APRICOT 2014

Network Security Tutorial

Petaling Jaya, Malaysia

25 February 2014

Presenter

Sheryl Hermoso (Shane)

Training Officer, APNIC

Sheryl has had various roles as a Network and Systems Administrator prior to joining APNIC. Starting her career as a Technical Support Assistant while studying at the University of the Philippines. Sheryl later finished her degree in Computer Engineering and continued to work in the same university as a Network Engineer, where she managed the DILNET network backbone and wireless infrastructure.

Areas of interests:

IPv6, DNS/DNSSEC, Network Security, IRM

Contact:

Email: sheryl@apnic.net

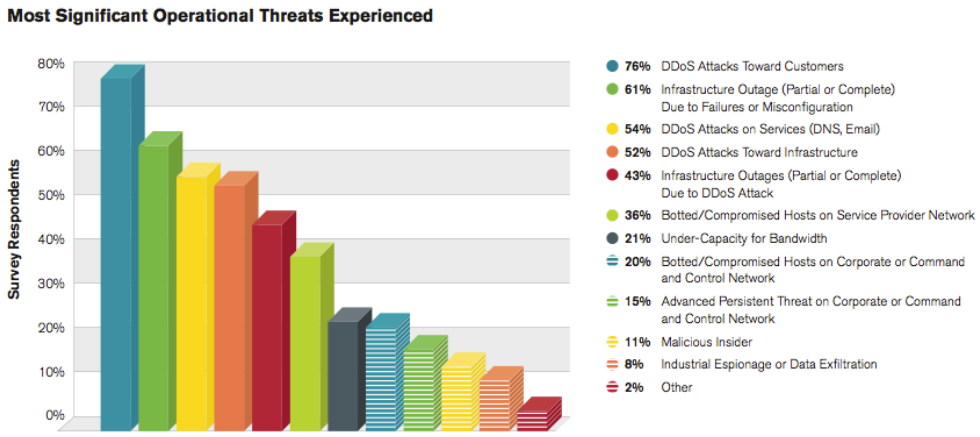
Overview

- Network Security Fundamentals
- Security on Different Layers and Attack Mitigation
- Cryptography
- Resource Registration
- RPKI and Resource Certification

APRICOT 2014

Network Security Fundamentals

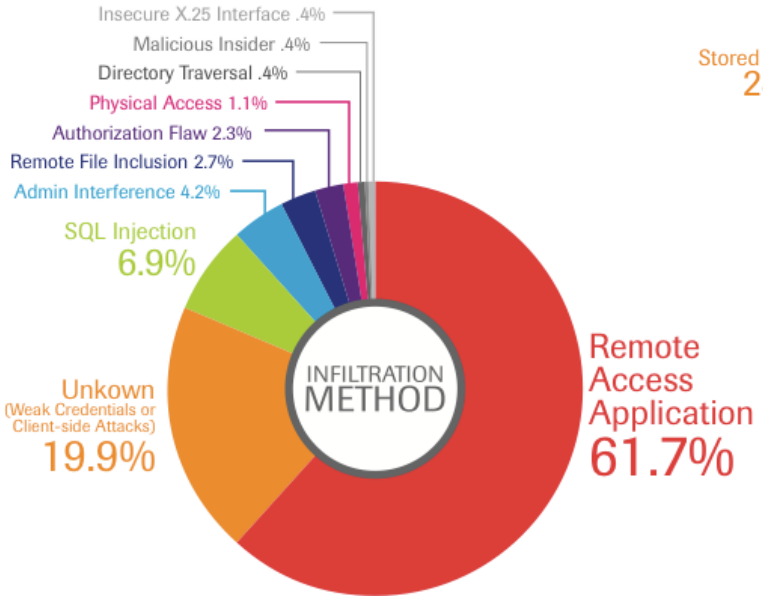
Attack Trends



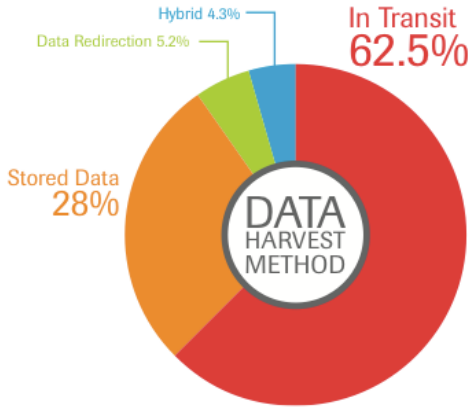
- Hacktivism and vandalism are the common DDoS attack motivation
- High-bandwidth DDoS attacks are the ‘new normal’
- First-ever IPv6 DDoS attacks are reported in 2011
- Trust issues across geographic boundaries

Source: Arbor Networks Worldwide Infrastructure Security Report Volume VIII

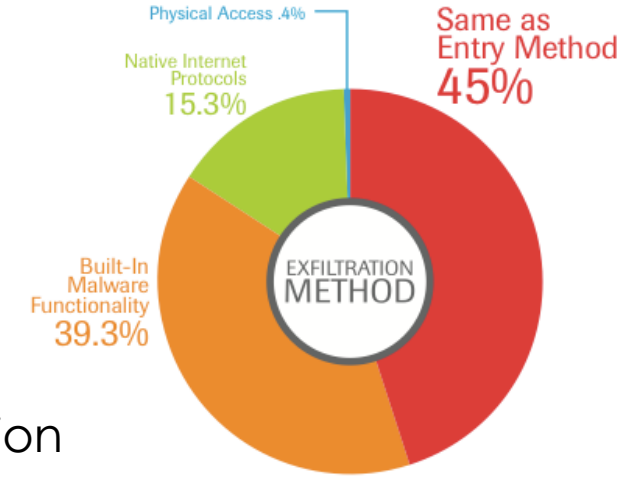
Attack Trends - Breach Sources



Infiltration



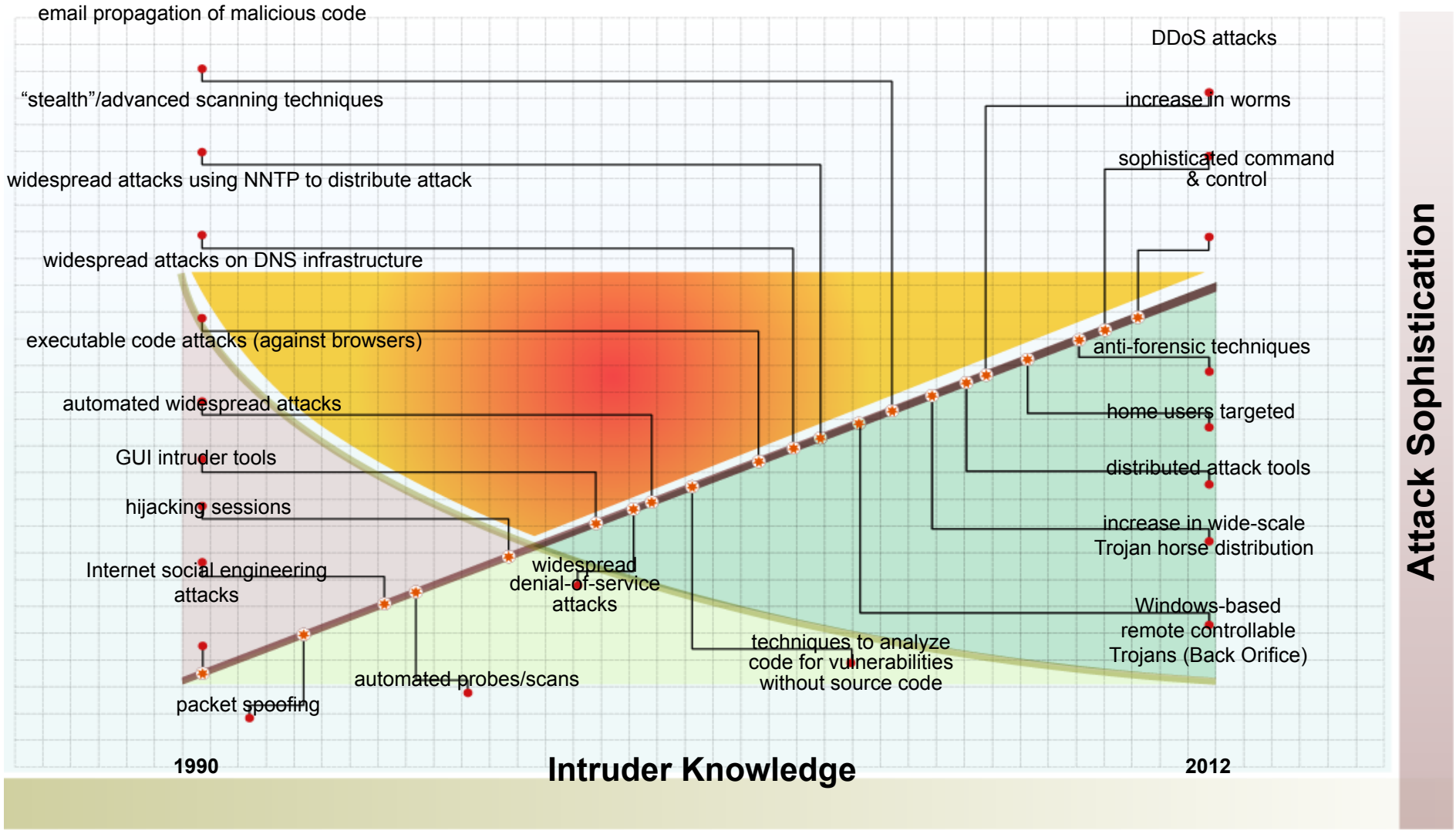
Aggregation



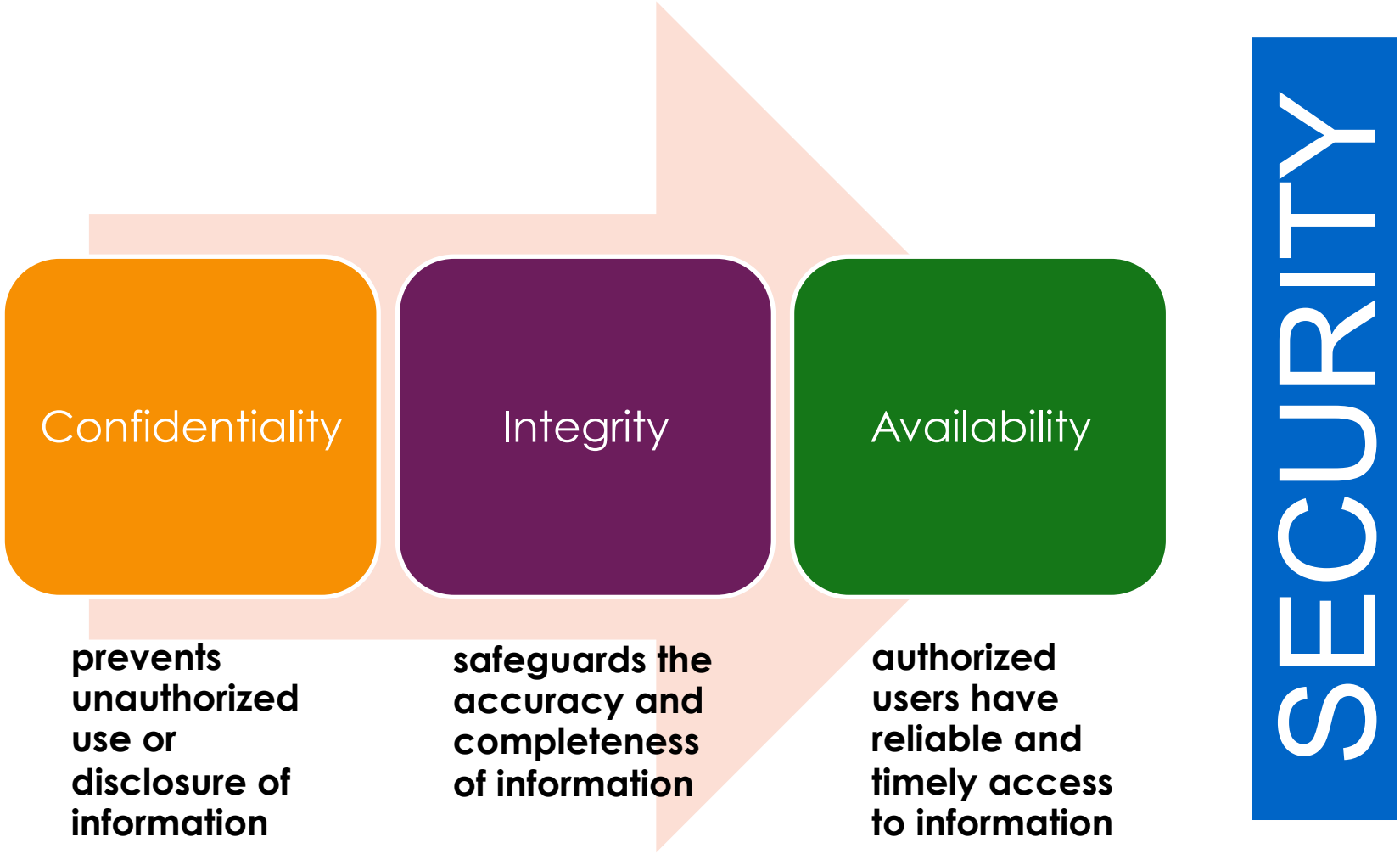
Exfiltration

Source: Trustwave 2012 Global Security Report

Evolution of Attack Landscape



Goals of Information Security



Access Control

- The ability to permit or deny the use of an object by a subject.
- It provides 3 essential services:
  - Authentication (who can login)
  - Authorization (what authorized users can do)
  - Accountability (identifies what a user did)

Authentication

- A means to verify or prove a user's identity
- The term "user" may refer to:
  - Person
  - Application or process
  - Machine or device
- Identification comes before authentication
  - Provide username to establish user's identity
- To prove identity, a user must present either of the following:
  - What you know (passwords, passphrase, PIN)
  - What you have (token, smart cards, passcodes, RFID)
  - Who you are (biometrics such as fingerprints and iris scan, signature or voice)

Trusted Network

- Standard defensive-oriented technologies
  - Firewall – first line of defense
  - Intrusion Detection – second line of defense
- Build TRUST on top of the TCP/IP infrastructure
  - Strong authentication
    - Two-factor authentication
    - something you have + something you know
  - Public Key Infrastructure (PKI)

Strong Authentication

- An absolute requirement
- Two-factor authentication
  - Passwords (something you know)
  - Tokens (something you have)
- Examples:
  - Passwords
  - Tokens
  - Tickets
  - Restricted access
  - PINs
  - Biometrics
  - Certificates

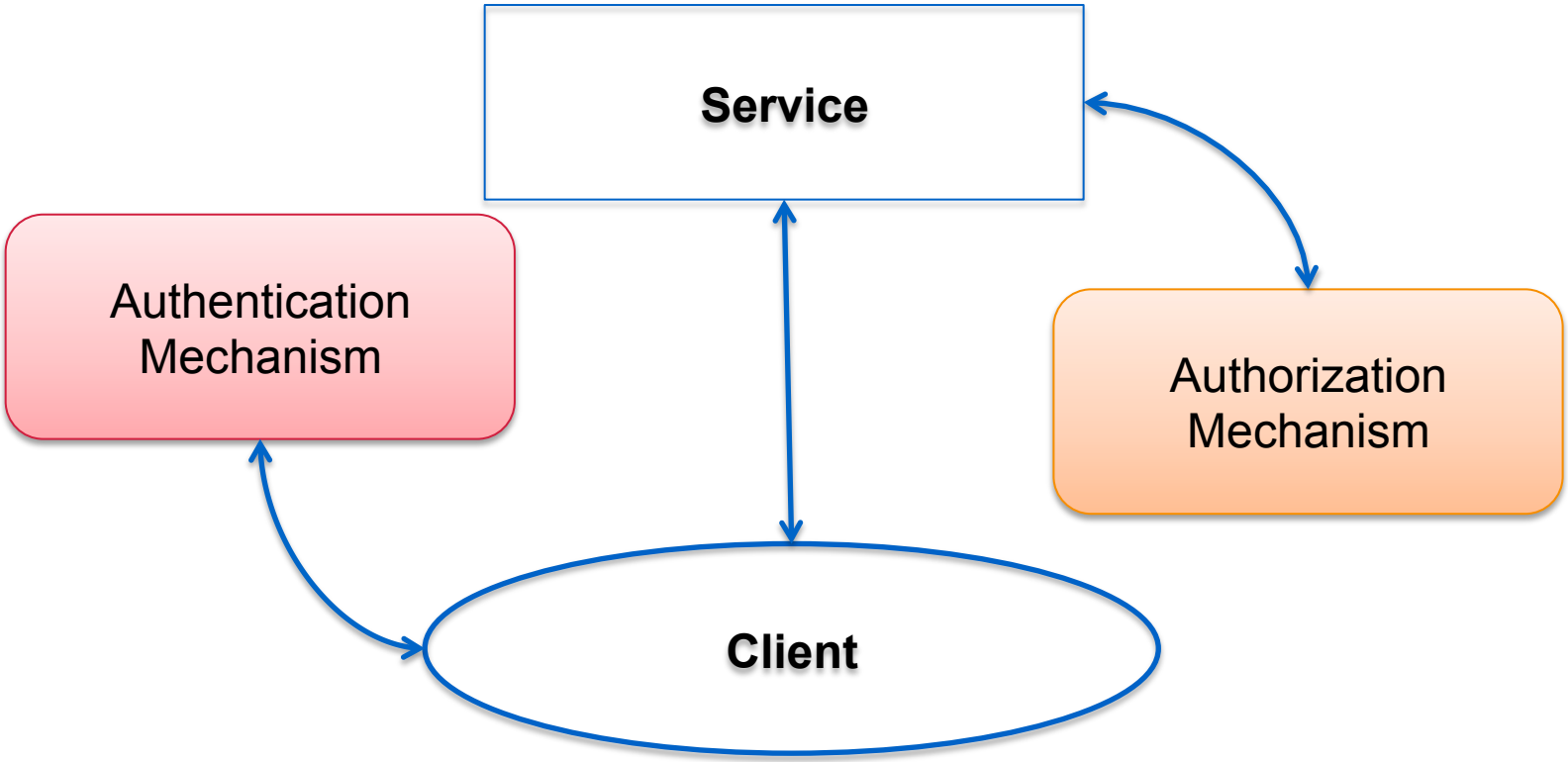
Two-factor Authentication

- Requires a user to provide at least two authentication ‘factors’ to prove his identity
  - something you know
    Username/userID and password
  - something you have
    Token using a one-time password (OTP)
- The OTP is generated using a small electronic device in physical possession of the user
  - Different OTP generated each time and expires after some time
  - An alternative way is through applications installed on your mobile device
- Multi-factor authentication is also common

