - SSL/TLS inserted between TCP and HTTP to make secure HTTP
- Extra handshake phase to authenticate and exchange shared session keys
  - Client might authenticate Web server but not vice-versa
    - Certificate Authority embedded in Web browser
- Performance optimization
  - Refer to shared state with session id
  - Can use same parameters across connections
    - Client sends session id, allowing server to skip handshake

SSL/TLS


Client
Initiate Request
Server
Server Certificate Chain
{Session key}Server's public key
{Data}Session key

IPSEC

- Framework for encrypted IP packets
  - Choice of algorithms not specified
- Uses new protocol headers inside IPv4 packets
  - Authentication header
    - For message integrity and origin authenticity
    - Optionally “anti-replay” protection (via sequence number)
  - Encapsulating Security Payload
    - Adds encryption for privacy
- Depends on key distribution (ISAKAMP)
  - Sets up security associations
- Ex: secure tunnels between corporate offices

ssh

- Encrypted channel
  - Diffie-Hellman key exchange (plus negotiated encryption scheme)
- Authentication
  - Client has private key on local machine (usually in `~/.ssh/id_rsa`) and public key on remote machine (in `~/.ssh/authorized_keys`)
  - Server sends a challenge for client to sign using private key
  - Server verifies challenge using public key

WPA2 (or, roughly, 802.11i)

- Successor to a broken WEP …
- Encryption based on AES, versus older RC4
  - CCMP protocol (replaces TKIP and WEP) provides confidentiality and integrity/authenticity
- "Pre-shared key mode" means everyone already has a secret that is used for encryption / confidentiality
  - Common in homes
- Or 802.1X extensible authentication
  - 802.11 AP ("authenticator") routes new clients ("supplicants") to an a RADIUS server ("authentication server")
  - They authenticate, and if authorized get keys
  - Common in businesses

Putting it all together

- If we have confidentiality/integrity at one layer (e.g., SSL, IPSEC, 802.11i) then do we need it at other layers too?

Security in Context

- A system is only as secure as its weakest link
- Often that weakest link is you!
- Example: You're a registered user with, say, 25 online services. How many different passwords do you have?
  - Want "single sign-on"
  - Need either:
    - A client-side password manager, or
    - A central, trusted authority *a la* Kerberos (Microsoft Passport, Google Checkout)

Social engineering

- Con person into giving out information
- Phone secretary, say:
  - "Hi. I'm your company's IT administrator. Your boss is currently traveling, and I can't reach them. I need their password to verify their account hasn't been broken into. This is really urgent."
- Somebody phones you, and says:
  - "Hi. I'm with the Bank of America credit card fraud division. We've detected suspicious activity on your account, and we want to ensure you haven't become a victim of identity theft. Before we start, I need to verify your identity. What is your bank account number? SSN?"
- Often far more effective than technical attack
  - requires all people with access to sensitive information to be conscious of security issues

CBS NEWS

BACK PRINT

Patricia Dunn: I Am Innocent

PALO ALTO, Calif., Oct. 8, 2006

(CBS) The Hewlett-Packard board of directors was a leaky ship. Secret board deliberations were ending up in the press left and right, and it was decided something had to be done.

That something is arguably the most famous leak investigation since Watergate, and because of it Pattie Dunn, who was chairman of the HP board of directors, now faces criminal charges, and could go to jail.

As **correspondent Lesley Stahl** reports, the charges stem from the use of something called pretexting, where phone records are retrieved by subterfuge and pretense – where someone calls the phone company and pretends to be someone else in order to obtain the records.

The tactic was apparently used to retrieve the phone records not only of HP board members but of reporters as well. Social security numbers were also obtained, board members and journalists were followed, and there was even discussion of planting spies in newsrooms.

On Thursday, Pattie Dunn was booked on four felony counts in connection with the investigation.

Microsoft Security Bulletin MS01-017

Erroneous VeriSign-Issued Digital Certificates Pose Spoofing Hazard

Originally posted: March 22, 2001
Updated: June 23, 2003

Summary

Who should read this bulletin:
All customers using Microsoft® products.

Impact of vulnerability:
Attacker could digitally sign code using the name "Microsoft Corporation".

Recommendation:
All customers should install the update discussed below.

