Internet and Network Security Fundamentals

Presenters

- Champika Wijayatunga

  Training Manager, APNIC

  champika@apnic.net

Overview

- Network Security Basics
- Security Issues, Threats and Attacks
- Cryptography and Public Key Infrastructure
- Security on Different Layers
- Layer 2 and BGP Security
- Server and Operational Security

Acknowledgements

- Merike Kaeo from Double Shot Security and the author of “Designing Network Security”.

- APNIC acknowledges her contribution and support with appreciation and thanks.

Network Security Basics

Why Security?

- Security threats are real…
  - And need protection against
- Fundamental aspects of information must be protected
- We can’t keep ourselves isolated from the INTERNET

Why Security?

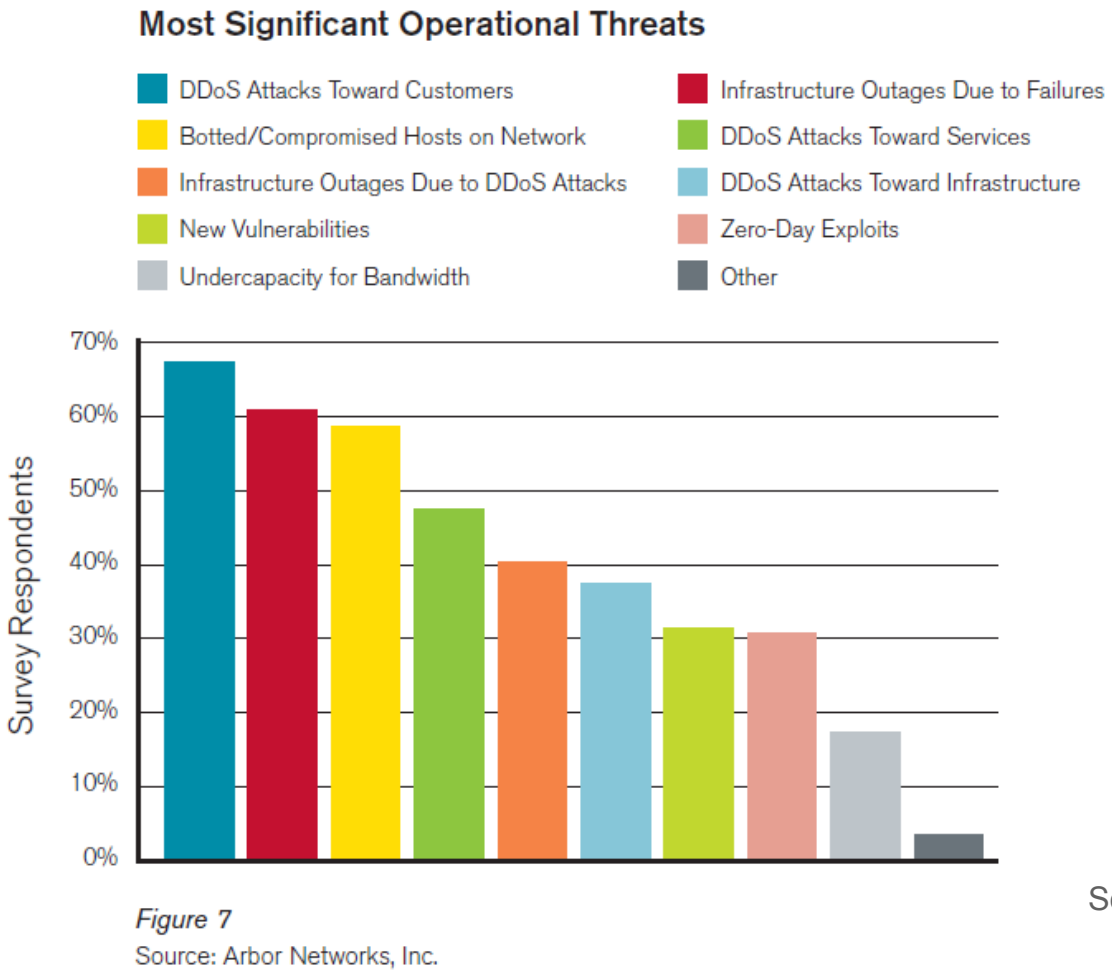
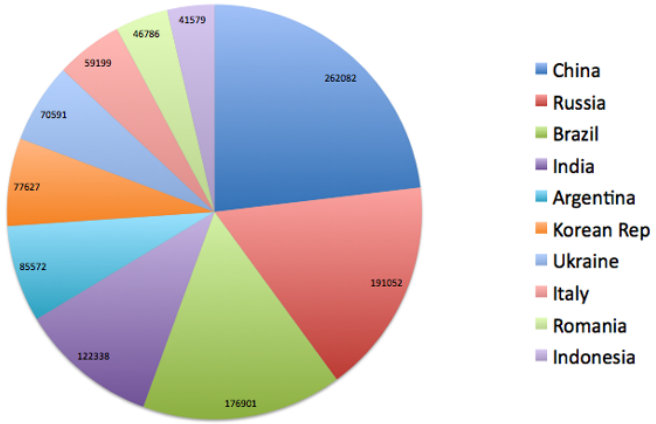


