CSE543 Computer and Network Security

Module: Network Security

Professor Trent Jaeger
Networking

• Fundamentally about transmitting information between two devices
• Direct communication is now possible between any two devices anywhere (just about)
  ▸ Lots of abstraction involved
  ▸ Lots of network components
  ▸ Standard protocols
  ▸ Wired and wireless
  ▸ Works in protection environment
• What about ensuring security?
The network...

Internet

LAN

(edge)

(perimeter)

(remote hosts/servers) (hosts/desktops)

(server)
The big picture ....

- Internet Protocol (IP)
  - Really refers to a whole collection of protocols making up the vast majority of the Internet

- Routing
  - How these packets move from place to place

- Network management
  - Administrators have to maintain the services and infrastructure supporting everyone’s daily activities
Network Security

• Every machine is connected
  ‣ What is trust model of the network?

• Not just limited to dogs as users
  ‣ What other ‘dogs’ are out there?
Network security: the high bits

• The network is …
  ‣ … a collection of interconnected computers
  ‣ … with resources that must be protected
  ‣ … from unwanted inspection or modification
  ‣ … while maintaining adequate quality of service.

• Another way of seeing network security is …
  ‣ … securing the network infrastructure such that the integrity, confidentiality, and availability of the resources is maintained.
The End-to-End Argument

• Clark et al. discussed a property of good systems that says features should be placed as close to resources as possible
  ‣ In communication, this means that we want the middle of the network to be simple, and the end-points to be smart (e.g., do everything you can at the end-points)
  • “Dumb, minimal network”
  ‣ This is the guiding principle of IP (Internet)
  ‣ Q: Does this have an effect on security?

• Note: this is a departure from the early networks which smart network, dumb terminals
Exploiting the network ...

• The Internet is extremely vulnerable to attack
  ‣ it is a huge open system ...
  ‣ which adheres to the *end-to-end* principle
    • smart end-points, dumb network

• Can you think of any *large-scale attacks* that would be enabled by this setup?
Security Problems in the TCP/IP Protocol Suite

• Bellovin’s observations about security problems in IP
  ‣ Not really a study of how IP is misused, e.g., IP addresses for authentication, but really what is inherently bad about the way in which IP is setup

• A really, really nice overview of the basic ways in which security and the IP design is at odds (circa 1989)
TCP/IP uses a *three-way handshake* to establish a connection:

1. $C \rightarrow S: Q_C$
2. $S \rightarrow C: Q_S, \text{ack}(Q_C)$ where sequence number $Q_S$ is nonce
3. $C \rightarrow S: \text{ack}(Q_S)$ … then send data

However, assume the bad guy does not hear msg 2, if he can guess $Q_S$, then he can get $S$ to accept whatever data it wants (useful if doing IP authentication, e.g., “rsh”).
Sequence Number Prediction (fixes)

- The only way you really fix this problem to stop making the sequence numbers predictable:
  - Randomize them -- you can use DES or some other mechanism to generate them randomly
  - There is an entire sub-field devoted to the creation and management of randomness in OSes

- Also, you could look for inconsistencies in timing information
  - Assumption: the adversary has different timing
  - OK, may be helpful, but far from definitive
What’s Changed?

- Collaborative TCP Sequence Number Inference Attack -- How to Crack Sequence Number Under A Second
  Zhiyun Qian, Z. Morley Mao, Yinglian Xie
  *In Proceedings of ACM Conference on Computer and Communications Security (CCS) 2012, Raleigh, NC.*

- Off-Path TCP Sequence Number Inference Attack -- How Firewall Middleboxes Reduce Security
  Zhiyun Qian, Z. Morley Mao

- Still have TCP sequence number attacks
Internet Control Message Protocol (ICMP)

- **ICMP** is used as a control plane for IP messages
  - Ping (connectivity probe)
  - Destination Unreachable (error notification)
  - Time-to-live exceeded (error notification)
- These are largely indispensable tools for network management and control
  - Error notification codes can be used to reset connections without any authentication
- **Solution:** verify/sanity check sources and content
  - ICMP “returned packets”
- **Real solution:** filter most of ICMP, ignore it
Address Resolution Protocol (ARP)

- Protocol used to map IP address onto the physical layer addresses (MAC)
  1) ARP request: who has x.x.x.x?
  2) ARP response: me!
- Policy: last one in wins
- Used to forward packets on the appropriate interfaces by network devices (e.g., bridges)

Q: Why would you want to spoof an IP address?
ARP poisoning

• Attack: replace good entries with your own
• Leads to
  ‣ Session hijacking
  ‣ Man-in-the-middle attacks
  ‣ Denial of service, etc.