Technical description:

In mid-March 2001, VeriSign, Inc., advised Microsoft that on January 29 and 30, 2001, it issued two VeriSign Class 3 code-signing digital certificates to an individual who fraudulently claimed to be a Microsoft employee. The common name assigned to both certificates is "Microsoft Corporation". The ability to sign executable content using keys that purport to belong to Microsoft would clearly be advantageous to an attacker who wished to convince users to allow the content to run.

The certificates could be used to sign programs, ActiveX controls, Office macros, and other executable content. Of these, signed ActiveX controls and Office macros would pose the greatest risk, because the attack scenarios involving them would be the most straightforward. Both ActiveX controls and Word documents can be delivered via either web pages or HTML mails. ActiveX controls can be automatically invoked via script, and Word documents can be automatically opened via script unless the user has applied the Office Document Open Confirmation Tool.

United States | Microsoft.com Hor

Microsoft

Search Microsoft.c

Help and Support

Help and Support Home | Select a Product | Search Knowledge Base

Update Available to Revoke Fraudulent Microsoft Certificates Issued by VeriSign

View products that this article applies to.

This article was previously published under Q293811

Article ID : 293811
Last Review : October 27, 2006
Revision : 3.3

On This Page

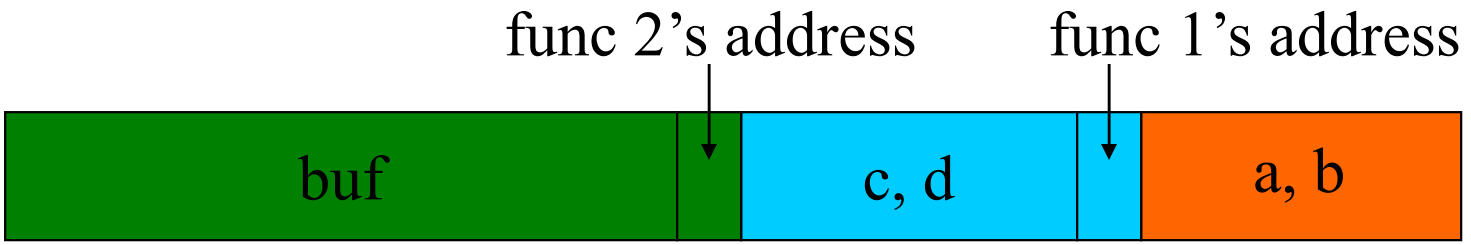
SUMMARY

In March, 2001, VeriSign, Inc. announced that it had issued two digital certificates to an individual who fraudulently claimed to be a Microsoft employee. This issue is discussed at length in Microsoft Security Bulletin MS01-017. VeriSign has revoked these certificates, and they are listed in the current VeriSign Certificate Revocation List (CRL). However, because the VeriSign code-signing certificates do not specify a CRL Distribution Point (CDP), it is not possible for any browser's CRL-checking mechanism to locate and use the VeriSign CRL. Microsoft has developed an update that rectifies this problem. The update package includes a CRL that contains the two certificates, and an installable revocation handler that consults the CRL on the local computer, rather than attempting to use the CDP mechanism.

Application Vulnerabilities

- Getting a network service to do something the designers didn't want
- The network isn't the fundamental weakness
  - Buffer overflows (unchecked input length)
    - Expecting 100 bytes, send lots more
  - SQL injection attacks
  - Open FTP servers that execute code
  - Many, many more…

buffer overflows on the stack




```
func_3()
{
   char buf[100];

   read_user_input(buf);
}
```

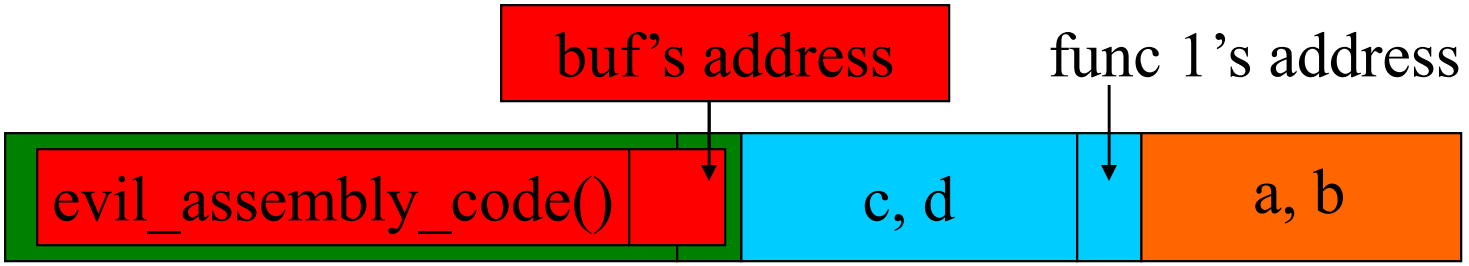
```
func_2()
{
   int c, d;

   func_3();
}
```

```
func_1()
{
   int a, b;

   func_2();
}
```

buffer overflows on the stack




```
func_3()
{
   char buf[100];

   read_user_input(buf);
}
```

```
func_2()
{
   int c, d;

   func_3();
}
```