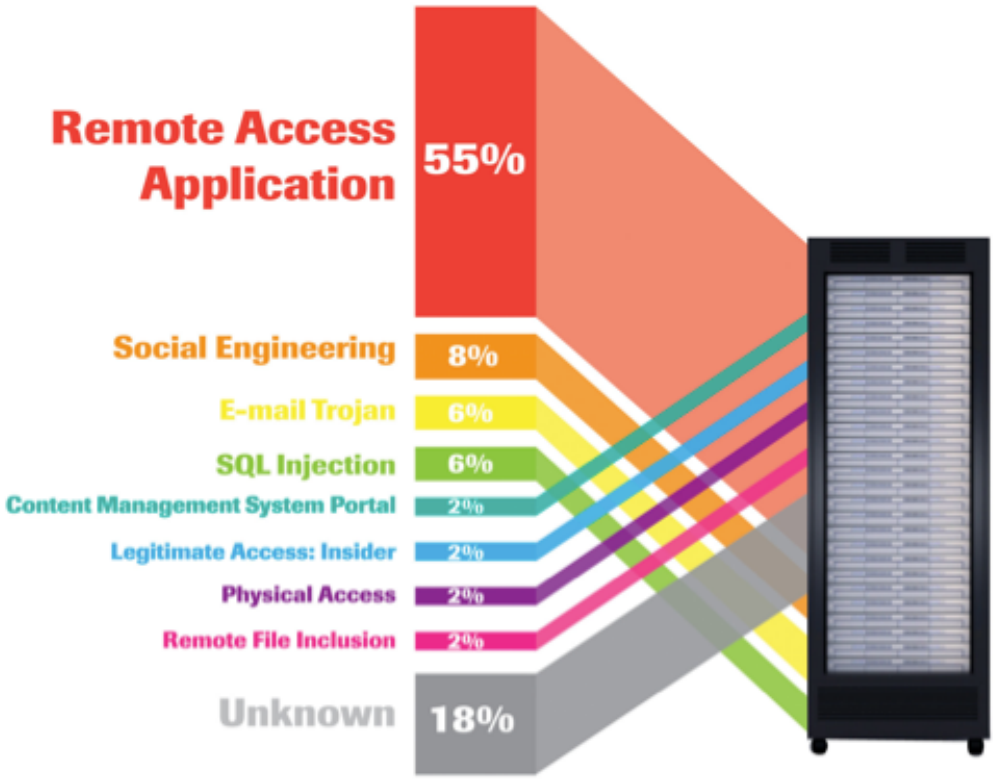
Figure 7
Source: Arbor Networks, Inc.



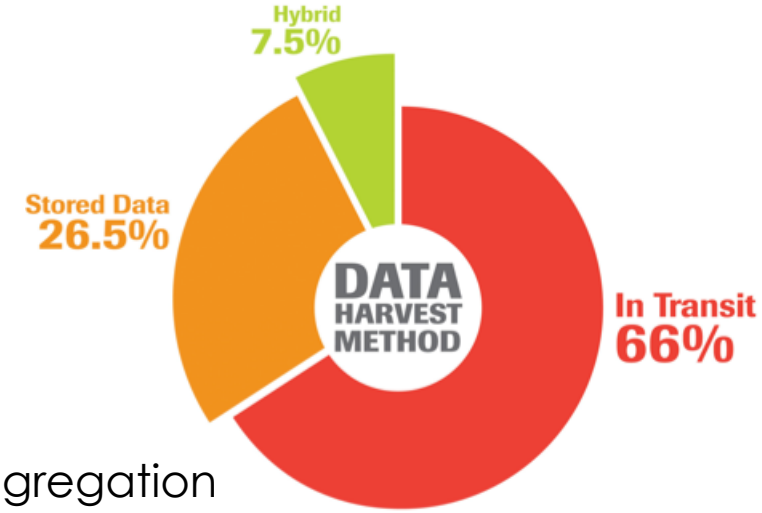
Source: http://www.arbornetworks.com/report