Authorization

- Defines the user's rights and permissions on a system
- Typically done after user has been authenticated
- Grants a user access to a particular resource and what actions he is permitted to perform on that resource
- Access criteria based on the level of trust:
  - Roles
  - Groups
  - Location
  - Time
  - Transaction type

Authentication vs. Authorization



"Authentication simply identifies a party, authorization defines whether they can perform certain action" – RFC 3552

Accountability

- The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity
  - Senders cannot deny sending information
  - Receivers cannot deny receiving it
  - Users cannot deny performing a certain action
- Supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention and after-action recovery and legal action

Source: NIST Risk Management Guide for Information Technology Systems

Threats, Risk and Vulnerability

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
    - Denial of Service / Unauthorized Access / Impersonation / Worms / Viruses
- Vulnerability
  - A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
- Risk
  - The possibility that a particular vulnerability will be exploited
    - Risk analysis: The process of identifying security risks, determining their impact, and identifying areas requiring protection

Threat

- “a motivated, capable adversary”
- Examples:
  - Human Threats
    - Intentional or unintentional
    - Malicious or benign
  - Natural Threats
    - Earthquakes, tornadoes, floods, landslides
  - Environmental Threats
    - Long-term power failure, pollution, liquid leakage

Vulnerability

- A weakness in security procedures, network design, or implementation that can be exploited to violate a corporate security policy
  - Software bugs
  - Configuration mistakes
  - Network design flaw
  - Lack of encryption
- Where to check for vulnerabilities?
- Exploit
  - Taking advantage of a vulnerability

Risk

- Likelihood that a vulnerability will be exploited
- Some questions:
  - How likely is it to happen?
  - What is the level of risk if we decide to do nothing?
  - Will it result in data loss?
  - What is the impact on the reputation of the company?
- Categories:
  - High, medium or low risk

Attack Motivation

- Criminal
  - Criminal who use critical infrastructure as a tools to commit crime
  - Their motivation is money
- War Fighting/Espionage/Terrorist
  - What most people think of when talking about threats to critical infrastructure
- Patriotic/Principle
  - Large groups of people motivated by cause - be it national pride or a passion aka Anonymous

Attack Motivation

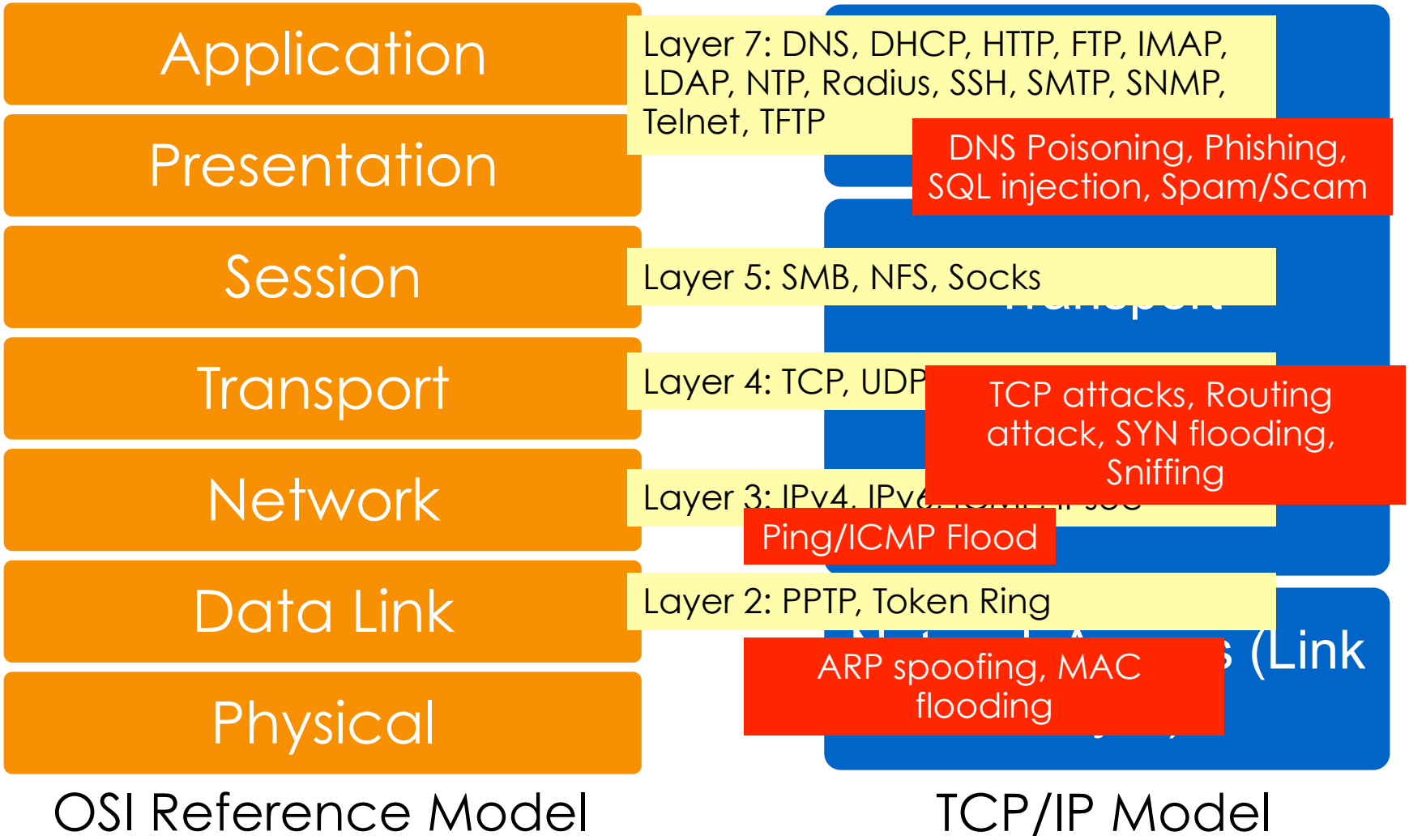
- Nation States want **SECRETS**
- Organized criminals want **MONEY**
- Protesters or activists want **ATTENTION**
- Hackers and researchers want **KNOWLEDGE**

(copied from NANOG60 keynote presentation by Jeff Moss, Feb 2014)

Common Types of Attack

- Ping sweeps and port scans - reconnaissance
- Sniffing – capture packet as they travel through the network
- Man-in-the-middle attack – intercepts messages that are intended for a valid device
- Spoofing - sets up a fake device and trick others to send messages to it
- Hijacking – take control of a session
- Denial of Service (DoS) and Distributed DoS (DDoS)

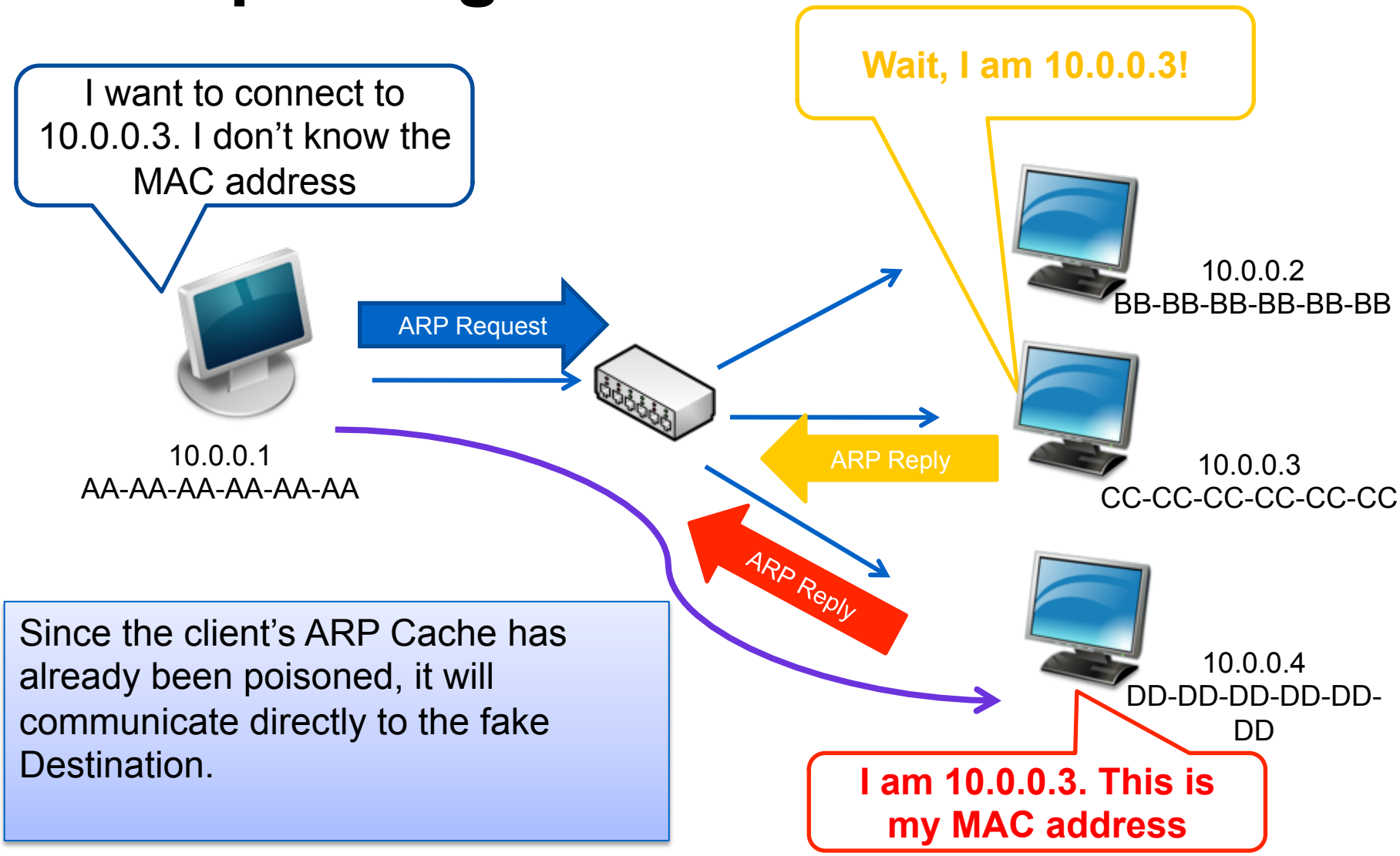
Attacks on Different Layers



Layer 2 Attacks

- ARP Spoofing
- MAC attacks
- DHCP attacks
- VLAN hopping

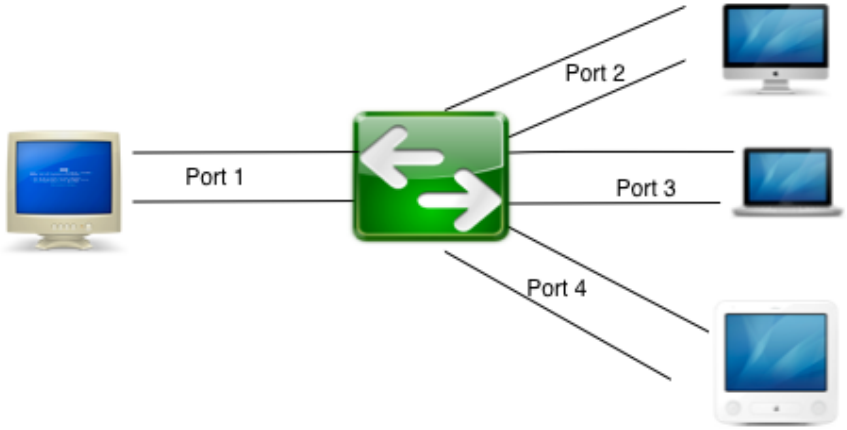
ARP Spoofing



Since the client's ARP Cache has already been poisoned, it will communicate directly to the fake Destination.

MAC Flooding

- Exploits the limitation of all switches – fixed CAM table size
- CAM = Content Addressable memory = stores info on the mapping of individual MAC addresses to physical ports on the switch.

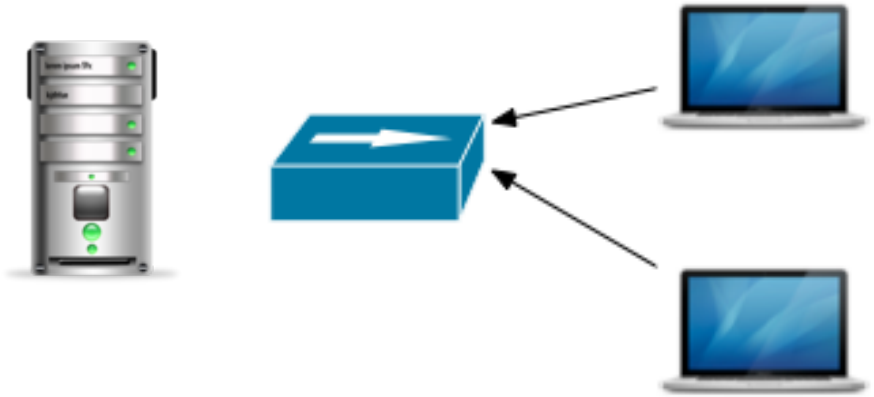


	Port 1	Port 2	Port 3	Port 4
00:01:23:45:67:A1	x			
00:01:23:45:67:B2		x		
00:01:23:45:67:C3			x	
00:01:23:45:67:D4				x

DHCP Attacks

- DHCP Starvation Attack
  - Broadcasting vast number of DHCP requests with spoofed MAC address simultaneously.
  - DoS attack using DHCP leases
- Rogue DHCP Server Attacks

Server runs out of IP addresses to allocate to valid users



Attacker sends many different DHCP requests with many spoofed addresses.

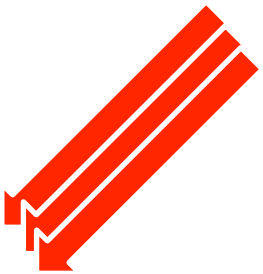
Layer 3 Attacks

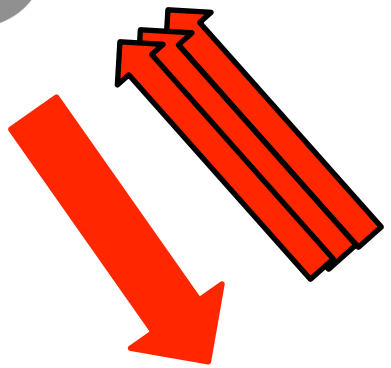
- ICMP Ping Flood
- ICMP Smurf
- Ping of death

Ping Flood

Attacker

Internet





Victim

Other forms of ICMP attack:
-Ping of death
-ICMP ping flood

Broadcas
t Enabled
Network

Mitigating Sniffing Attacks

- Avoid using insecure protocols like basic HTTP authentication and telnet.
- If you have to use an insecure protocol, try tunneling it through something to encrypt the sensitive data.
- Run ARPwatch.
- Try running tools like `sniffdet` and Sentinel to detect network cards in promiscuous mode that may be running sniffing software.

Routing Attacks

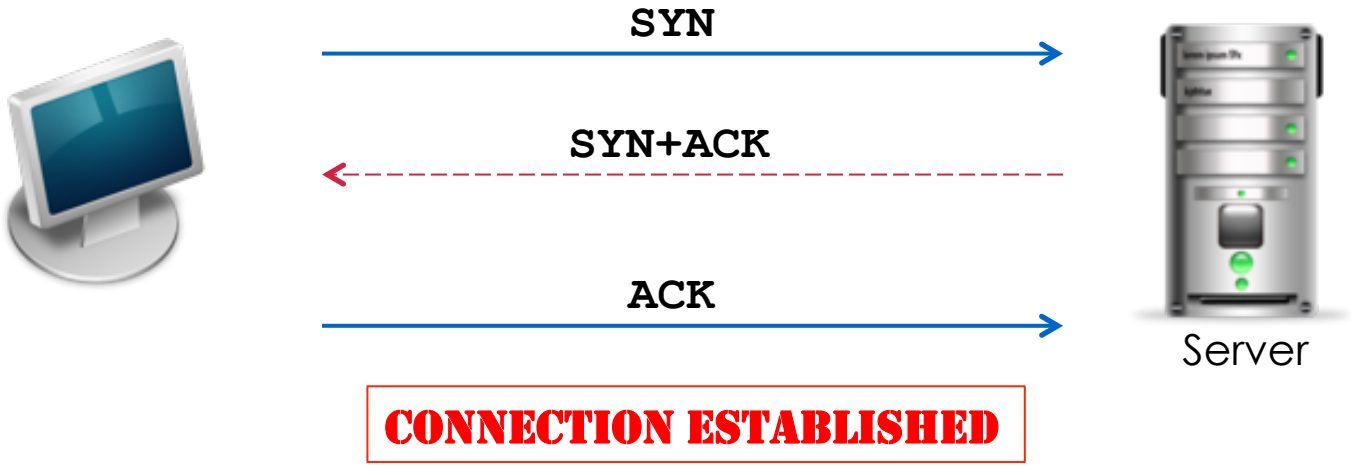
- Attempt to poison the routing information
- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP attacks
  -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

TCP Attacks

- SYN Flood – occurs when an attacker sends SYN requests in succession to a target.
- Causes a host to retain enough state for bogus half-connections such that there are no resources left to establish new legitimate connections.