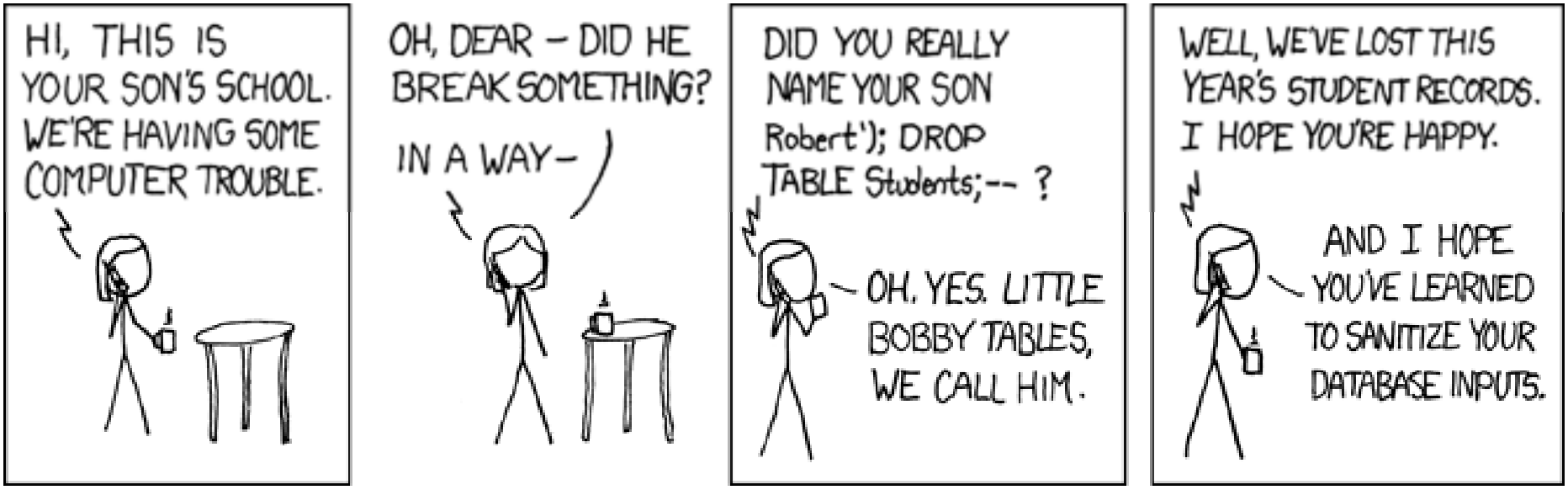
```
func_1()
{
   int a, b;

   func_2();
}
```

Attacker is supplying input to buf… so buf gets a very carefully constructed string containing assembly code, and overwriting func 2's address with buf's address. When func3 returns, it will branch to buf instead of func2.

SQL Injection

- Imagine a web site that takes your name, looks up info about you in a database
  - You might write code that says something like “select * from table where name=‘$NAME’
  - What if $NAME is:
    Joe’; update table set BankAccount=1000000 --


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

XKCD #327

Operation Bot Roast

HOME PAGE | MY TIMES | TODAY'S PAPER | VIDEO | MOST POPULAR | TIMES TOPICS

The New York Times

Technology

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

Search Tech News & 8,000+ Products

Go

Browse Products

-- Select a Product Category --

Go

Police swoop in on New Zealand botmaster

By LIAM TUNG, FOR ZDNET AUSTRALIA
Published: November 30, 2007

New Zealand Police this week cracked down on an alleged botnet ringleader in New Zealand, who the FBI claims had illegal control over 1 million computers.