Most infrastructure attacks are unreported

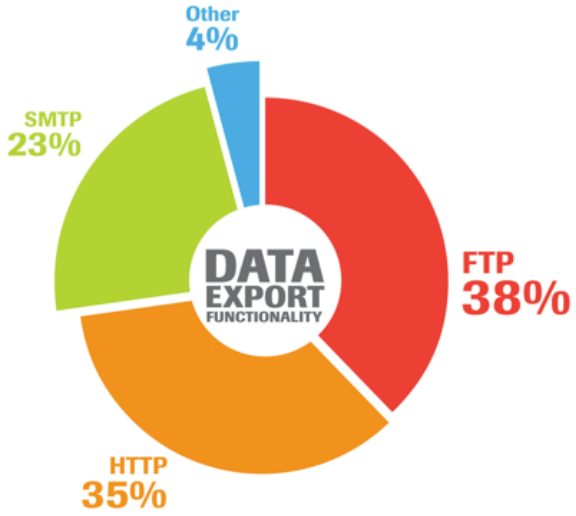
Breach Sources



Infiltration



Aggregation



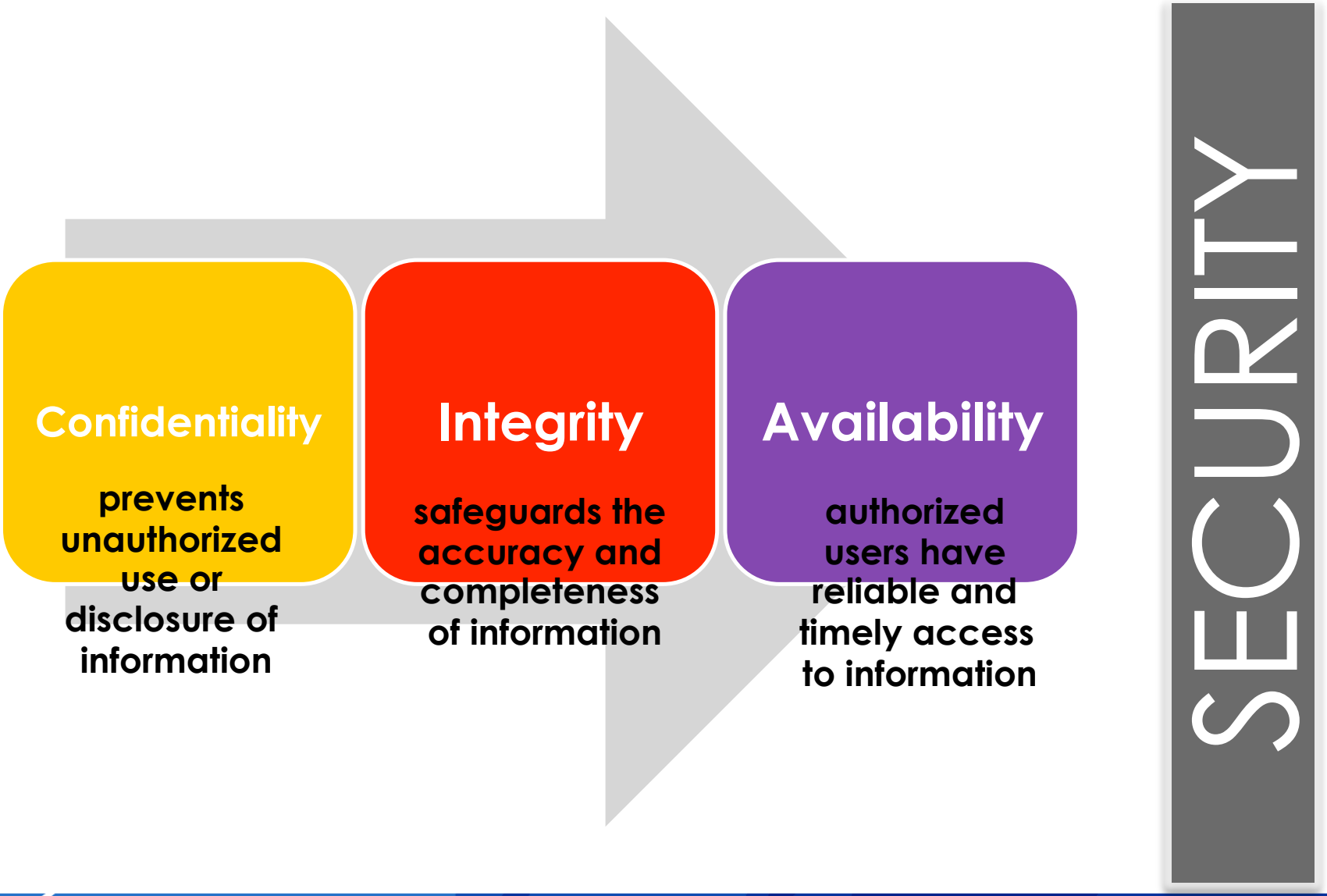
Exfiltration

Source: Trustwave Global Security Report
https://www.trustwave.com/global-security-report.php