• Lots of other ways to abuse ARP.
• Nobody has really come up with a good solution
  ‣ Except smart bridges, routers that keep track of MACs
• However, some not worried
  ‣ If adversary is in your perimeter, you are in big trouble
  ‣ You should validate the source of each packet independently
• Post office protocol - mail retrieval
  ‣ Passwords passed in the clear (duh)
  ‣ Solution: SSL, SSH, Kerberos

• Simple mail transport protocol (SMTP) - email
  ‣ Nothing authenticated: SPAM
  ‣ Nothing hidden: eavesdropping
  ‣ Solution: your guess is as good as mine

• File Transfer protocol - file retrieval
  ‣ Passwords passed in the clear (duh)
  ‣ Solution: SSL, SSH, Kerberos
DNS - The domain name system

• DNS maps between IP address (12.1.1.3) and domain and host names (ada.cse.psu.edu)
  ‣ How it works: the “root” servers redirect you to the top level domains (TLD) DNS servers, which redirect you to the appropriate sub-domain, and recursively ....
  ‣ Note: there are 13 “root” servers that contain the TLDs for .org, .edu, and country specific registries (.fr, .ch)
A DNS query

ISP Nameserver

User PC

DNS Cache

www.patrickmcdaniel.org = 207.140.168.131
“Glue” information

• Suppose you ask a name server for a record and it redirects you to another name server (NS record)
  ‣ e.g., if you ask a root for a NS (name server) record for NET, it returns NS records for the authoritative servers for .net
• It will also give you the A (resource) record for the authoritative servers you were directed to
  ‣ avoid looking them up
  ‣ This is known as the “glue” records
DNS Vulnerabilities

• **Nothing is authenticated**, so really the game is over
  ‣ You cannot really trust what you hear …
  ‣ But, many applications are doing just that.
  ‣ Spoofing of DNS is really dangerous

• **Moreover, DNS is a catalog of resources**
  ‣ Zone-transfers allow bulk acquisition of DNS data
  ‣ … and hence provide a map for attacking the network

• **Lots of opportunity to abuse the system**
  ‣ Relies heavily on caching for efficiency -- cache pollution
  ‣ Once something is wrong, it can remain that way in caches for a long time (e.g., it takes a long time flush)
  ‣ Data may be corrupted before it gets to authoritative server
A Cache Poisoning Attack

• All requests have a unique query ID
• The nameserver/resolver uses this information to match up requests and responses
• If an adversary can guess the query ID, then it can forge the responses and pollute the DNS cache
  ‣ 16-bit query IDs (not hard)
  ‣ Some servers increment IDs (or use other bad algo.)
  ‣ First one in wins!!!
• Note: If you can observe the traffic going to a name server, you can pretty much arbitrarily own the Internet for the clients it serves.
Kaminsky DNS Vulnerability

1. Query a random host in a victim zone, e.g., 1234.cse.psu.edu

2. Spoof responses* as before, but *delegate authority* to some server which you own.
   1. The glue records you give make you authoritative

3. You now own the domain.

*the original attack exploited poor ID selection
Kaminski Fixes

• Make the ID harder to guess (randomized ports)
  ‣ Amplified ID space from $2^{16}$ to $2^{27}$

• Prevent foreign requests from being processed
  ‣ E.g., filter requests from outside domain

• Observe and filter conflicting requests
  ‣ E.g., if you see a lot of bogus looking requests, be careful

• All of this treats the symptoms, not the disease.
  ‣ Lack of authenticated values
  ‣ Thus, if you can observe request traffic, prevent legitimate responses, or are just plain patient, you can mount these attacks.
Other Issues (Bailey et al)

- DNS Resolvers
  - Amplification attacks - Spoof IP address of DNS requestor
  - Disable recursive DNS resolution
- A and PTR records
  - Malicious IPs often have inconsistent A and PTR records
  - Make PTR records consistent with A records
- BGP Misconfiguration
  - Border Gateway Protocol (BGP) to exchange advertised routes
  - New route announcements should be infrequent and long-lived
- Egress Filtering
  - Prevent IP address spoofing by filtering egress packets not from inside your network
Configuration Guidelines