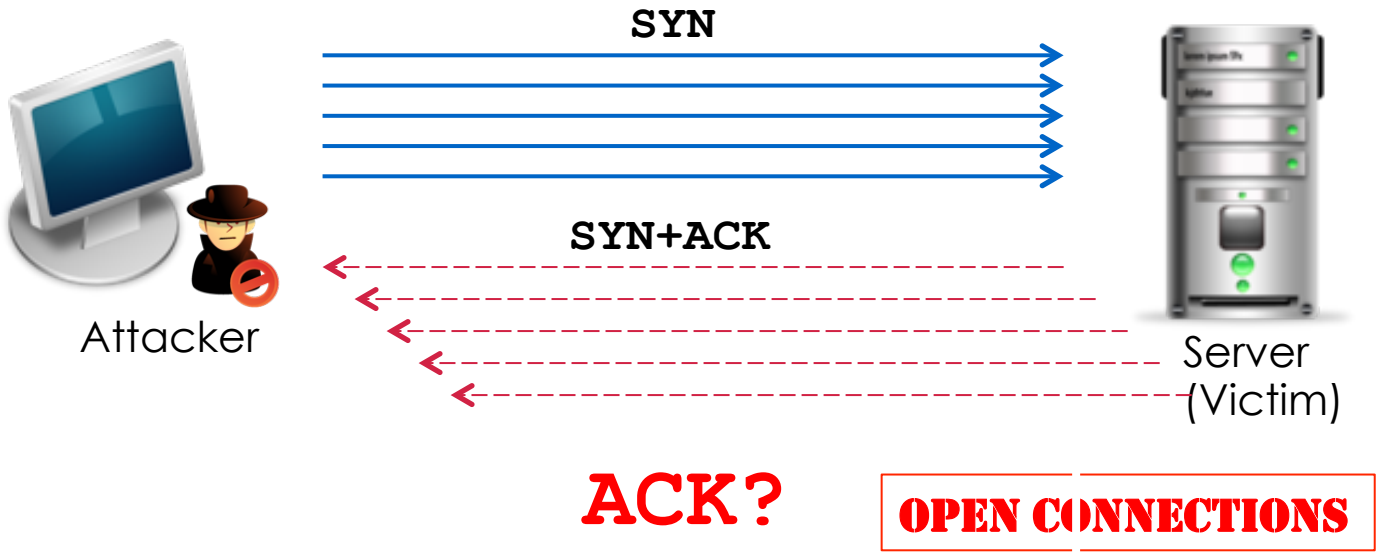
TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



TCP Attacks

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



Application Layer Attacks

- Applications don't authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

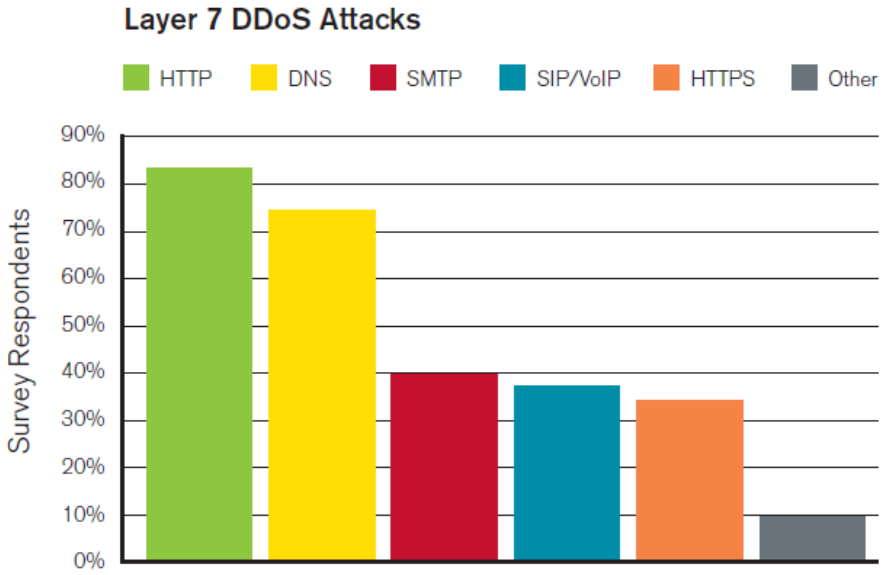


Figure 8
Source: Arbor Networks, Inc.

Application Layer Attacks

- Scripting vulnerabilities
- Cookie poisoning
- Buffer overflow
- Hidden field manipulation
- Parameter tampering
- Cross-site scripting
- SQL injection

Application Layer DDoS: Slowloris

- Incomplete HTTP requests
- Properties
  - Low bandwidth
  - Keep sockets alive
  - Only affects certain web servers
  - Doesn't work through load balancers
  - Managed to work around accf_http

Web Application Security Risks

- Injection
- Cross-Site Scripting
- Broken authentication and Session Management
- Insecure Direct Object References
- Cross-site Request Forgery (CSRF)
- Insecure Cryptographic Storage
- Failure to Restrict URL Access
- Insufficient Transport Layer Protection
- Unvalidated Redirects and Forwards

Source: OWASP Top 10 Application Security Risks, 2010

DNS Changer

- “Criminals have learned that if they can control a user’s DNS servers, they can control what sites the user connects to the Internet.”
- How: infect computers with a malicious software (malware)
- This malware changes the user’s DNS settings with that of the attacker’s DNS servers
- Points the DNS configuration to DNS resolvers in specific address blocks and use it for their criminal enterprise
- For more: see the NANOG presentation by Merike

Rogue DNS Servers

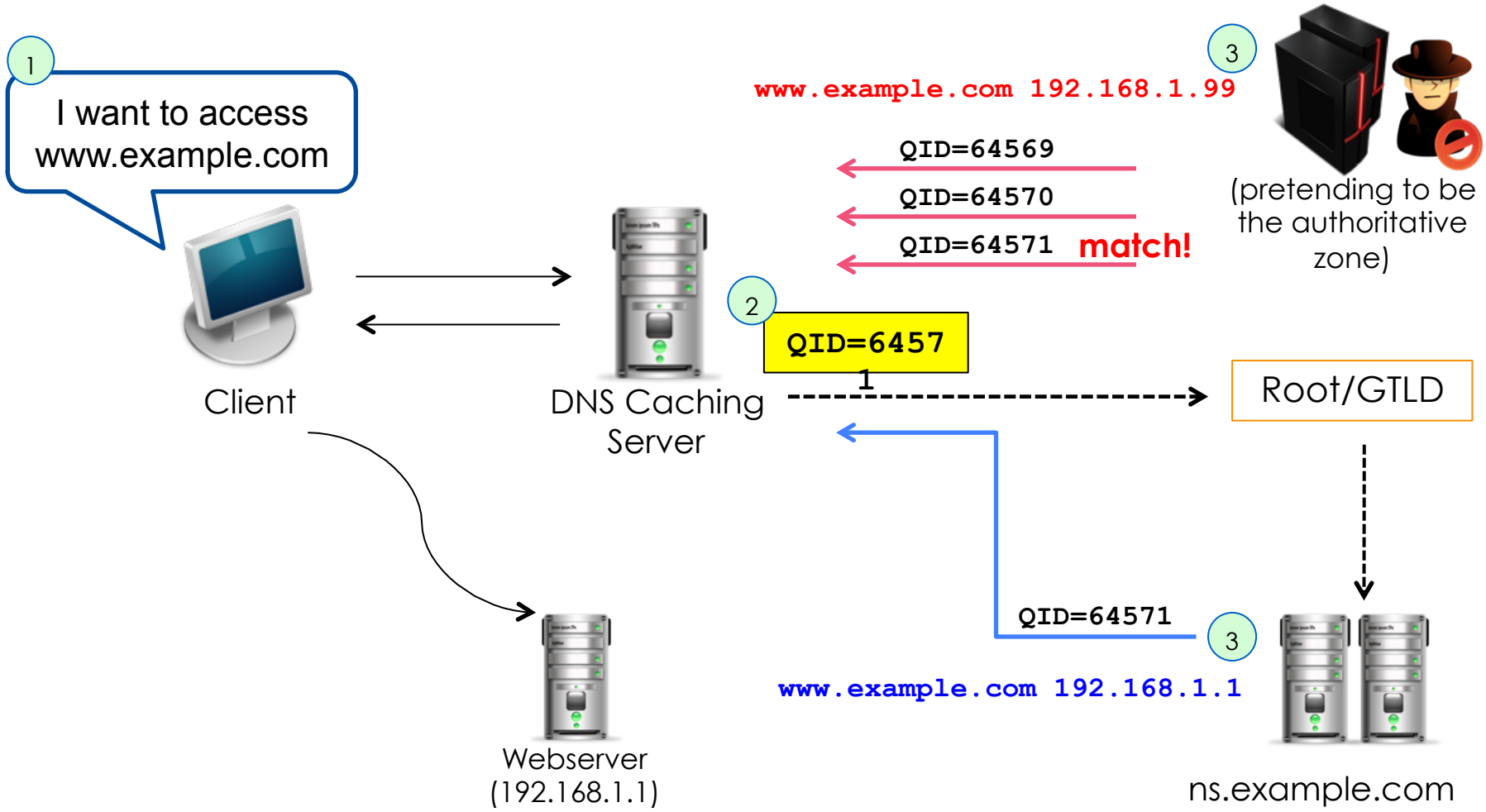
- 85.225.112.0 through 85.255.127.255
- 67.210.0.0 through 67.210.15.255
- 93.188.160.0 through 93.188.167.255
- 77.67.83.0 through 77.67.83.255
- 213.109.64.0 through 213.109.79.255
- 64.28.176.0 through 64.28.191.255

- If your computer is configured with one of these DNS servers, it is most likely infected with DNSChanger malware

DNS Cache Poisoning

- Caching incorrect resource record that did not originate from authoritative DNS sources.
- Result: connection (web, email, network) is redirected to another target (controlled by the attacker)

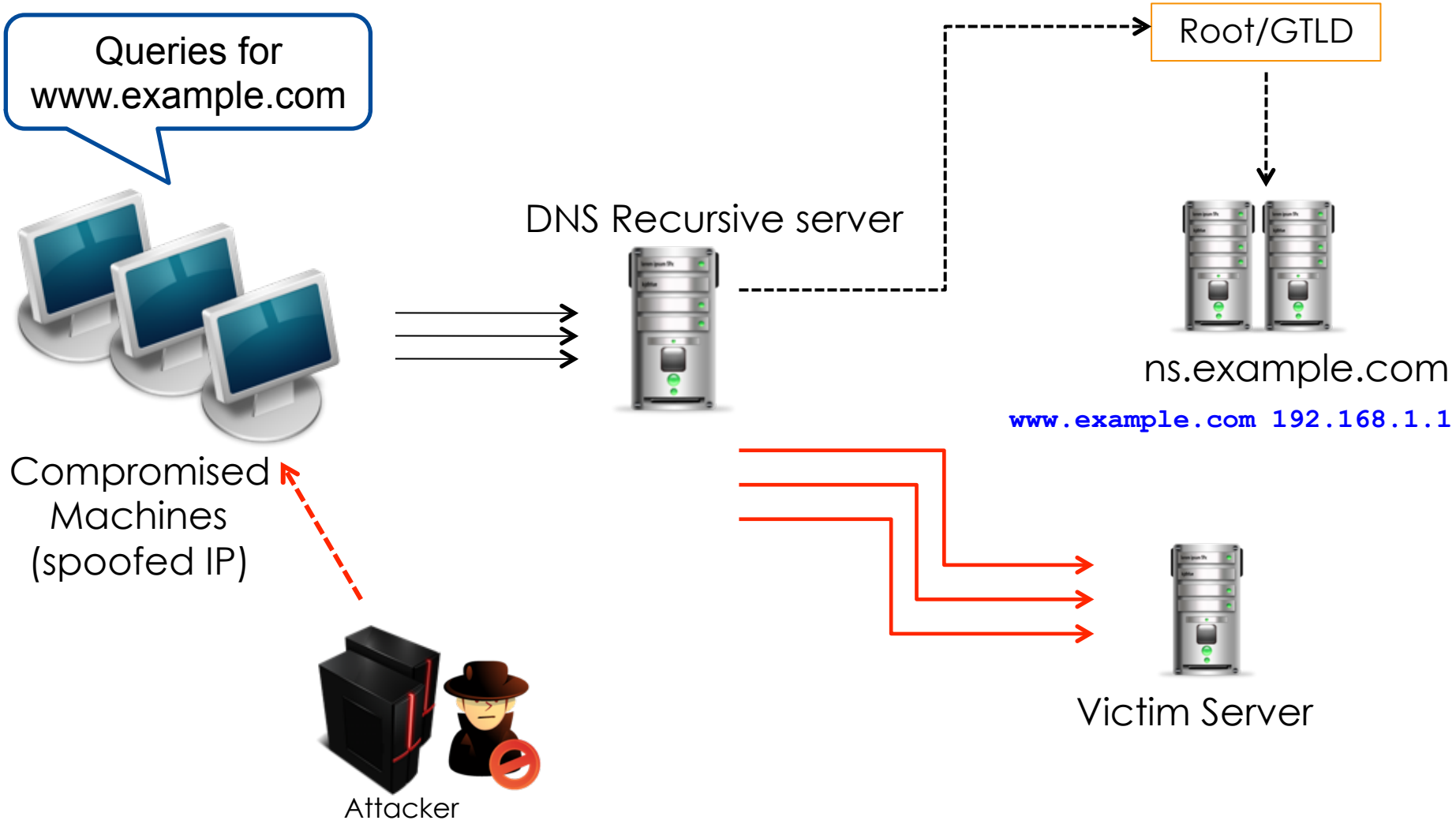
DNS Cache Poisoning



DNS Amplification

- A type of reflection attack combined with amplification
  - Source of attack is reflected off another machine
  - Traffic received is bigger (amplified) than the traffic sent by the attacker
- UDP packet's source address is spoofed

DNS Amplification Attack



Wireless Attacks

- WEP – first security mechanism for 802.11 wireless networks
- Weaknesses in this protocol were discovered by Fluhrer, Mantin and Shamir, whose attacks became known as “FMS attacks”
- Tools were developed to automate WEP cracking
  - Chopping attacks were released to crack WEP more effectively and faster
- Cloud-based WPA cracker
  - https://www.wpacracker.com/

Botnet

- Collection of compromised computers (or ‘bot’)
- Computers are targeted by malware (malicious software)
- Once controlled, an attacker can use the compromised computer via standards-based network protocol such as IRC and HTTP
- How to become a bot:
  - Drive-by downloads (malware)
  - Go to malicious websites (exploits web browser vulnerabilities)
  - Run malicious programs (Trojan) from websites or as email attachment

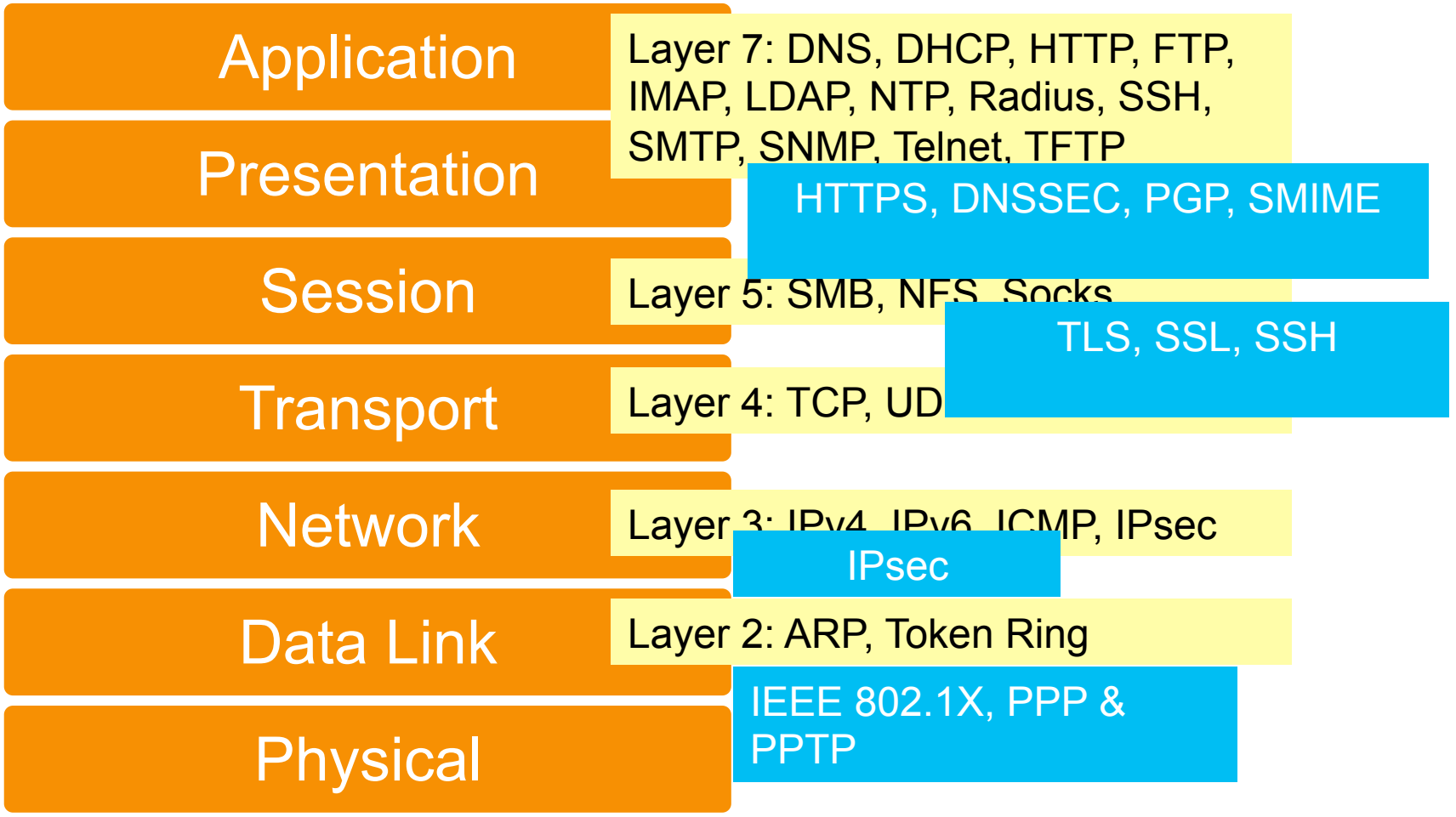
Password Cracking

- Dictionary attacks
  - Guessing passwords using a file of 1M possible password values
    - Ordinary words and people's names
  - Offline dictionary attack when the entire password file has been attacked
  - Use random characters as password with varying upper and lower case, numbers, and symbols
- Brute-force attacks
  - Checking all possible values until it has been found
  - The resource needed to perform this attack grows exponentially while increasing the key size
- Social engineering

Pharming and Phishing

- Phishing – victims are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site
  - Typically uses fraud emails with clickable links to fake websites
- Pharming – redirect a website's traffic to another fake site by changing the victim's DNS settings or hosts file

Security on Different Layers



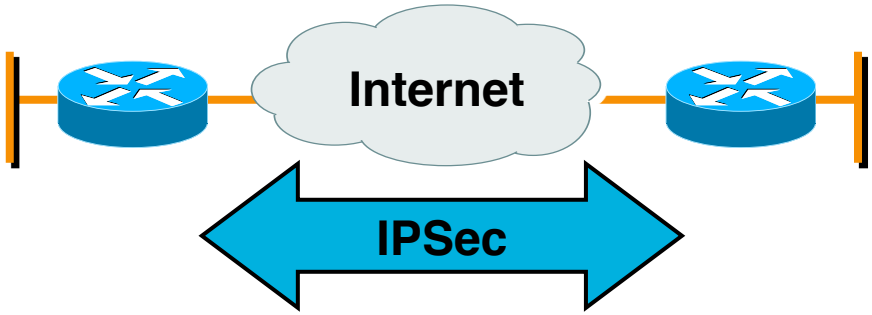
Link-Layer Security

- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

VPN Protocols

- PPTP (Point-to-Point tunneling Protocol)
  - Developed by Microsoft to secure dial-up connections
  - Operates in the data-link layer
- L2F (Layer 2 Forwarding Protocol)
  - Developed by Cisco
  - Similar as PPTP
- L2TP (Layer 2 Tunneling Protocol)
  - IETF standard
  - Combines the functionality of PPTP and L2F
- IPsec (Internet Protocol Security)
  - Open standard for VPN implementation
  - Operates on the network layer