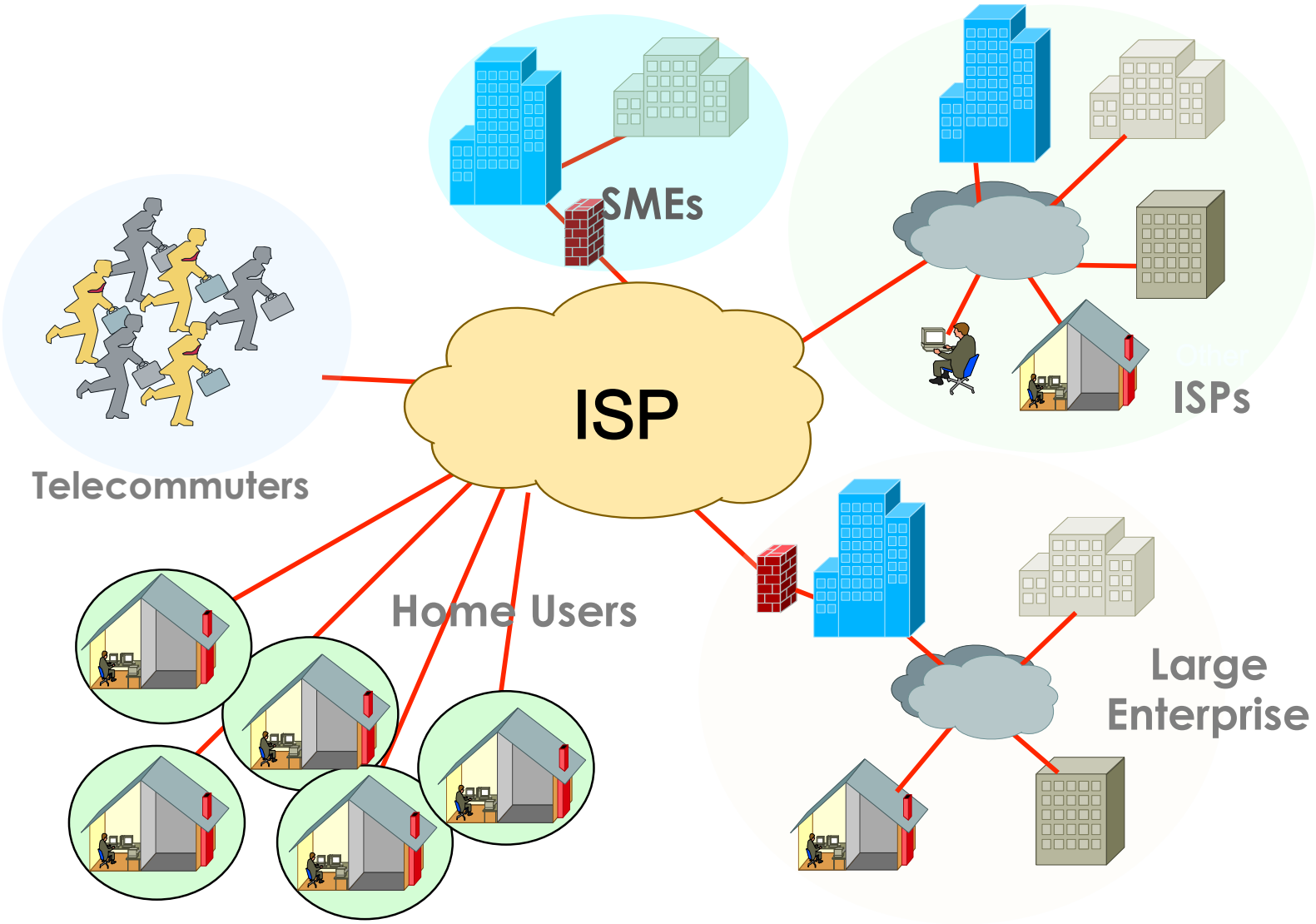
Types of Security

- Computer Security
  - generic name for the collection of tools designed to protect data and to thwart hackers
- Network Security
  - measures to protect data during their transmission
- Internet Security
  - measures to protect data during their transmission over a collection of interconnected networks