- Well-documented in published Request for Comments (RFCs) and Best Current Practices (BCPs)

<table>
<thead>
<tr>
<th>Symptoms</th>
<th>Best Current Practices</th>
<th>Functions</th>
<th>Attacks</th>
<th>Dataset</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Recursive Resolvers</td>
<td>BCP 140/RFC 5358</td>
<td>Naming Infrastructure</td>
<td>DNS Amplification</td>
<td>Global</td>
</tr>
<tr>
<td>DNS Source Port Randomization</td>
<td>RFC 5452</td>
<td>Naming Infrastructure</td>
<td>DNS Cache Poisoning</td>
<td>Global</td>
</tr>
<tr>
<td>Consistent A and PTR records</td>
<td>RFC 1912</td>
<td>Naming Infrastructure</td>
<td>-</td>
<td>Partial</td>
</tr>
<tr>
<td>BGP Misconfiguration</td>
<td>RFC 1918, RFC 6598</td>
<td>Routing Infrastructure</td>
<td>-</td>
<td>Global</td>
</tr>
<tr>
<td>Egress Filtering</td>
<td>BCP 38/RFC 2827</td>
<td>Transit</td>
<td>-</td>
<td>Partial</td>
</tr>
<tr>
<td>Untrusted HTTPS Certificates</td>
<td>RFC 5246, RFC 2459</td>
<td>Web Application</td>
<td>Man-in-the-middle</td>
<td>Global</td>
</tr>
<tr>
<td>Open SMTP Mail Relays</td>
<td>RFC 2505</td>
<td>Mail Application</td>
<td>SPAM</td>
<td>Global</td>
</tr>
<tr>
<td>Publicly Available out-of-band Management Devices</td>
<td>Manufacturer's Guideline</td>
<td>Server</td>
<td>Compromising Hosts</td>
<td>Global</td>
</tr>
</tbody>
</table>

TABLE I. SUMMARY OF MISMANAGEMENT METRICS AND THE THIRD-PARTY, PUBLIC DATA SOURCES USED FOR VALIDATION
DNSSEC

- A standard-based (IETF) solution to security in DNS
  - Prevents data spoofing and corruption
  - Public key based solution to verifying DNS data
  - Authenticates
    - Communication between servers
    - DNS data
      - content
      - existence
      - non-existence
    - Public keys (a bootstrap for PKI?)

Secure zones in .nl

NL public KEY

Current status of the secure .nl zones

<table>
<thead>
<tr>
<th>Zone</th>
<th>Status</th>
<th>Key id</th>
<th>Key alg</th>
</tr>
</thead>
<tbody>
<tr>
<td>dta.nl</td>
<td>active</td>
<td>613652</td>
<td>RSA/SHA1</td>
</tr>
<tr>
<td>freewan.nl</td>
<td>active</td>
<td>17907</td>
<td>RSA/SHA1</td>
</tr>
<tr>
<td>zt.net.nl</td>
<td>active</td>
<td>16310</td>
<td>RSA/SHA1</td>
</tr>
<tr>
<td>at.nl</td>
<td>active</td>
<td>35361</td>
<td>RSA/SHA1</td>
</tr>
<tr>
<td>openfortress.nl</td>
<td>active</td>
<td>42325</td>
<td>RSA/SHA1</td>
</tr>
<tr>
<td>fn.nl</td>
<td>processing</td>
<td>16217</td>
<td>RSA/SHA1</td>
</tr>
</tbody>
</table>
DNSSEC Mechanisms

- Securing the DNS records
  - Each domain signs their “zone” with a private key
  - Public keys published via DNS
  - *Indirectly* signed by parent zones
  - Ideally, you only need a self-signed root, and follow keys down the hierarchy
DNSSEC Mechanisms

• **TSIG**: transaction signatures protect DNS operations
  ‣ Zone loads, some server to server requests (master -> slave), etc.
  ‣ Time-stamped signed responses for dynamic requests
  ‣ A misnomer -- it currently uses shared secrets for TSIG (HMAC) or do real signatures using public key cryptography

• **SIG0**: a public key equivalent of TSIG
  ‣ Works similarly, but with public keys
  ‣ Not as popular as TSIG

• Note: these mechanisms assume clock sync. (NTP)