Network Layer Security - IPsec

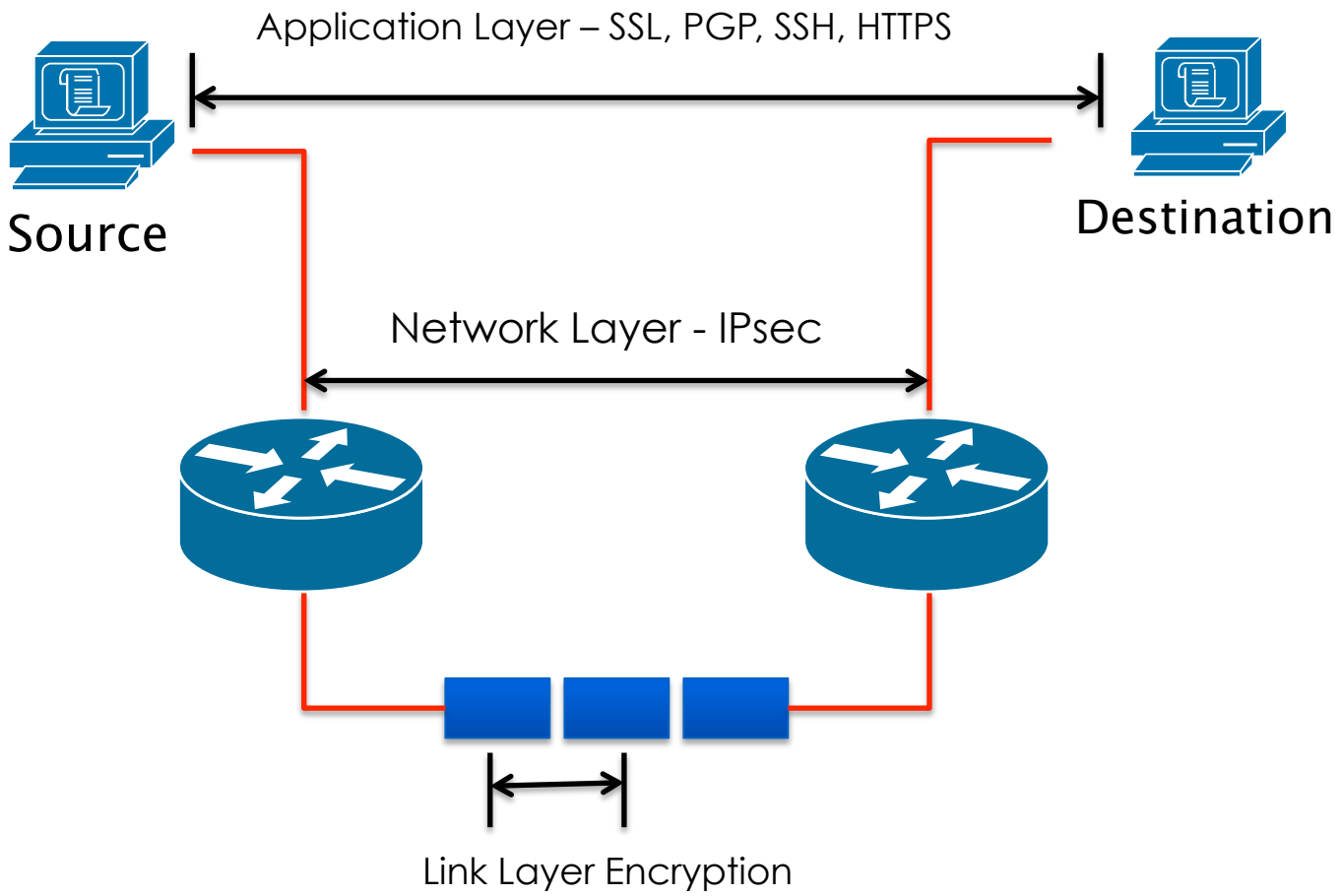


- IETF standard that enables encrypted communication between peers:
  - Consists of open standards for securing private communications
  - Network layer encryption ensuring data confidentiality, integrity, and authentication
  - Scales from small to very large networks

What Does IPsec Provide ?

- Confidentiality….many algorithms to choose from
- Data integrity and source authentication
  - Data “signed” by sender and “signature” verified by the recipient
  - Modification of data can be detected by signature “verification”
  - Because “signature” based on a shared secret, it gives source authentication
- Anti-replay protection
  - Optional : the sender must provide it but the recipient may ignore
- Key Management
  - IKE – session negotiation and establishment
  - Sessions are rekeyed or deleted automatically
  - Secret keys are securely established and authenticated
  - Remote peer is authenticated through varying options

Different Layers of Encryption



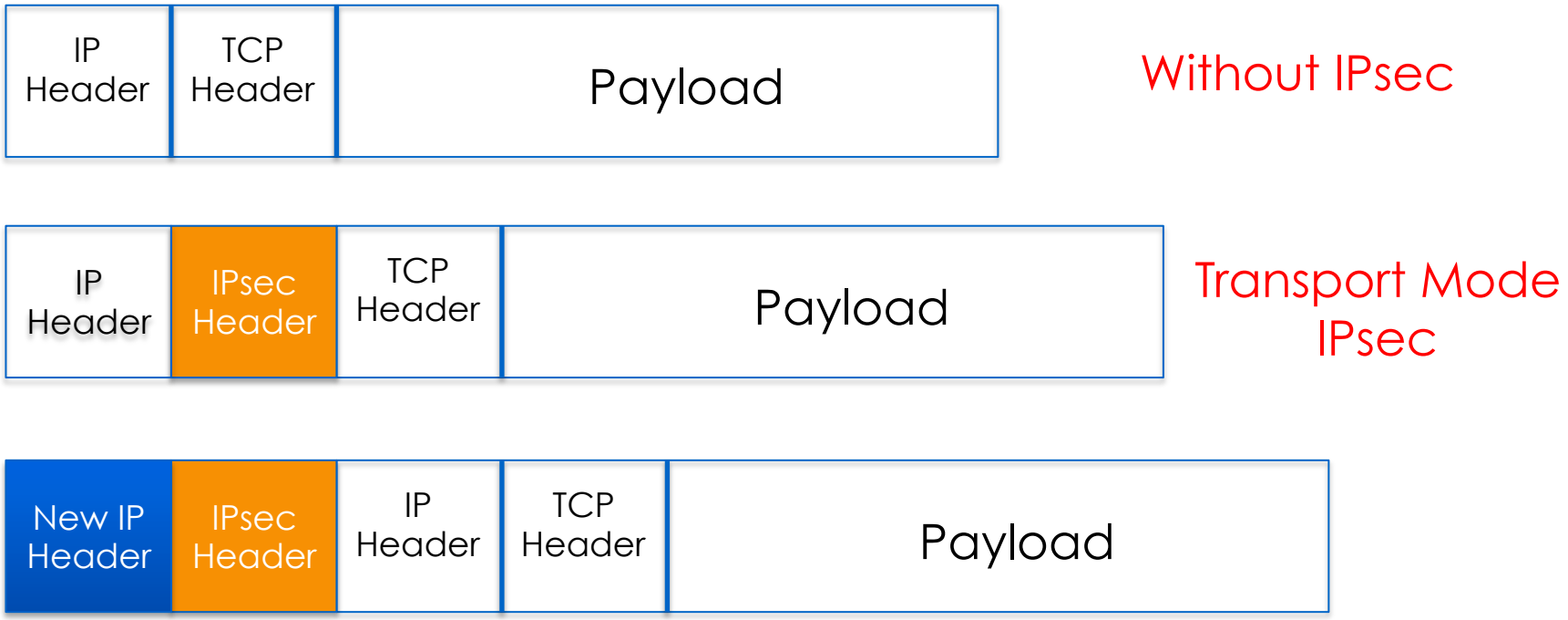
Relevant Standard(s)

- IETF specific
  - rfc2409: IKEv1
  - rfc4301: IPsec Architecture (updated)
  - rfc4303: IPsec ESP (updated)
  - rfc5996: IKEv2 (previously rfc4306 and rfc4718)
  - rfc4945: IPsec PKI Profile
- IPv6 and IPsec
  - rfc4294: IPv6 Node Requirements
  - Rfc4552: Authentication/Confidentiality for OSPFv3
  - rfc4877: Mobile IPv6 Using IPsec (updated)
  - rfc4891: Using IPsec to secure IPv6-in-IPv4 Tunnels

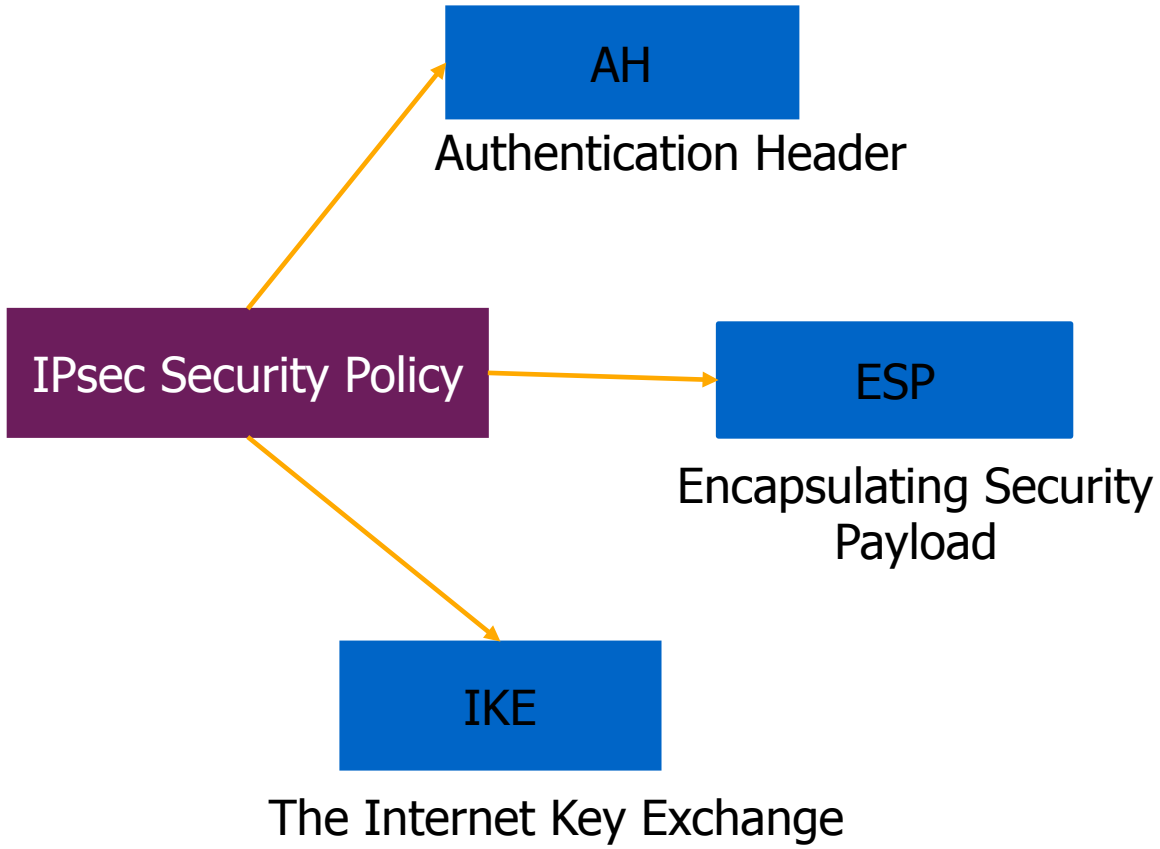
IPsec Modes

- Tunnel Mode
  - Entire IP packet is encrypted and becomes the data component of a new (and larger) IP packet.
  - Frequently used in an IPsec site-to-site VPN
- Transport Mode
  - IPsec header is inserted into the IP packet
  - No new packet is created
  - Works well in networks where increasing a packet's size could cause an issue
  - Frequently used for remote-access VPNs

Tunnel vs. Transport Mode IPsec



IPsec Architecture



Pretty Good IPsec Policy

- IKE Phase 1 (aka ISAKMP SA or IKE SA or Main Mode)
  - 3DES (AES-192 if both ends support it)
  - Lifetime (8 hours = 480 min = 28800 sec)
  - SHA-2 (256 bit keys)
  - DH Group 14 (aka MODP# 14)
- IKE Phase 2 (aka IPsec SA or Quick Mode)
  - 3DES (AES-192 if both ends support it)
  - Lifetime (1 hour = 60 min = 3600 sec)
  - SHA-2 (256 bit keys)
  - PFS 2
  - DH Group 14 (aka MODP# 14)

RFC2827 (BCP38) – Ingress Filtering

- If an ISP is aggregating routing announcements for multiple downstream networks, strict traffic filtering should be used to prohibit traffic which claims to have originated from outside of these aggregated announcements.
- The ONLY valid source IP address for packets originating from a customer network is the one assigned by the ISP (whether statically or dynamically assigned).
- An edge router could check every packet on ingress to ensure the user is not spoofing the source address on the packets which he is originating.

Guideline for BCP38

- Networks connecting to the Internet
  - Must use inbound and outbound packet filters to protect network
- Configuration example
  - Outbound—only allow my network source addresses out
  - Inbound—only allow specific ports to specific destinations in
- Use the following techniques
  - Static ACLs on the edge of the network
  - Unicast RPF strict mode
  - IP source guard

Receiving Prefixes

- There are three scenarios for receiving prefixes from other ASNs
  - Customer talking BGP
  - Peer talking BGP
  - Upstream/Transit talking BGP
- Each has different filtering requirements and need to be considered separately

Receiving Prefixes: From Customers

- ISPs should only accept prefixes which have been assigned or allocated to their downstream customer
- If ISP has assigned address space to its customer, then the customer IS entitled to announce it back to his ISP
- If the ISP has NOT assigned address space to its customer, then:
  - Check in the five RIR databases to see if this address space really has been assigned to the customer. **L**egitimacy of **A**ddress (LoA) check
  - The tool: whois –h jwhois.apnic.net x.x.x.0/24
    - (jwhois queries all RIR database)

Receiving Prefixes: From Customers

- Example use of whois to check if customer is entitled to announce address space:

```
$ whois -h whois.apnic.net 2406:6400::/32

Inet6num:       2406:6400::/32
netname:        APNIC-AP
descr:          Asia Pacific Network Information Centre
descr:          Regional Internet Registry for the Asia-Pacific
descr:          6 Cordelia Street
descr:          South Brisbane, QLD 4101
descr:          Australia
country:        AU
admin-c:        AIC1-AP
tech-c:         NO4-AP
mnt-by:         APNIC-HM
mnt-irt:        IRT-APNIC-AP
changed:        hm-changed@apnic.net
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20110309
source:         APNIC
```

Portable – means its an assignment to the customer, the customer can announce it to you

Receiving Prefixes: From Peers

- A peer is an ISP with whom you agree to exchange prefixes you originate into the Internet routing table
  - Prefixes you accept from a peer are only those they have indicated they will announce
  - Prefixes you announce to your peer are only those you have indicated you will announce

Receiving Prefixes: From Peers

- Agreeing what each will announce to the other:
  - Exchange of e-mail documentation as part of the peering agreement, and then ongoing updates

    OR
  - Use of the Internet Routing Registry and configuration tools such as the IRRToolSet

    http://www.isc.org/software/irrtoolset

Receiving Prefixes: From Upstream

- Upstream/Transit Provider is an ISP who you pay to give you transit to the WHOLE Internet
- Receiving prefixes from them is not desirable unless really necessary
  - Traffic Engineering – see BGP Multihoming presentations
- Ask upstream/transit provider to either:
  - originate a default-route

    OR
  - announce one prefix you can use as default

Transport Layer Security

- Secure Socket Layer (SSL)
- Secure Shell Protocol
- SOCKS Protocol

SSL/TLS

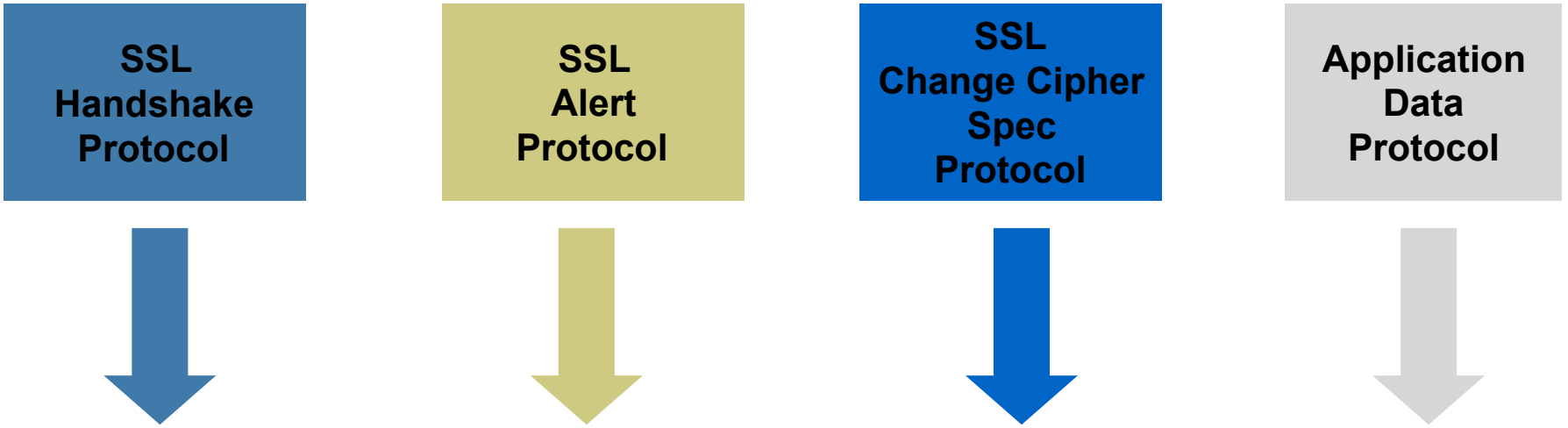
- Most widely-used protocol for security
- Encrypts the segments of network connections above the Transport Layer
- SSL and TLS
  - SSL v3.0 specified in an I-D in 1996 (draft-freier-ssl-version3-02.txt)
  - TLS v1.0 specified in RFC 2246 in 1999
  - TLS v1.0 = SSL v3.1 ≈ SSL v3.0
  - TLS v1.1 in 2006
  - TLS v1.2 in 2008
- Goals of protocol
  - Secure communication between applications
  - Data encryption
  - Server authentication
  - Message integrity
  - Client authentication (optional)