Goals of Security



Basic ISP Infrastructure



Module 2

NETWORK SECURITY CONCEPTS

Terminology

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

AAA

- Authentication
- Authorization
- Accountability

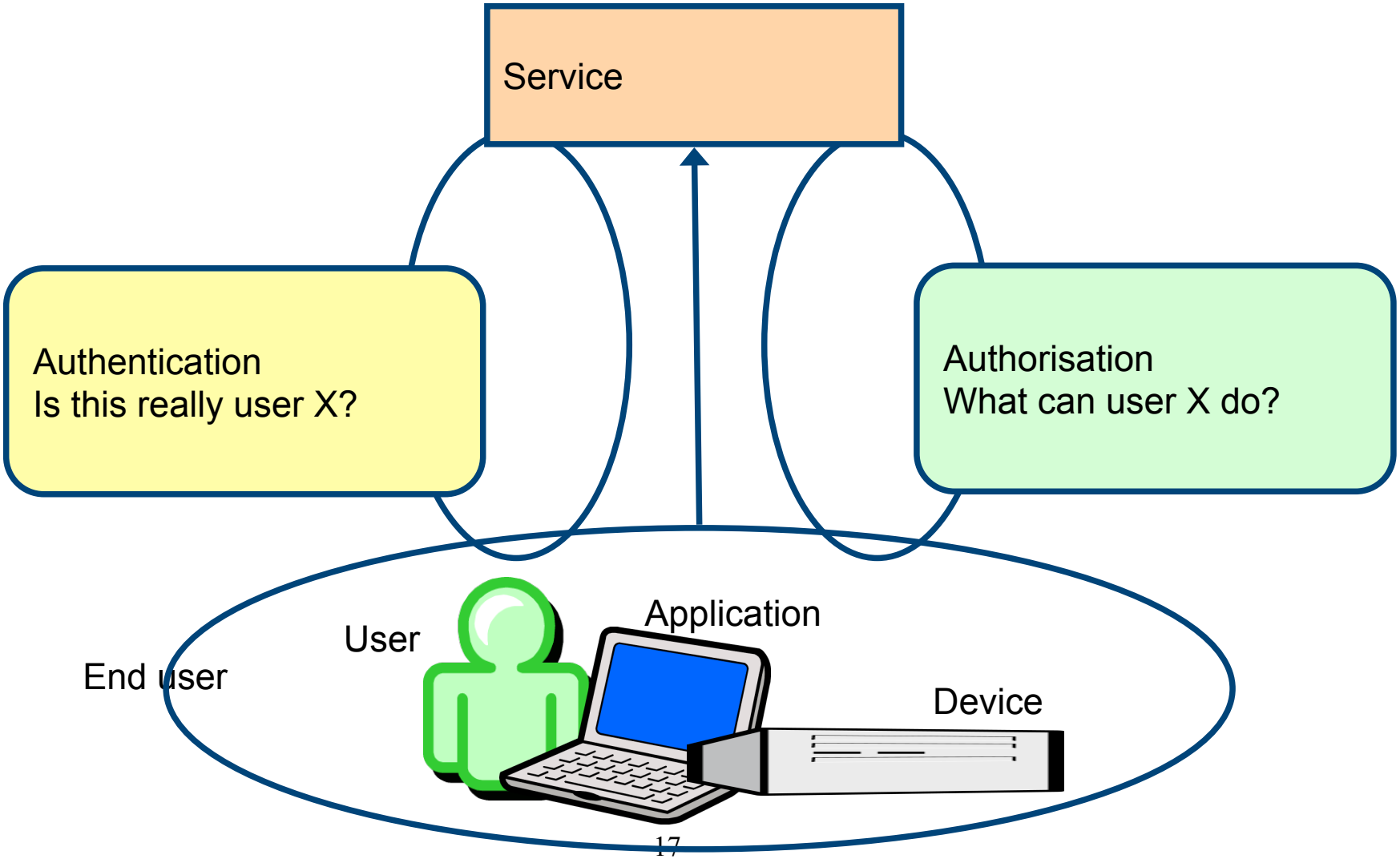
Authentication

- Validating a claimed identity of an end user or a device such as host, server, switch, router, etc.
- *Must be careful to understand whether a technology is using user, device or application authentication.*

Authorization

- The act of granting access rights to a user, groups of users, system, or program.
  - Typically this is done in conjunction with authentication.

Authentication and authorisation



Non-Repudiation

- A property of a cryptographic system that prevents a sender from denying later that he or she sent a message or performed a certain action.

Audit

A chronological record of system activities that is sufficient to enable the reconstruction and examination of a given sequence of events

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
- Exploit
  - Taking advantage of a vulnerability

Risk

- The possibility that a particular vulnerability will be exploited
  - Risk analysis: the process of identifying:
    - Security risks
    - Determining their impact
    - And identifying areas require protection

Threat

- Any circumstance or event with the potential to cause harm to a networked system
  - Denial of service

    Attacks make computer resources (e.g., bandwidth, disk space, or CPU time) unavailable to its intended users
  - Unauthorised access

    Access without permission issues by a rightful owner of devices or networks