SIGN IN TO E-MAIL OR SAVE THIS

PRINT

ARTICLE TOOLS SPONSORED BY

JUNO

c|net CNET News.com

More resources from CNET:

- More Tech News
- Download Free Shareware
- Find Product Reviews
- Compare Product Prices

Search CNET for:

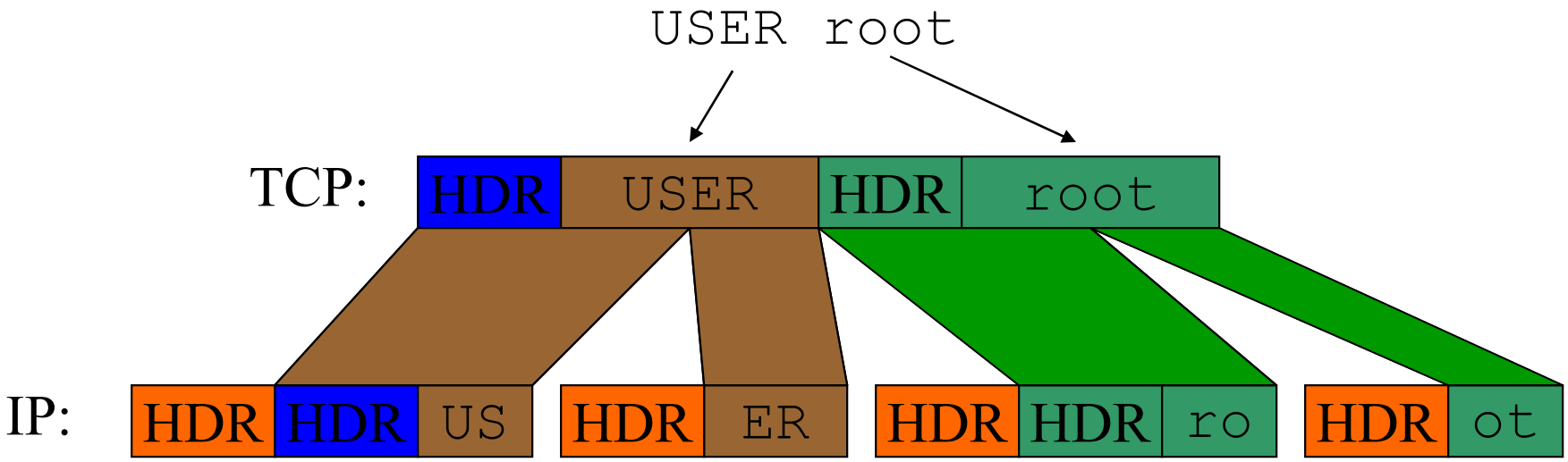
The sweep is part of the FBI's second phase of "Operation Bot Roast"--the same operation which resulted in four felony charges against 26-year-old Los Angeles security consultant John Schiefer.

Firewalls

- Originally, fairly basic: intent was to do per-packet inspection to block unused ports, for example
- Make sure we know exactly what's getting into the network and carefully think about their security
- Problem: a bug in your HTTP server (or its configuration) won't be caught by a basic firewall!
- Later firewalls became smarter – they'd reconstruct the flow. Keep per-flow state (previously impossible)
- Deny, for example, a HTTP request that contains "bobby tables".

Reconstructing Flows

- Let's say you want to search for the text "USER root". Is it enough to just search the data portion of TCP segments you see?



(Uh oh… we have to reassemble frags and resequence segs)

Fun with Fragments

Imagine an attacker sends:

1. 

2. 