Benefits of TLS

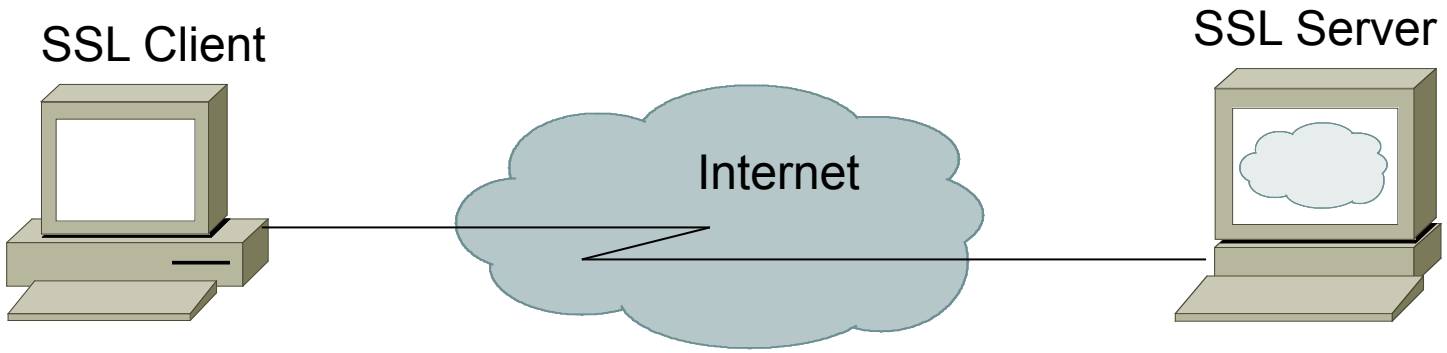
- Application-layer independent
  - can be implemented with any applications
  - a wide range of applications supporting it
- SSL makes use of both asymmetric and symmetric key cryptography.
  - performance reasons.
  - Only the initial "client key exchange message" is encrypted with asymmetric encryption.
  - Symmetric encryption is better in terms of performance/speed
- Uses X.509 certificates
  - Certificates and Public Key Infrastructure
- SSL protocol layers comes on top of TCP (transport Layer), and is below application layer.
  - no network infrastructure changes are required to deploy SSL
- Each and every connection that's made, through SSL has got one session information.
  - Session can also be reused or resumed for other connections to the server

SSL Protocol Building Blocks

SSL is a Combination of a Primary Record Protocol with Four 'Client' Protocols



The SSL Handshake Process



ClientHello

1 Client initiates SSL connection / sends supported cipher suites

Server returns digital certificate to client and selected cipher suite 2

ServerHello
Certificate
ServerKeyExchange
ClientCertReq (opt)
ServerDone

ClientKeyExchange

3 Client sends shared secret encrypted with server's public key

4 Message encryption and integrity algorithms are negotiated

ChangeCipherSpec
Finished

5 Session keys are generated

ChangeCipherSpec
Finished

6 **Secure session tunnel is established**

<- Application Data ->

SSL version, Random data (ClientHello.random), sessionID, cipher suits, compression algorithm

Client computes the premaster key

SSL version, Cipher suits, Random data (ServerHello.random), session ID

Applications Using SSL/TLS

Protocol	Defined Port Number	SSL/TLS Port Number
HTTP	80	443
NNTP	119	563
LDAP	389	636
FTP-data	20	989
FTP-control	21	990
Telnet	23	992
IMAP	143	993
POP3	110	995
SMTP	25	465

Attacks on SSL (a little harder…)

- BEAST Attack (2011)
  - Browser Exploit Against SSL/TLS
  - CBC vulnerability discovered in 2002
  - Fixed in TLS 1.1
- CRIME Attack (2012)
  - Compression Ratio Info-leak Made Easy
  - Exploit against HTTP compression
  - ‘fixed’ by disabling TLS Compression
- BREACH Attack (2013)
  - Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext
  - Presented at BlackHat 2013 (Aug)
  - Attacks HTTP responses using HTTP Compression

Easy enough IF tools become available.

Public Key Infrastructure

- Combines public key cryptography and digital signatures to ensure confidentiality, integrity, authentication, non-repudiation, and access control
- Digital certificate – basic element of PKI; secure credential that identifies the owner
- Basic Components:
  - Certificate Authority (CA)
  - Registration Authority (RA)
  - Repository
  - Archive

Secure Shell Protocol (SSH)

- Protocol for secure remote login
- Provides support for secure remote login, secure file transfer, and secure forwarding of TCP/IP and X Window System traffic
- Consists of 3 major components:
  - Transport layer protocol (server authentication, confidentiality, integrity)
  - User authentication protocol (authenticates client to the server)
  - Connection protocol (multiplexes the encrypted tunnel into several logical channels)

Application Layer Security

- HTTPS
- PGP (Pretty Good Privacy)
- SMIME (Secure Multipurpose Internet Mail Extensions)
- TSIG and DNSSEC
- Wireless Encryption - WEP, WPA, WPA2

HTTPS

- Hypertext Transfer Protocol Secure
- Widely-used, message-oriented communications protocol
- Connectionless oriented protocol
- Technically not a protocol in itself, but simply layering HTTP on top of the SSL/TLS protocol
- Encapsulates data after security properties of the session
- Not to be confused with S-HTTP

Note: A website must use HTTPS everywhere, otherwise it is still vulnerable to some attacks

Pretty Good Privacy (PGP)

- Stands for Pretty Good Privacy, developed by Phil Zimmerman in 1995
- PGP is a hybrid cryptosystem
  - combines some of the best features of both conventional and public key cryptography
- Assumptions:
  - All users are using public key cryptography and have generated private/public key pairs (using RSA or El Gamal)
  - All users also use symmetric key system (DES or Rijndael)
- Offers authentication, confidentiality, compression, e-mail compatibility and segmentation

PGP - Trust

- Centralized / hierarchal trust – where certain globally trusted bodies sign keys for every one else.
- Decentralized webs of trust – where you pick who you trust yourself, and decide if you trust who those people trust in turn.
- Which works better for what reasons?

Key management: Partying

- Key signing parties are ways to build webs of trust.
- Each participant carries identification, as well as a copy of their key fingerprint. (maybe some $ as well ☺)
- Each participant decides if they're going to sign another key based on their personal policy.
- Keys are easiest kept in a keyring on an openpgp keyserver in the aftermath of the party.

Questions

Cryptography

Cryptography

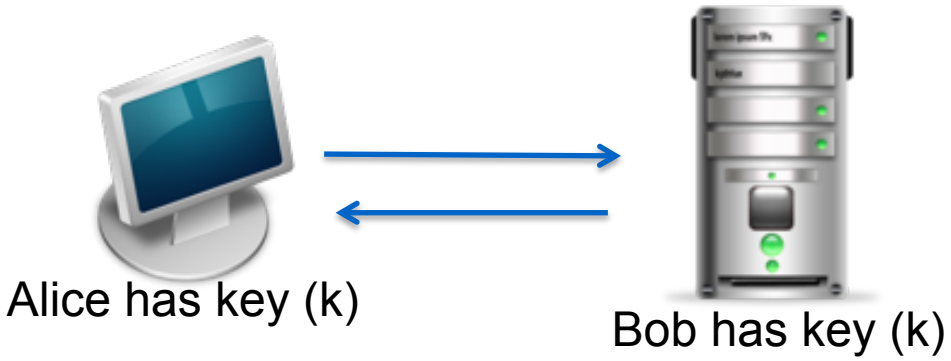
- Cryptography deals with creating documents that can be shared secretly over public communication channels
- Other terms closely associated
  - Cryptanalysis = code breaking
  - Cryptology
    - Kryptos (hidden or secret) and Logos (description) = secret speech / communication
    - combination of cryptography and cryptanalysis
- Cryptography is a function of plaintext and a cryptographic key

$$C = F(P, k)$$

Notation:
Plaintext (P)
Ciphertext (C)
Cryptographic Key (k)

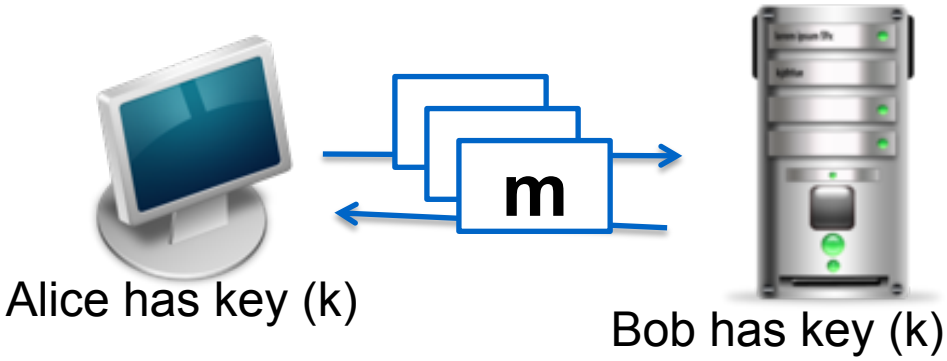
Crypto Core

- Secure key establishment



- Secure communication

Confidentiality and integrity



Source: Dan Boneh, Stanford

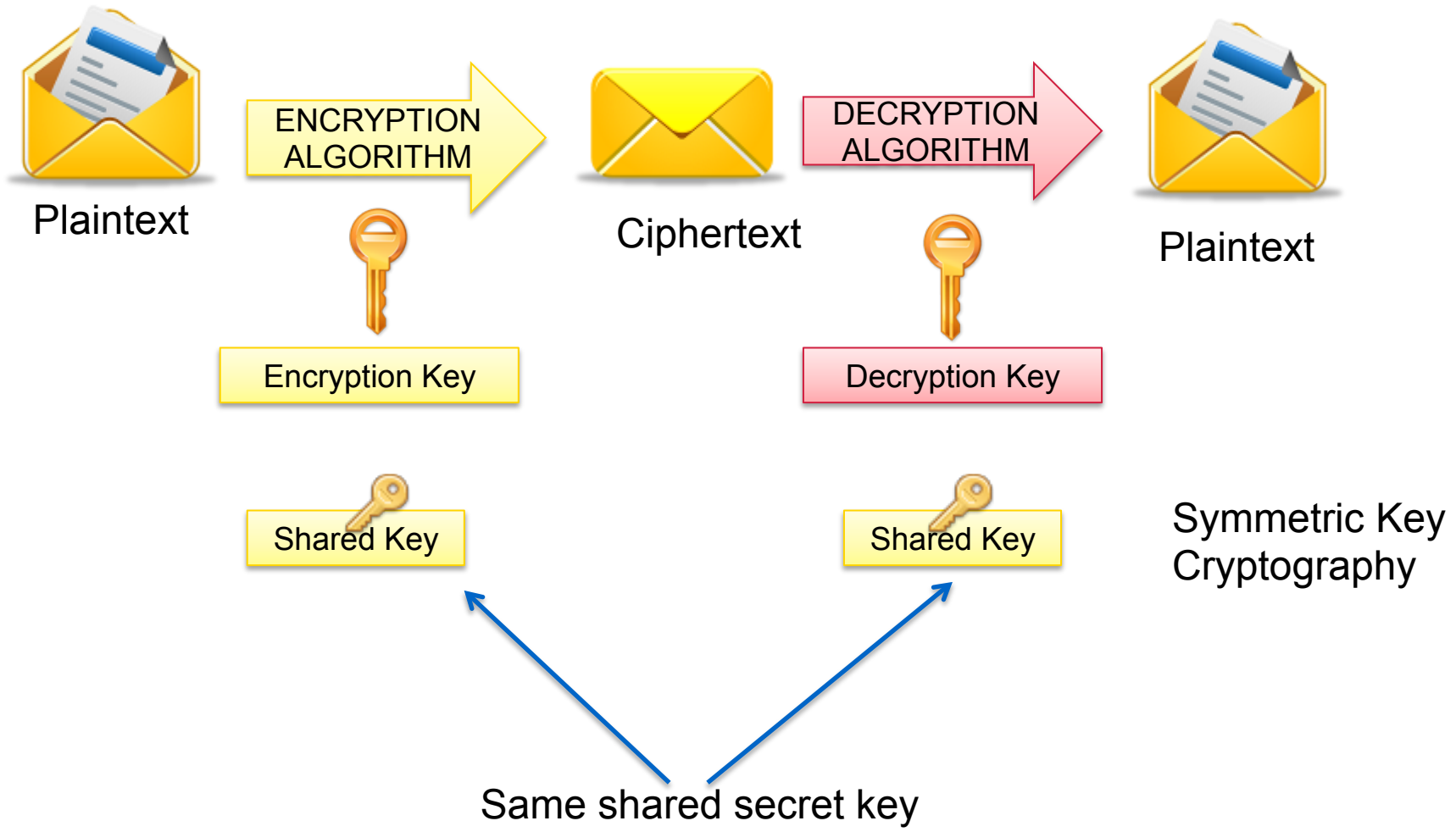
Encryption

- process of transforming plaintext to ciphertext using a cryptographic key
- Used all around us
  - In Application Layer – used in secure email, database sessions, and messaging
  - In session layer – using Secure Socket Layer (SSL) or Transport Layer Security (TLS)
  - In the Network Layer – using protocols such as IPsec
- Benefits of good encryption algorithm:
  - Resistant to cryptographic attack
  - They support variable and long key lengths and scalability
  - They create an avalanche effect
  - No export or import restrictions

Symmetric Key Algorithm

- Uses a single key to both encrypt and decrypt information
- Also known as a secret-key algorithm
  - The key must be kept a “secret” to maintain security
  - This key is also known as a private key
- Follows the more traditional form of cryptography with key lengths ranging from 40 to 256 bits.
- Examples:
  - DES, 3DES, AES, RC4, RC6, Blowfish

Symmetric Encryption



Symmetric Key Algorithm

- DES – block cipher using shared key encryption, 56-bit
- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- AES – replacement for DES; it is the current standard
- RC4 – variable-length key, “stream cipher” (generate stream from key, XOR with data)
- RC6
- Blowfish

Symmetric Key Algorithm

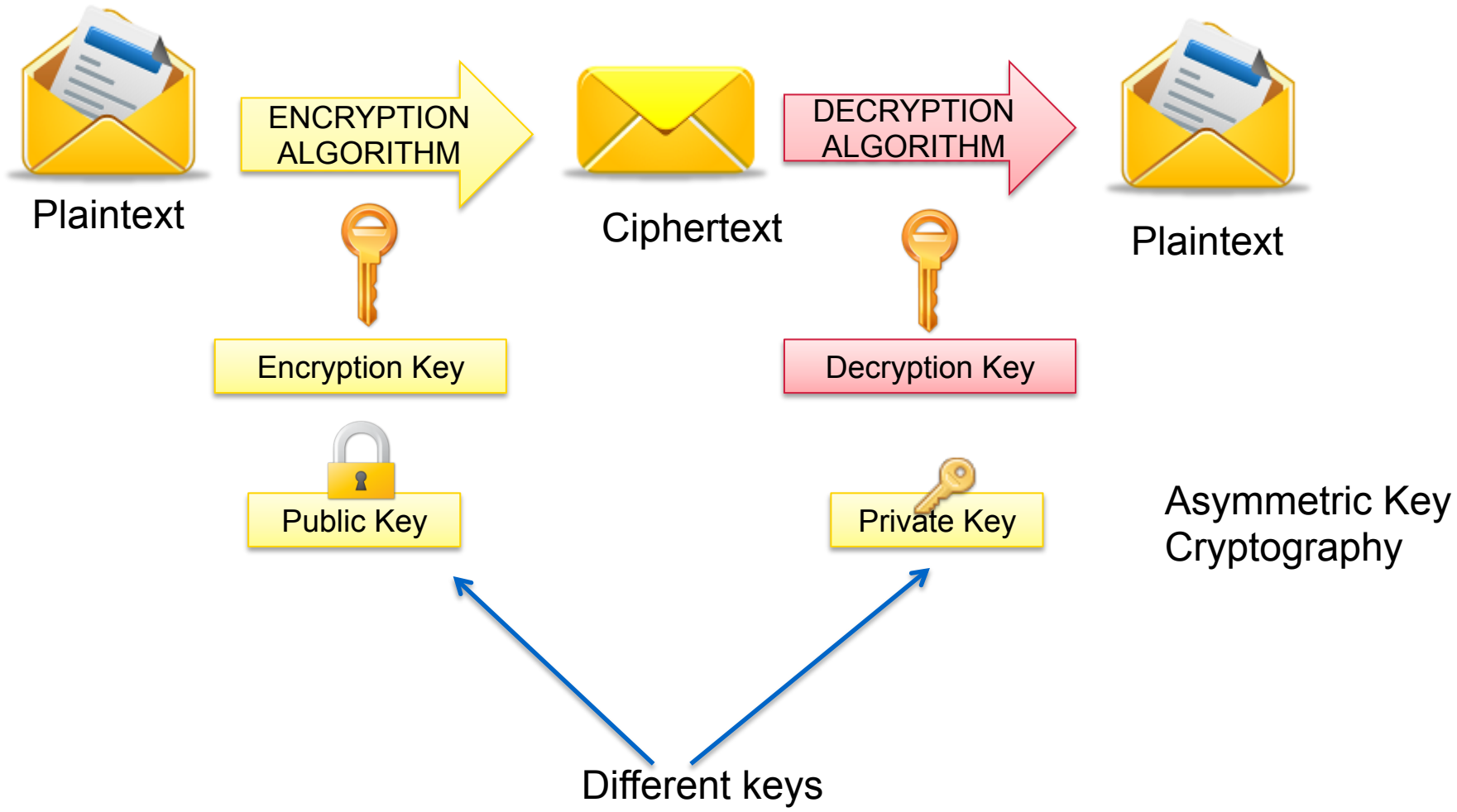
Symmetric Algorithm	Key Size
DES	56-bit keys
Triple DES (3DES)	112-bit and 168-bit keys
AES	128, 192, and 256-bit keys
IDEA	128-bit keys
RC2	40 and 64-bit keys
RC4	1 to 256-bit keys
RC5	0 to 2040-bit keys
RC6	128, 192, and 256-bit keys
Blowfish	32 to 448-bit keys

Note:
Longer keys are more difficult to crack, but more computationally expensive.