  - Impersonation
  - Worms
  - Viruses

Risk management vs. cost of security

- Risk mitigation
  - The process of selecting appropriate controls to reduce risk to an acceptable level
- The level of acceptable risk
  - Determined by comparing the risk of security hole exposure to the cost of implementing and enforcing the security policy
- Assess the cost of certain losses and do not spend more to protect something than it is actually worth

Attack sources

- Active vs. passive
  - Active = Writing data to the network

    Common to disguise one's address and conceal the identity of the traffic sender
  - Passive = Reading data on the network

    Purpose = breach of confidentiality

    Attackers gain control of a host in the communication path between two victim machines

    Attackers has compromised the routing infrastructure to arrange the traffic pass through a compromised machine

Attack sources

- On-path vs. Off-path
  - On-path routers (transmitting datagrams) can read, modify, or remove any datagram transmitted along the path
  - Off-path hosts can transmit datagrams that appear to come from any hosts but cannot necessarily receive datagrams intended for other hosts

    If attackers want to receive data, they have to put themselves on-path
  - How easy is it to subvert network topology?

    It is not easy thing to do but, it is not impossible
- Insider or outsider
  - What is definition of perimeter/border?
- Deliberate attack vs. unintentional event
  - Configuration errors and software bugs are as harmful as a deliberate malicious network attack

What are security aims?