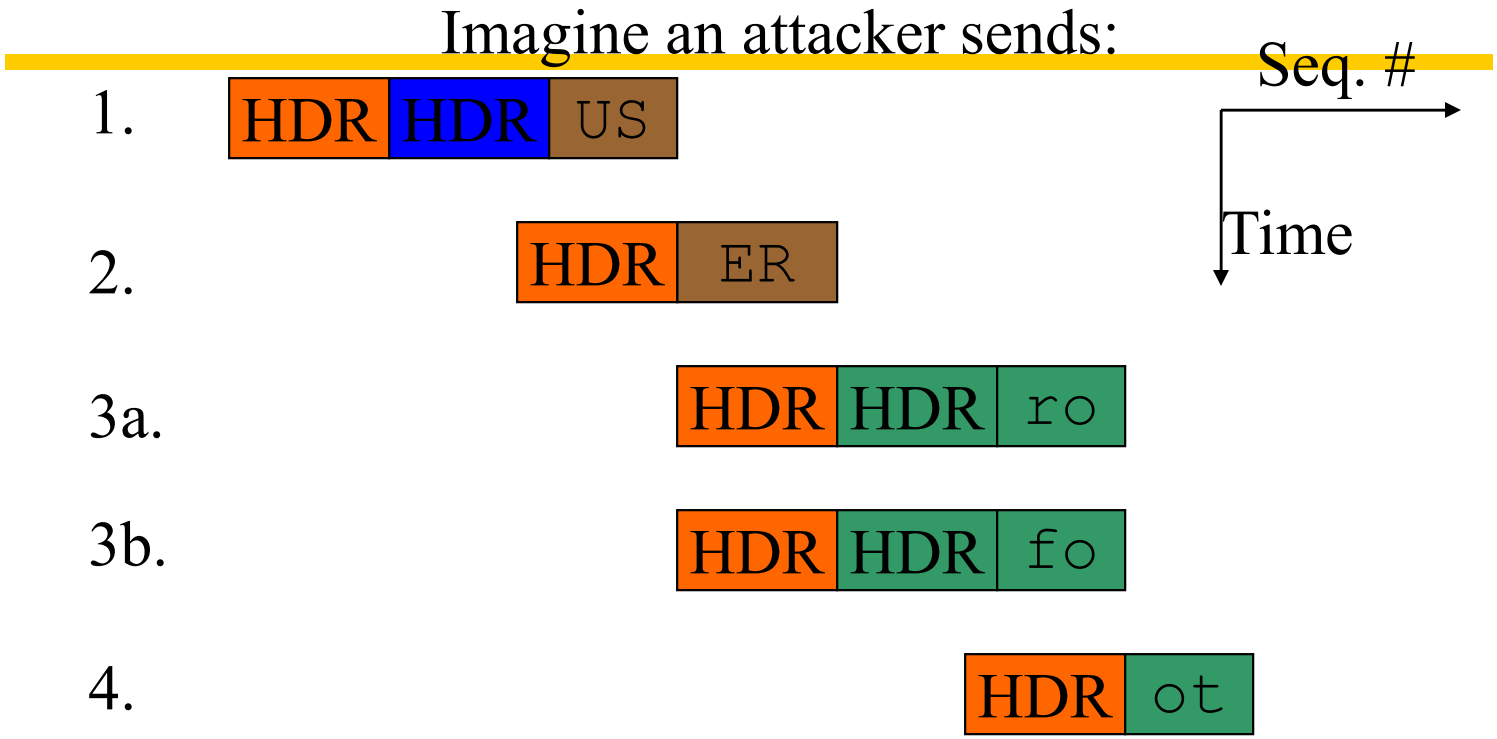
3. 1,000,000 unrelated fragments

4. 

5. 

Think of the entire campus as being a massively parallel computer.
That supercomputer is solving the flow-reconstruction problem.
Now we're asking a single host to try to solve that same problem.

More Fragment Fun



Should we consider 3a part of the data stream "USER root"?
Or is 3b part of the data stream? "USER foot"!

- If the OS makes a different decision than the monitor: Bad.
- Even worse: Different OS's have different protocol interpretations, so it's impossible for a firewall to agree with all of them

Trickery

- Non-standard parts of standards
  - IP fragment overlap behavior
  - TCP sequence number overlap behavior
  - Invalid combinations of TCP options
- Other ways to force a disparity between the monitor and the end-station
  - TTL
  - Checksum
  - Overflowing monitor buffers