Asymmetric Key Algorithm

- Also called public-key cryptography
  - Keep private key private
  - Anyone can see public key
- separate keys for encryption and decryption (public and private key pairs)
- Examples:
  - RSA, DSA, Diffie-Hellman, ElGamal, PKCS

Asymmetric Encryption



Asymmetric Key Algorithms

- RSA – the first and still most common implementation
- DSA – specified in NIST's Digital Signature Standard (DSS), provides digital signature capability for authentication of messages
- Diffie-Hellman – used for secret key exchange only, and not for authentication or digital signature
- ElGamal – similar to Diffie-Hellman and used for key exchange
- PKCS – set of interoperable standards and guidelines

Symmetric vs. Asymmetric Key

Symmetric	Asymmetric
generally fast Same key for both encryption and decryption	Can be 1000 times slower Uses two different keys (public and private) Decryption key cannot be calculated from the encryption key Key lengths: 512 to 4096 bits Used in low-volume

Hash Functions

- produces a condensed representation of a message (hashing)
- The fixed-length output is called the hash or message digest
- A hash function takes an input message of arbitrary length and outputs fixed-length code.
  - Given x, we can compute the value f(x).
  - Given f(x), it is hard to get the value of x.
- A form of signature that uniquely represents the data
  - Collision-free
- Uses:
  - Verifying file integrity - if the hash changes, it means the data is either compromised or altered in transit.
  - Digitally signing documents
  - Hashing passwords

Hash Functions

- Message Digest (MD) Algorithm
  - Outputs a 128-bit fingerprint of an arbitrary-length input
  - MD4 is obsolete, MD5 is widely-used
- Secure Hash Algorithm (SHA)
  - SHA-1 produces a 160-bit message digest similar to MD5
  - Widely-used on security applications (TLS, SSL, PGP, SSH, S/MIME, IPsec)
  - SHA-256, SHA-384, SHA-512 are also commonly used, which can produce hash values that are 256, 384, and 512-bits respectively
- RIPEMD
  - Derived from MD4, but performs like SHA
  - RIPEMD-160 is the most popular version

Digital Signature

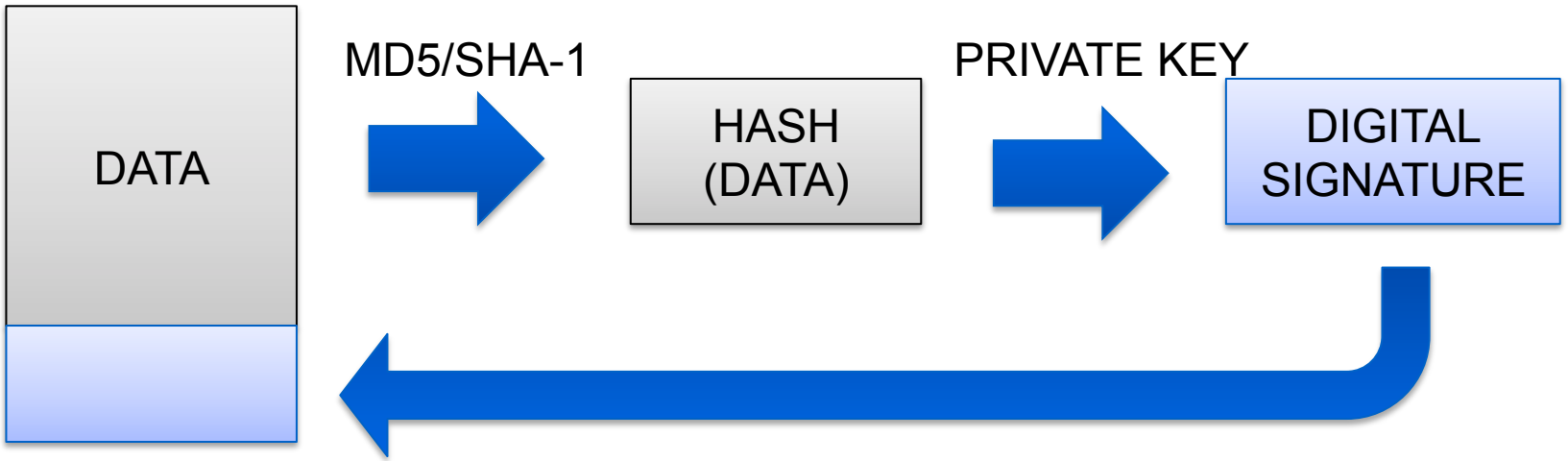
- A digital signature is a message appended to a packet
- The sender encrypts message with own private key instead of encrypting with intended receiver's public key
- The receiver of the packet uses the sender's public key to verify the signature.
- Used to prove the identity of the sender and the integrity of the packet

Digital Signature

- Two common public-key digital signature techniques:
  - RSA (Rivest, Shamir, Adelman)
  - DSS (Digital Signature Standard)
- Used in a lot of things:
  - Email, software distribution, electronic funds transfer, etc
- A common way to implement is to use a hashing algorithm to get the message digest of the data, then use an algorithm to sign the message

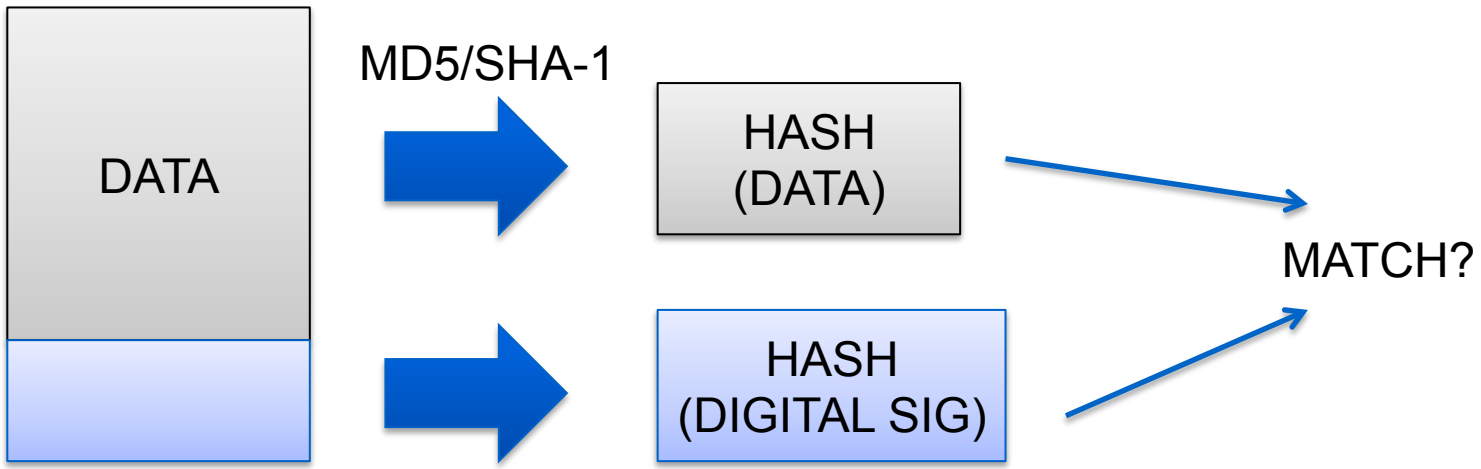
Digital Signature Process

1. Hash the data using one of the supported hashing algorithms (MD5, SHA-1, SHA-256)
2. Encrypt the hashed data using the sender's private key
3. Append the signature (and a copy of the sender's public key) to the end of the data that was signed)



Signature Verification Process

1. Hash the original data using the same hashing algorithm
2. Decrypt the digital signature using the sender's public key. All digital signatures contain a copy of the signer's public key
3. Compare the results of the hashing and the decryption. If the values match then the signature is verified. If the values do not match, then the data or signature was probably modified.



Encrypted Communications

- Use encrypted communications whenever you need to keep information confidential
- Verify via network sniffer (e.g. wireshark) that your communication is indeed encrypted
- An important aspect is credential management (creating, distributing, storing, revoking, renewing)
- Understand if/when credentials are lost that you may not be able to recover the data
- Have a plan in place in case you forget your password that protects your private keys

Questions

APRICOT 2014

RPKI and Resource Certification

SIDR Working Group

- Secure Inter-Domain Routing (SIDR)
- Its purpose is to “reduce vulnerabilities to the inter-domain routing system”
- Addresses two vulnerabilities:
  - Is an Autonomous System authorized to originate an IP prefix?
  - Is the AS-Path represented in the route the same as the path through which the NLRI traveled?
- Projects:
  - PKI, RPKI, BGPsec

Source: SIDR WG
https://datatracker.ietf.org/wg/sidr/charter/

BGP Security (BGPsec)

- Extension to BGP that provides improved security for BGP routing
- Currently an IETF Internet draft
- Implemented via a new optional non-transitive BGP path attribute that contains a digital signature
- Two things:
  - BGP Prefix Origin Validation (using RPKI)
  - BGP Path Validation

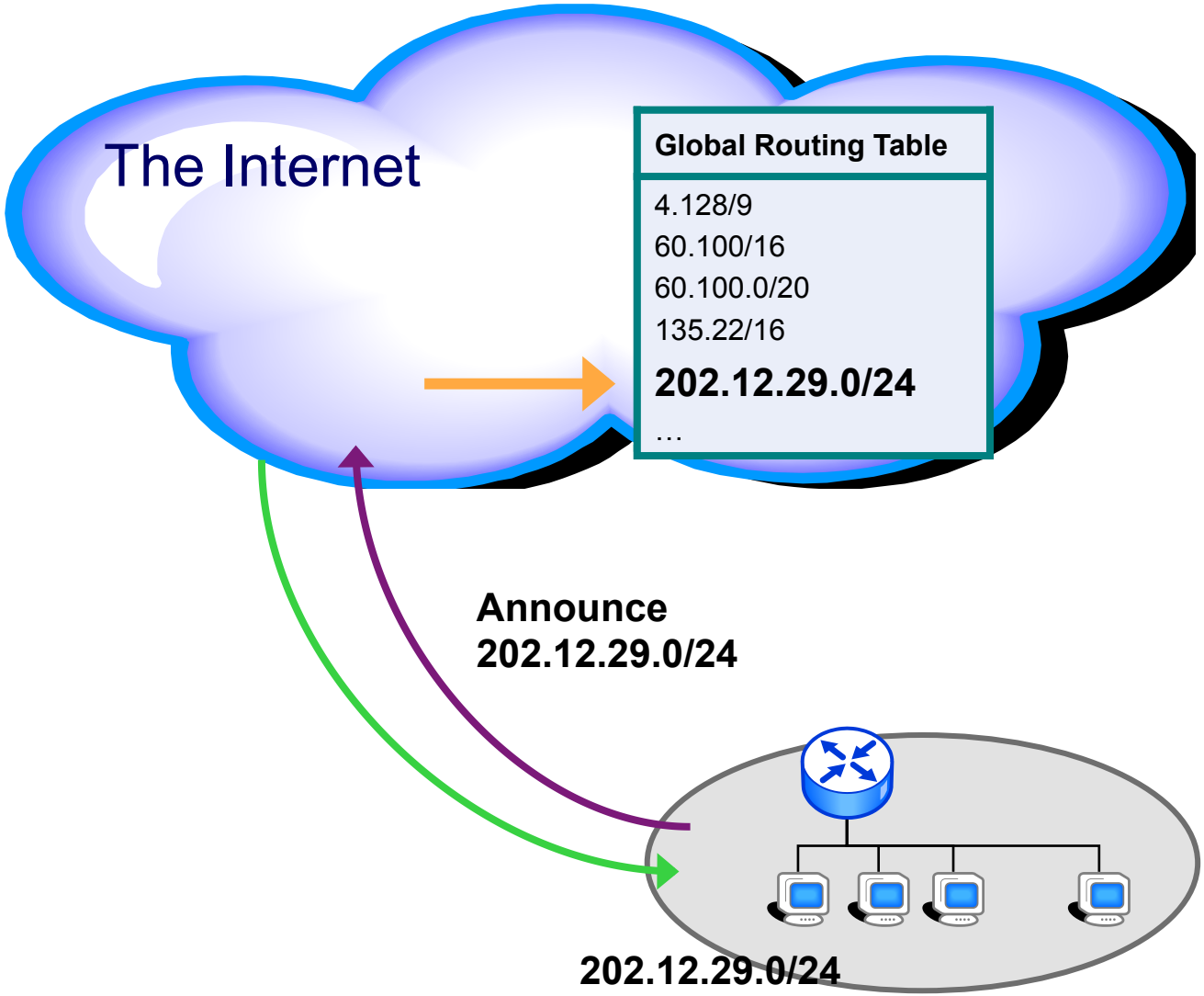
Three Pieces

- RPKI – Resource Public Key Infrastructure, the Certificate Infrastructure to Support the other Pieces (deployed at all RIRs)
- Origin Validation – Using the RPKI to detect and prevent mis-originations of someone else's prefixes (in deployment)
- AS-Path Validation AKA BGPsec – Prevent Path Attacks on BGP (future work)

What is RPKI?

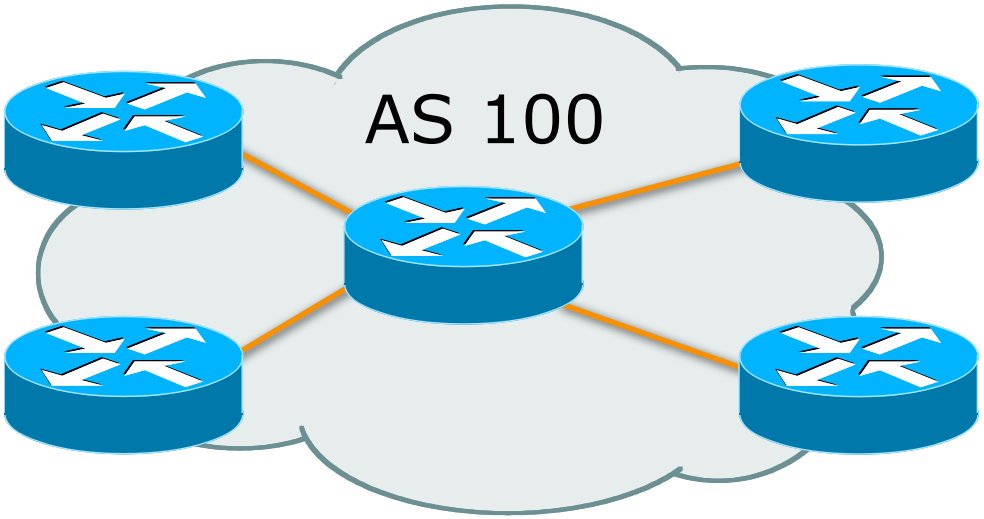
- Resource Public Key Infrastructure (RPKI)
- A robust security framework for verifying the association between resource holder and their Internet resources
- Created to address the issues in RFC 4593
- Uses X.509 v3 certificates
  - With RFC3779 extensions
- Helps to secure Internet routing by validating routes
  - Proof that prefix announcements are coming from the legitimate holder of the resource
- A system to manage the creation and storage of digital certificates and the associated Route Origin Authorization documents

Internet Routing



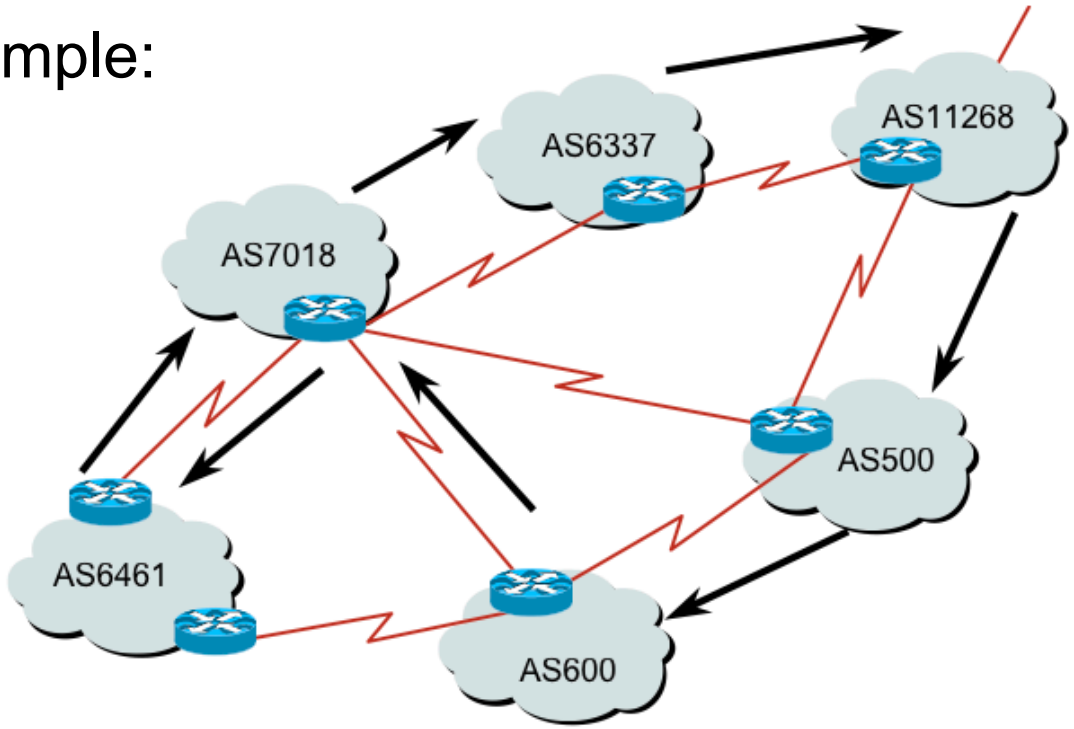
Autonomous System (AS)

- Collection of networks with same routing policy
- Single routing protocol
- Usually under single ownership, trust and administrative control



What is AS path?

- An AS path example:




```
12.6.126.0/24 207.126.96.43  1021  0 6461 7018 6337 11268 i
```

AS Path

Benefits of RPKI - Routing

- Prevents “Route Hijacking”
  - when an entity participating in Internet routing announces a prefix without authorization
  - Reason: malicious attack
- Prevents **mis-origination**
  - A prefix that is originated by an AS which does not own it
  - Reason: configuration mistake

“Right” to Resources

- ISP gets their resources from the RIR
- ISP notifies its upstream of the prefixes to be announced
- Upstream _MUST_ check the Whois database if resource has been delegated to customer ISP.

We need to be able to Authoritatively prove who owns an IP Prefix and what AS(s) may announce it.