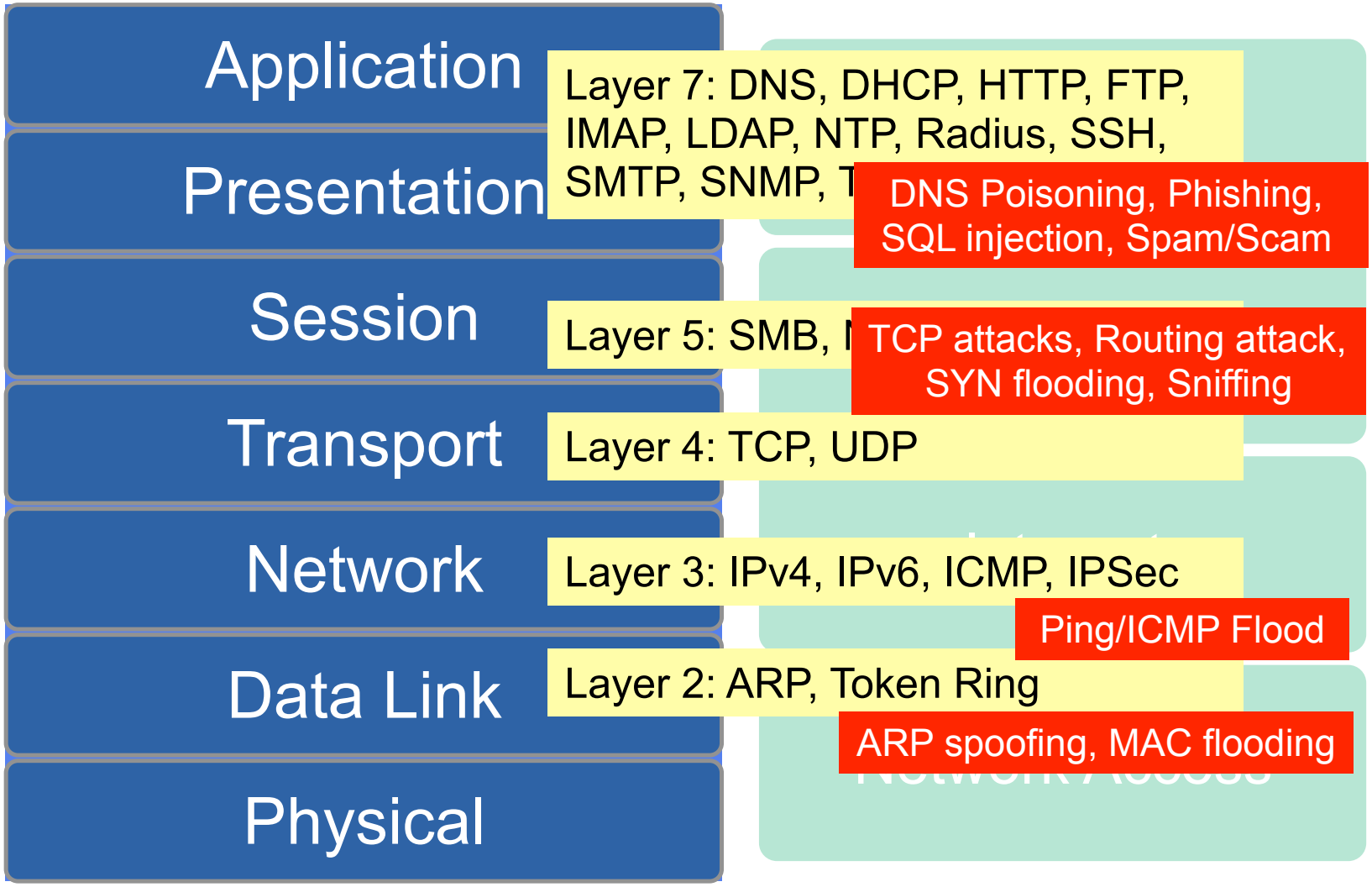
- Controlling data / network access
- Preventing intrusions
- Responding to incidences
- Ensuring network availability
- Protecting information in transit

Security services

- Authentication
- Authorisation
- Access control
- Data integrity
- Data confidentiality
- Auditing / logging
- DoS mitigation