See http://www.secnet.com/papers/ids-html/ for detailed examples

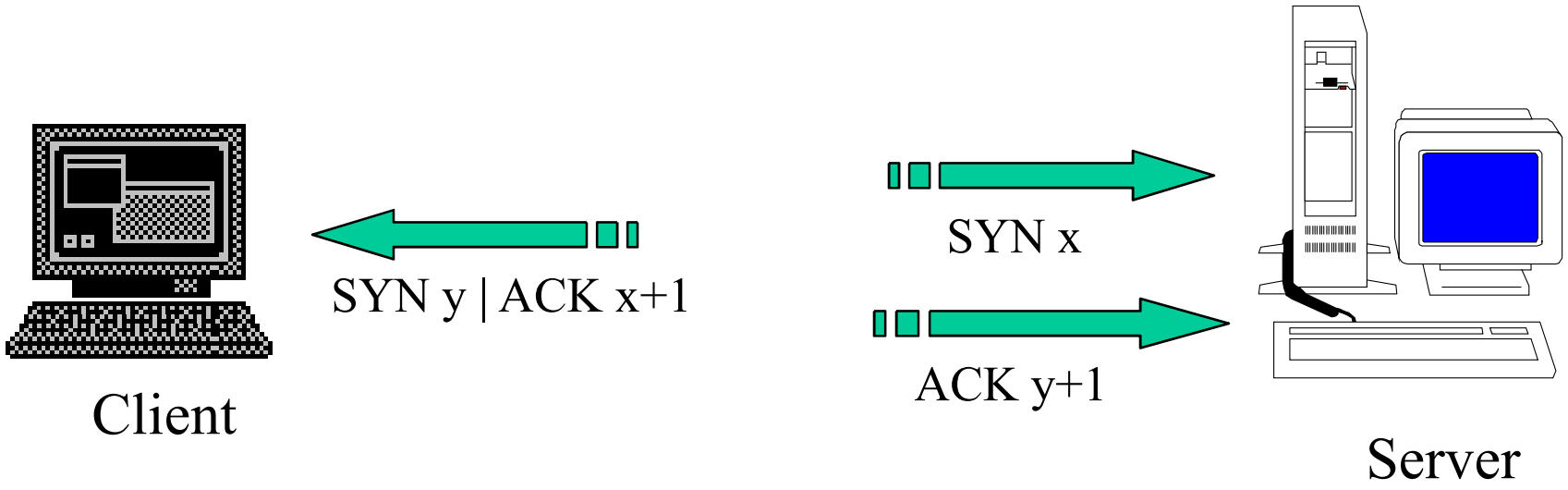
DNS Attacks

- Cache poisoning:
  - Ask for EVILHOST.COM (say, because of spam)
  - EvilHost.com's DNS server complies, but also "just happens" to tell you the IP of BankOfAmerica.com
  - DNS client puts it in cache. Fun!
  - Once this bug was found, DNS clients stopped accepting info they didn't request

TCP Layer Attacks / SYN flood

- TCP SYN Flooding
  - Exploit state allocated at server after initial SYN packet
  - Send a SYN and don't reply with ACK
  - Server will wait for 511 seconds for ACK
  - Finite queue size for incomplete connections (1024)
  - Once the queue is full it doesn't accept requests
- Solution: "Syn Cookies"
  - Construct a special sequence number that has connection info "encrypted"
  - Client sends it back with the ACK; re-encrypt and make sure it matches

(Remember the 3-way handshake)



TCP Session Hijack

- TCP Session Hijack
  - When is a TCP packet valid?
    - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it
      - Many earlier systems had predictable initial sequence number
  - Inject arbitrary data to the connection

TCP Session Poisoning

- TCP Session Poisoning
  - Send RST packet
    - Will tear down connection
  - Do you have to guess the exact sequence number?
    - Anywhere in window is fine
    - For 64k window it takes 64k packets to reset
    - About 15 seconds for a T1
  - Can reset BGP connections