X.509 Certificate with 3779 Extension

- Resource certificates are based on the X.509 certificate format - RFC 5280
- Extended by RFC 3779 – this extension binds a list of resources (IP, ASN) to the subject of the certificate
- SIA – Subject Information Access; contains a URI that references the directory

Components

- Global RPKI
  - Certificate Authority (CA)
  - Internet Registries (RIR, NIR, Large LIR)
  - Issue certificates for customers
  - Allow customers to use the CA's GUI to issue ROAs for their prefixes
  - Maintains a publication repository
- Relying Party (RP) / Local Cache
  - Has software which gathers data from the CAs
  - Local set of one or more collected and verified caches
- Routers
  - Fetches data from a local cache using RPKI to Router Protocol

Resource Certification

- RIRs have been developing a new service for their members
- APNIC has now launched Resource Certification for the AP region
- The goal is to improve the security of inter-domain routing and augmenting the information published in the APNIC Whois Database

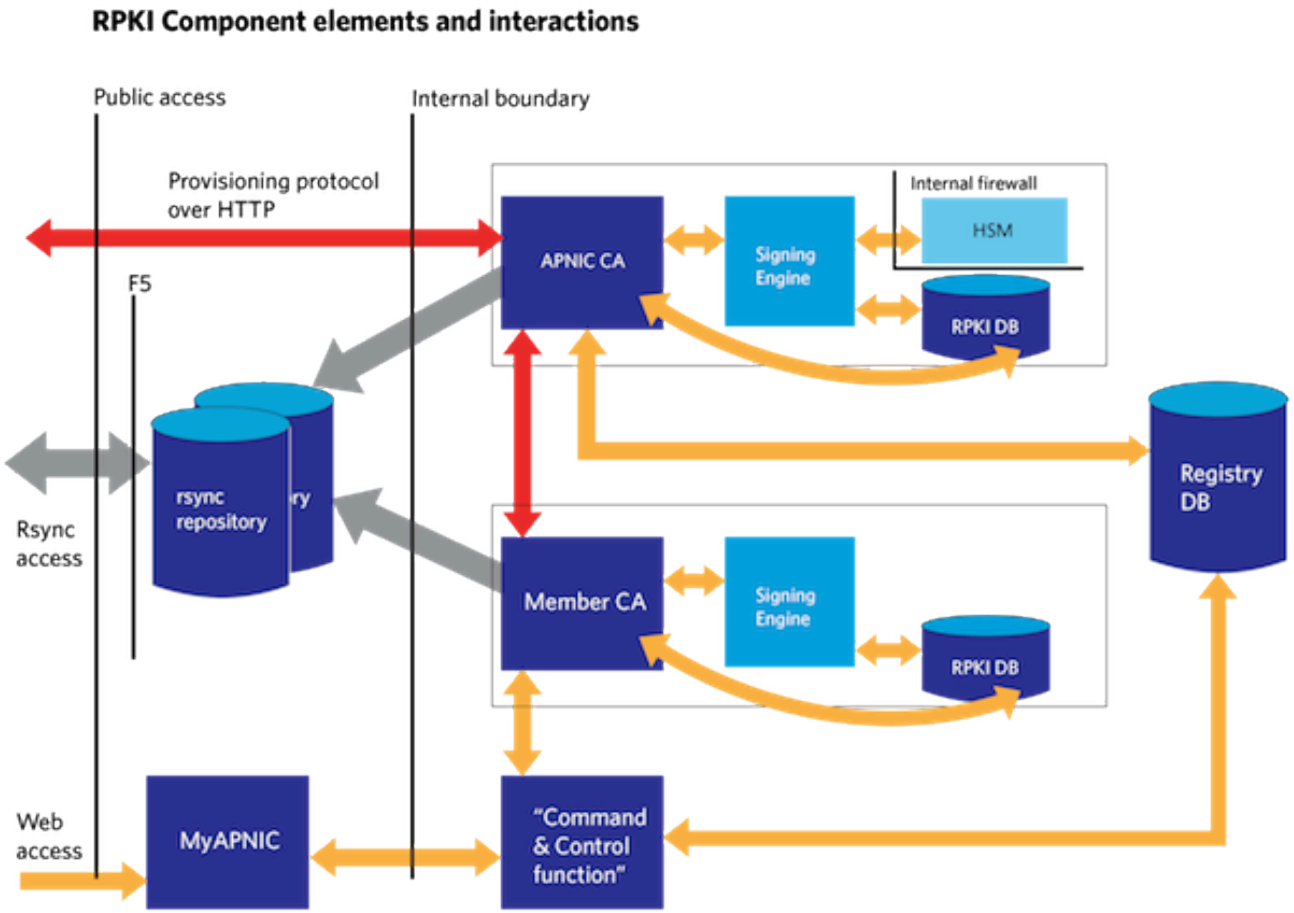
Resource Certification Benefits

- Routing information corresponds to properly delegated address resources
- Resource Certification gives resource holders proof that they hold certain resources
- Resource holders can attest to those resources when distributing them
- Resource Certification is a highly robust means of preventing the injection of false information into the Internet's routing system.

APNIC Resource Certification

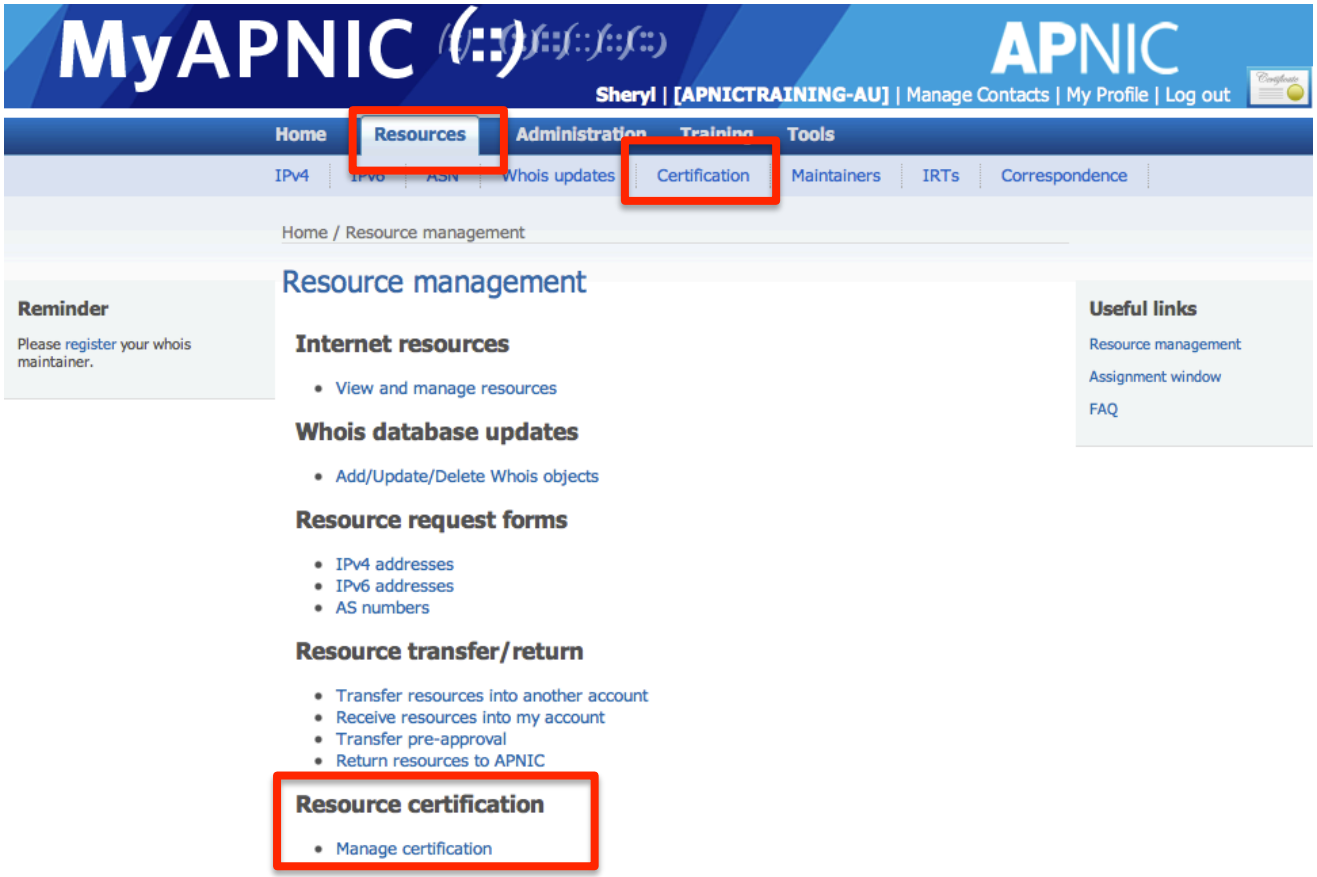
- A robust security framework for verifying the association between resource holders and their Internet resources.
- Initiative from APNIC aimed at
  - improving the security of inter-domain routing, and
  - augmenting the information published in the Whois database
- Verifies a holder's current "right-of-use" over an Internet resource
  - Verify public key through a chain of interlocking certificates that connect a Trust Anchor to the signer's public key certificate.
  - Routing advertisements are now verifiable

How it Works


RPKI Component elements and interactions
Public access
Internal boundary
Provisioning protocol over HTTP
Internal firewall
HSM
APNIC CA
Signing Engine
RPKI DB
F5
rsync repository
Rsync access
Registry DB
Member CA
Signing Engine
RPKI DB
Web access
MyAPNIC
"Command & Control function"