Routing Attacks

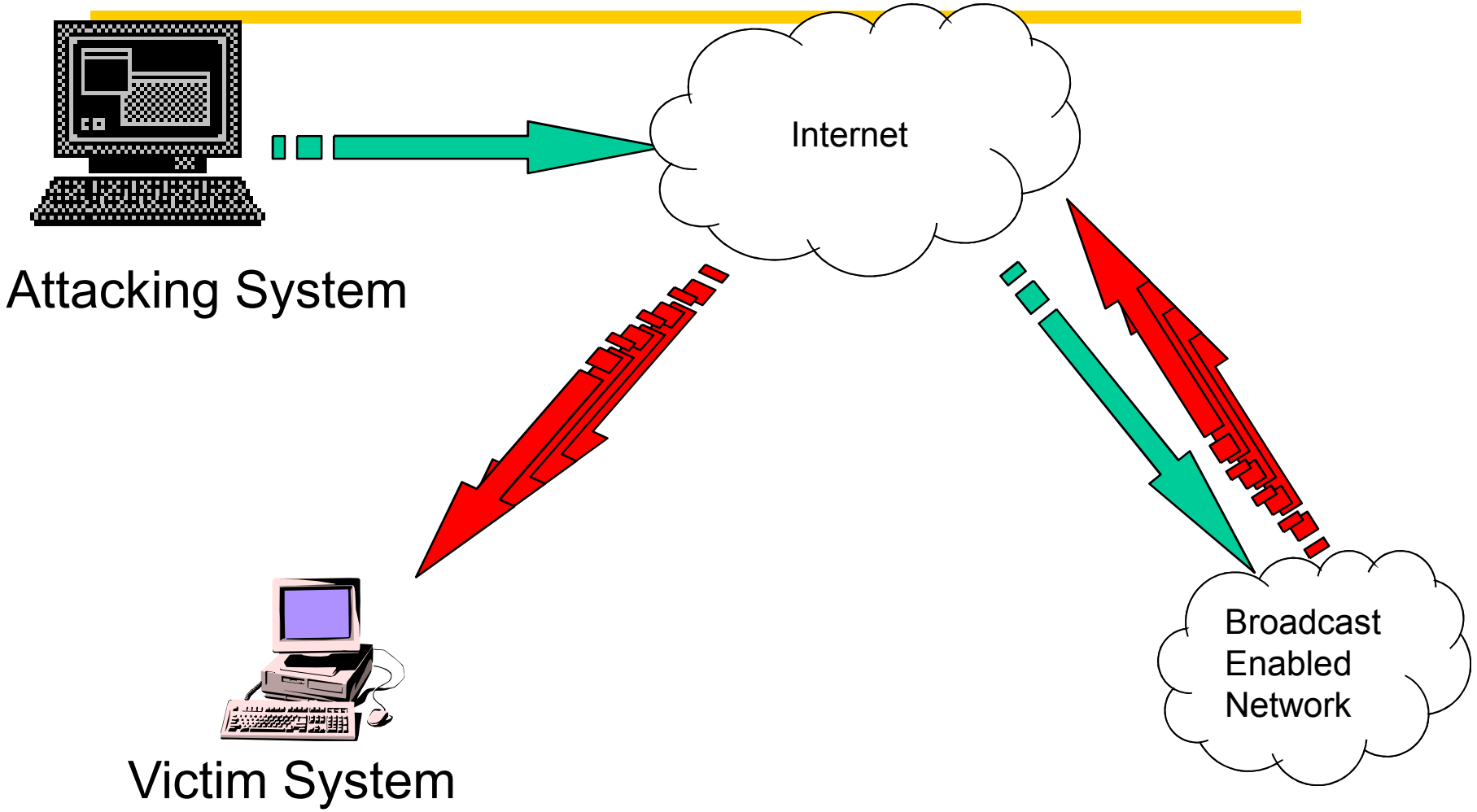
- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP
  - ASes can announce arbitrary prefix
  - ASes can alter path

- Today, these are generally just solved through reputation: don't accept updates from people you haven't arranged for in advance.

Security Flaws in IP

- Source IP address can be forged
  - Leads to the "Smurf Attack"
- Protocols that require no handshake (UDP) can be tricked if they do IP-based authentication
- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive
  - Denial of service

Ping Flood ("Smurf" attack)



ICMP Attacks

- No authentication
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - Man in the middle attack, sniffing
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
- Many more…
  - http://www.sans.org/rr/whitepapers/threats/477.php

Denial of Service

- Attacker can deny service to legitimate users if they can overwhelm the system providing the service
  - System is full of bugs … just send it packets that trigger them
  - System has limited bandwidth, CPU, memory, etc. … just sent it too many packets to handle
- Big issue in practice and lack of effective solutions
  - Today, patch as found (CERT) or build implementation to tolerate DOS
  - Tomorrow, design protocols to withstand, possibly network support for shutting down attack?
- Two broad classes:
  - Nasty packets trigger implementation bugs, e.g., Ping of Death
  - Packet floods target bandwidth, CPU, memory, e.g., SYN flood

Complication: Spoofed Addresses

- Why reveal your real address? Instead, "spoof" it.
  - Can implicate others and appear to be many hosts
- Solution?
  - Ingress filtering (ISPs check validity of source addresses) helps, but has poor incentive patterns and is not a complete solution
- Opportunity: "backscatter analysis"
  - host responds to spoofed packet, sends response packet to essentially random IP
  - if you have a large number of unused IPs, just listen and you'll hear the backscatter -- can measure DOS attacks!

Distributed DOS (DDOS)

- Use automated tools to set up a network of zombies
  - Trin00, TFN, mstream, Stacheldraht, …