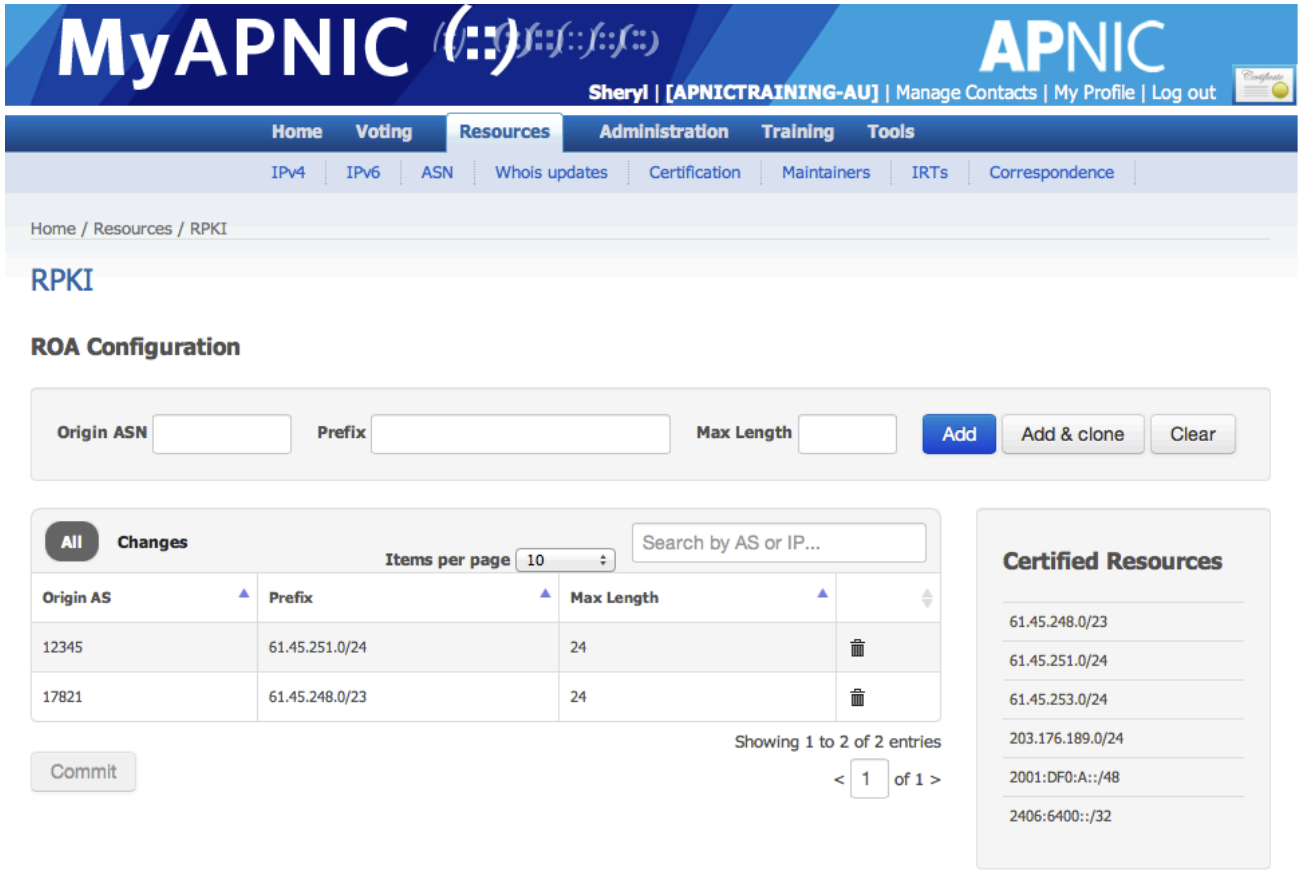
Creating ROA Records

- Login to MyAPNIC, then **Resources -> Certification**

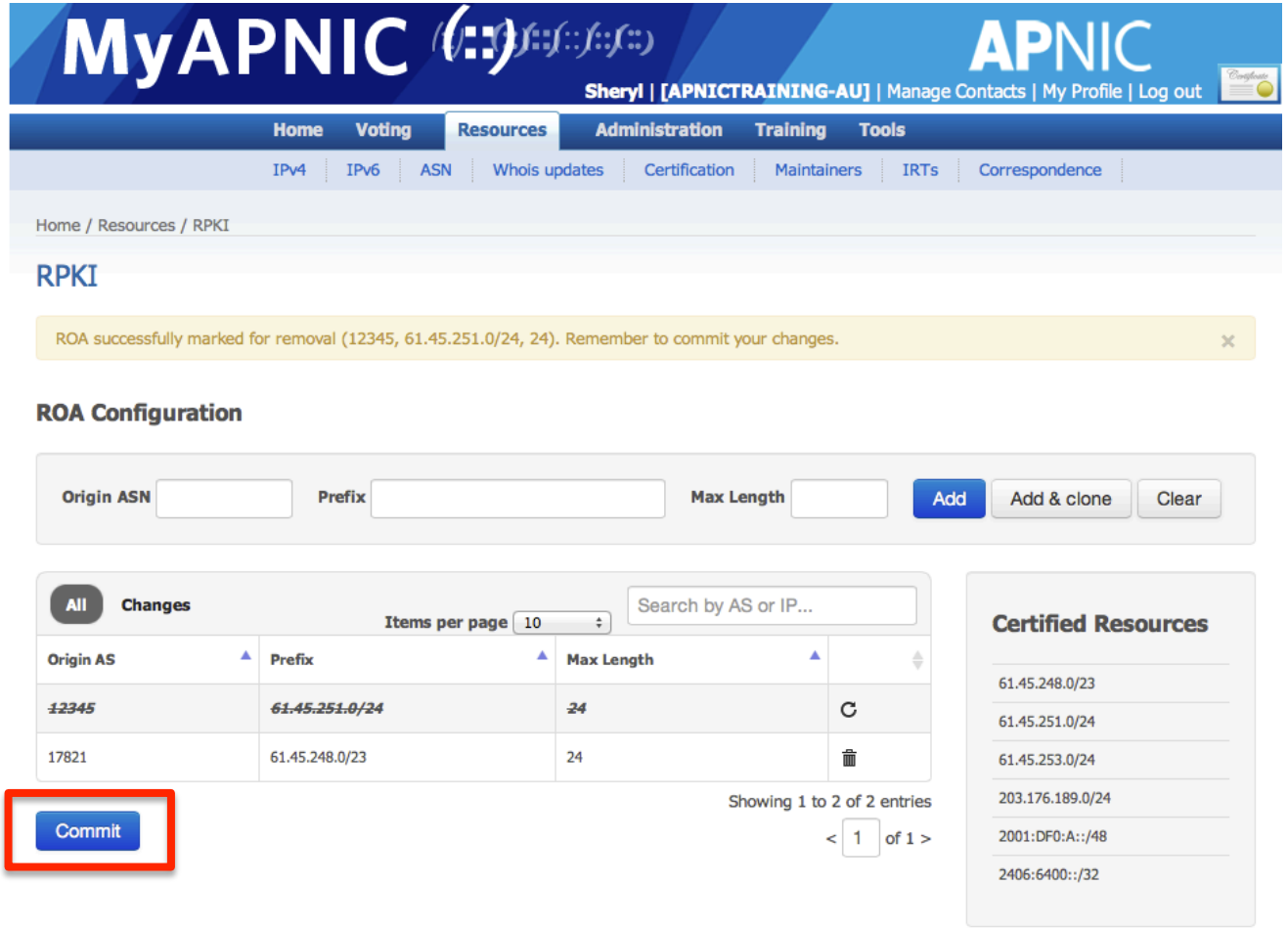


Adding ROA Records

- Simple view and add using the form



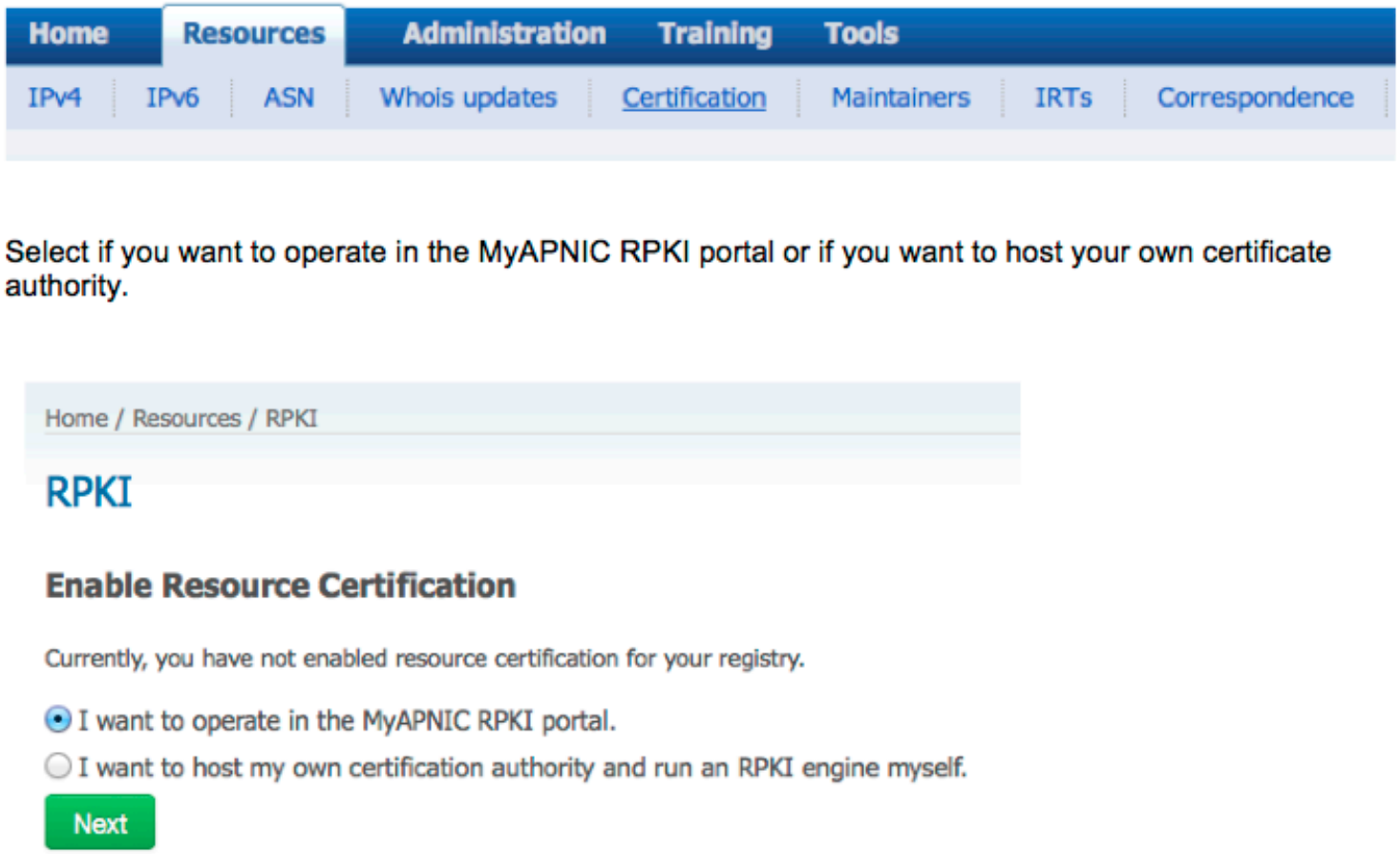
Deleting ROA Records



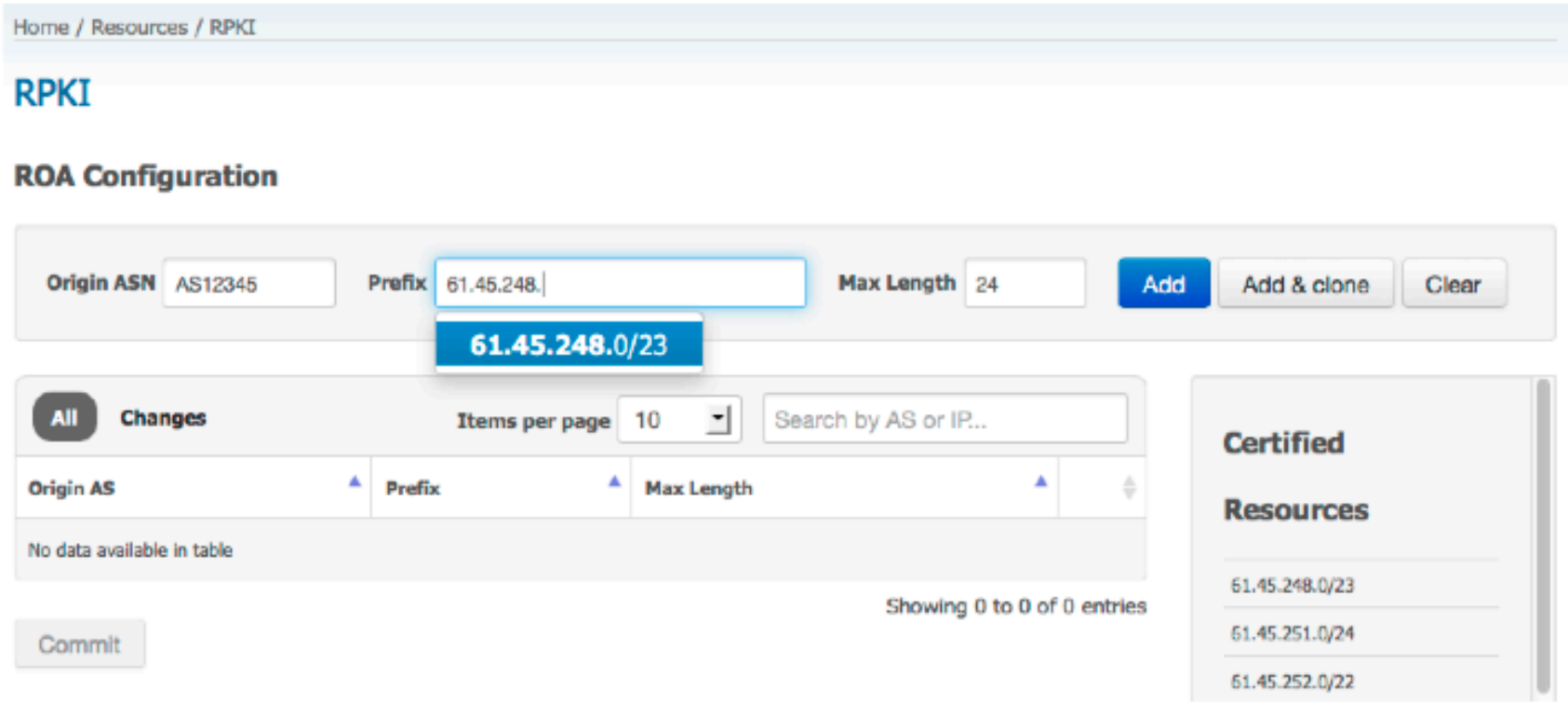
Resource Certification

- Collaborative effort by all the RIR
- Secure the Internet routing Infrastructure
- Resource Certification uses RPKI framework
- Public repository http://rpki.apnic.net
- Creation on Route Origin Authorization (ROA) Object

Activate RPKI engine



Create ROA objects



Questions

Tools

APRICOT 2014

Resource Registration

Network Security Workshop

What is the APNIC Database?

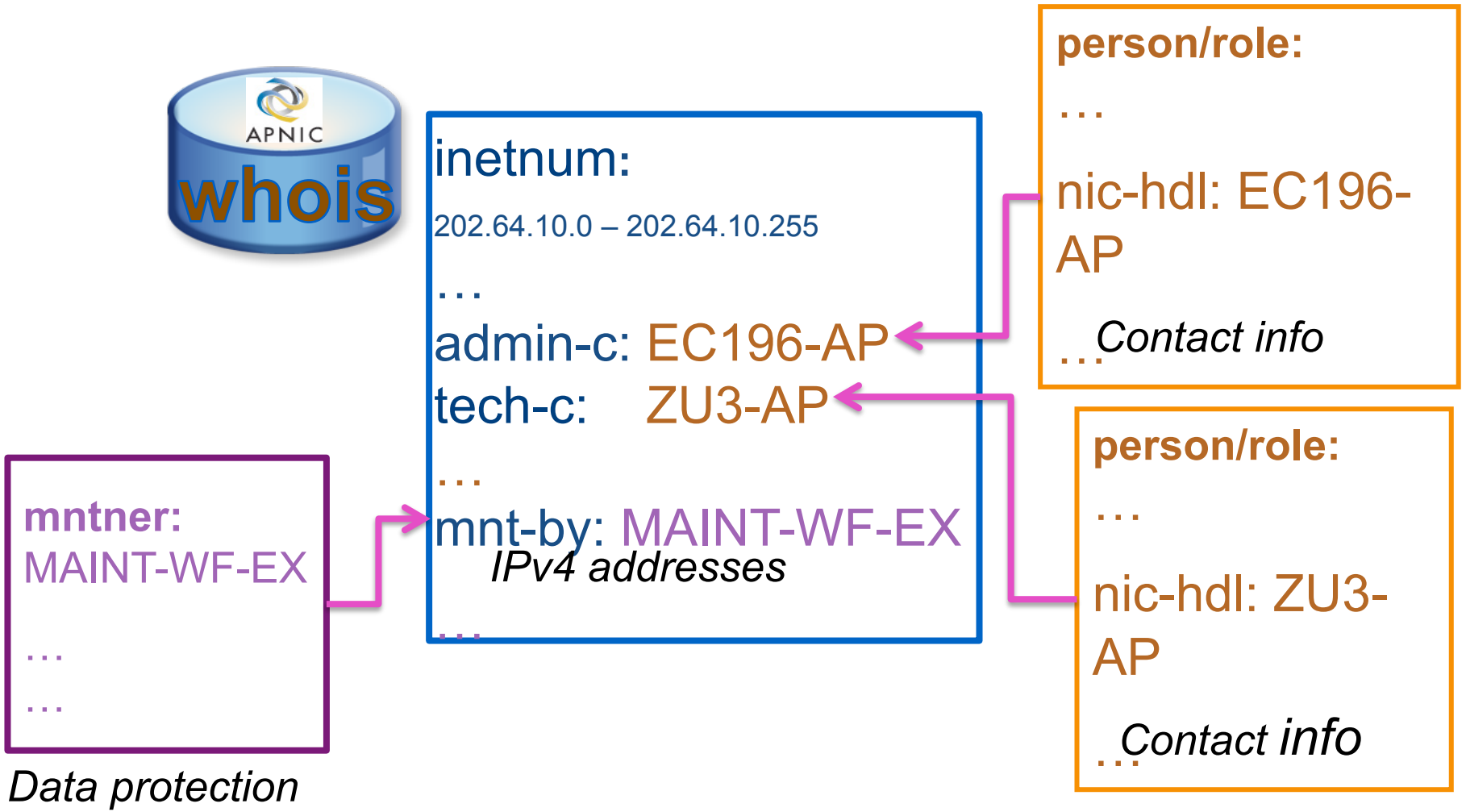
- Public network management database
  - Operated by Internet Registries
    - Public data only
    - (For private data, please see “Privacy of customer assignment” module)
- Tracks network resources
  - IP addresses, ASNs, Reverse Domains, Routing policies
- Records administrative information
  - Contact information (persons/roles)
  - Authorization

Object Types

OBJECT	PURPOSE
• person	contact persons
• role	contact groups/roles
• inetnum	IPv4 addresses
• Inet6num	IPv6 addresses
• aut-num	Autonomous System number
• domain	reverse domains
• route	prefixes being announced
• mntner	(maintainer) data protection
• mnt-irt	Incident Response Team

http://www.apnic.net/db/

Inter-Related Objects



IRT Object

- Incident Response Team (IRT)
  - Dedicated abuse handling teams (not netops)
- Implemented in Nov 2010 through Prop-079
- Abuse contact information
- Mandatory object reference in inetnum, inet6num, and aut-num objects

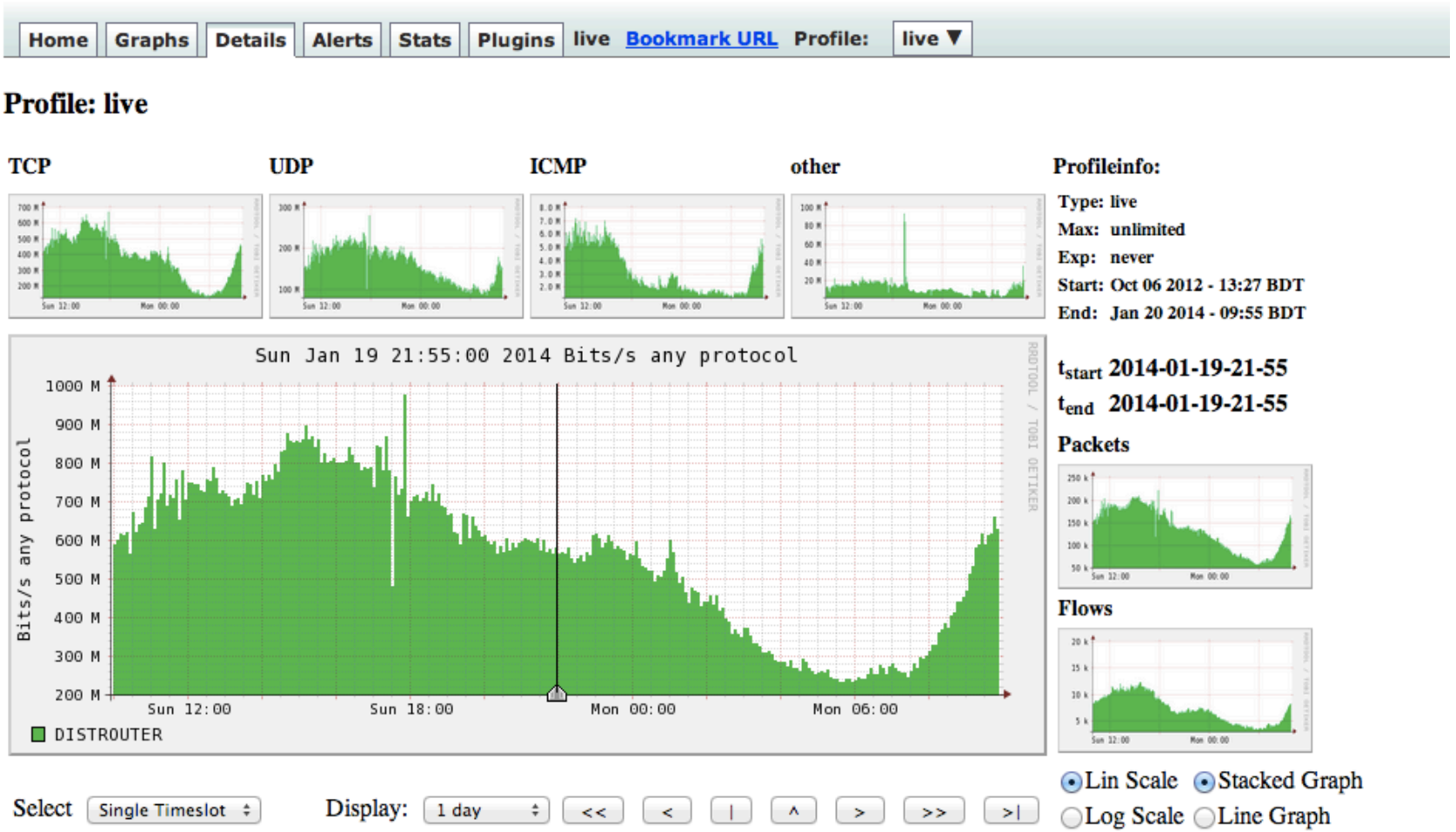
IRT Object

- Why provide abuse contact
  - Dedicated contacts or team that specifically resolve computer security incidents
  - Efficient and accurate response
  - Stops the tech-c and admin-c from getting abuse reports
  - Shared response to address abuse

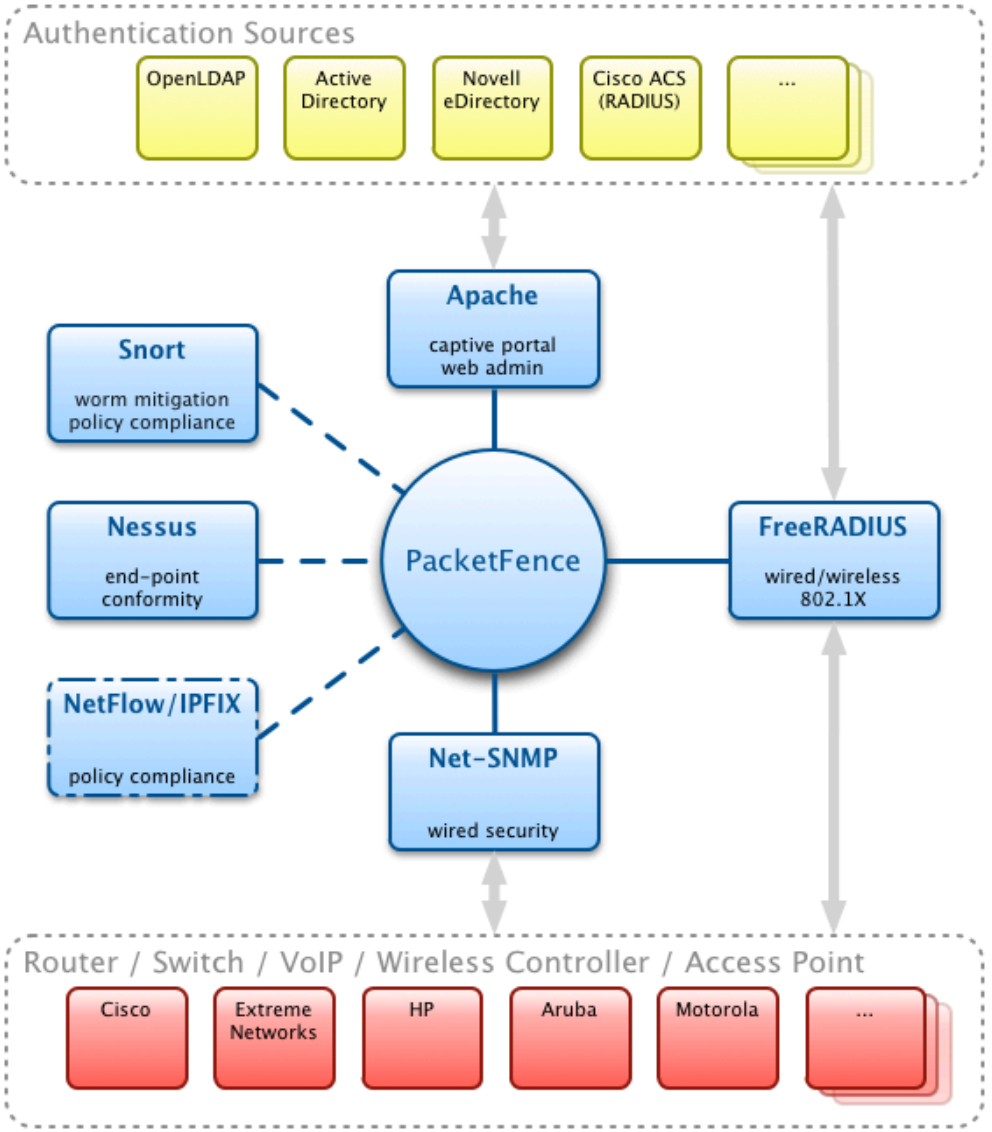
Other Tools

- Logging and monitoring systems
  - Syslog, SNMP, Nagios, Cacti, Netflow, Nfsen
- Detection and data gathering
  - IDS system, active scanners, packet analyzers, Netflow
- Firewalls and NAC
  - IPTables, Packetfence

NetFlow


Home
Graphs
Details
Alerts
Stats
Plugins
live
Bookmark URL
Profile:
live
Profile: live
TCP
UDP
ICMP
other
Profileinfo:
Type: live
Max: unlimited
Exp: never
Start: Oct 06 2012 - 13:27 BDT
End: Jan 20 2014 - 09:55 BDT
Sun Jan 19 21:55:00 2014 Bits/s any protocol
Bits/s any protocol
1000 M
900 M
800 M
700 M
600 M
500 M
400 M
300 M
200 M
Sun 12:00
Sun 18:00
Mon 00:00
Mon 06:00
DISTROUTER
t_{start} 2014-01-19-21-55
t_{end} 2014-01-19-21-55
Packets
Flows
Select
Single Timeslot
Display:
1 day
<<
<
|
^
>
>>
>|
Lin Scale
Stacked Graph
Log Scale
Line Graph

Packetfence



Host Security

- Encrypting emails
  - IMAPS
  - SMTP over TLS/SSL
  - Use PGP
- Browser
  - Set browser preferences
  - Add-ons or plugins (NoScript, HTTPS Everywhere, Adblock, etc)
- File encryption
  - Full disk encryption (FileVault for Mac, Bitlocker on Windows, Truecrypt)

The Challenge

- Keeping up with the security requirements of changing technology
  - Policies and standards must be updated
- Changing usage – more mobile phones, BYOD
- Think like a hacker

Security Management

- Network security is a part of a bigger information security plan
- Policies vs. Standards vs. Guidelines
- Must develop and implement comprehensive security policy
  - Minimum password length, frequency of password change
  - Access of devices, host firewalls
  - User creation/deletion process
  - Data signing/encryption
  - Encrypting all communication (remote access)
  - Use of digital certificates
- Disaster Recovery and Attack Mitigation Plan

Questions

APRICOT 2014

Thank you!