Threats and Attacks

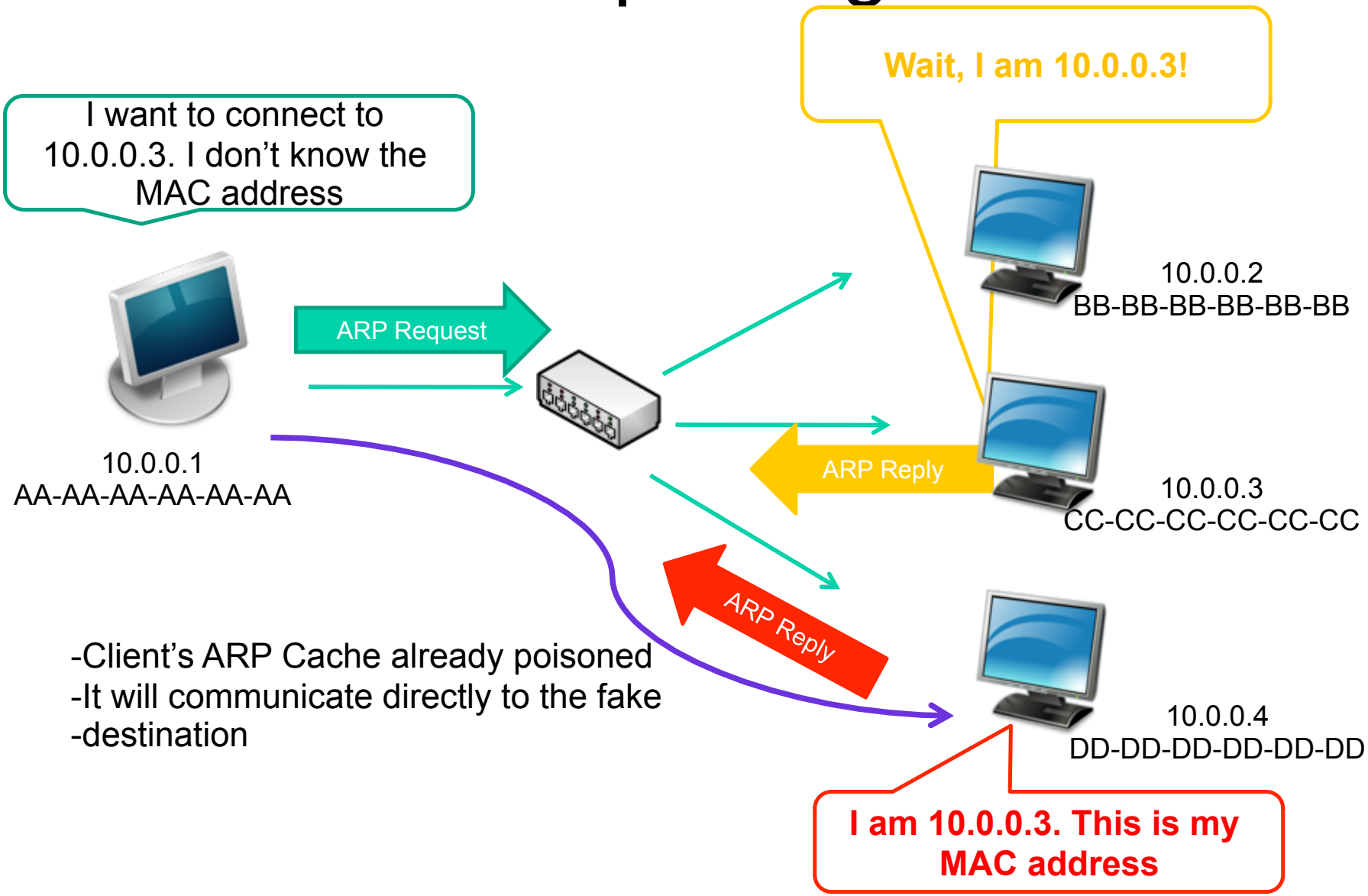
Attacks on Different Layers



Layer 2 Attacks

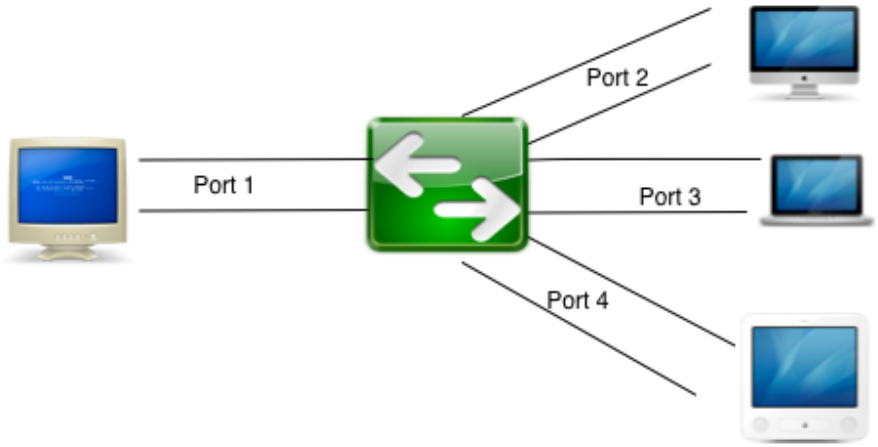
- ARP Spoofing
- MAC attacks
- DHCP attacks
- VLAN hopping

ARP Spoofing



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.



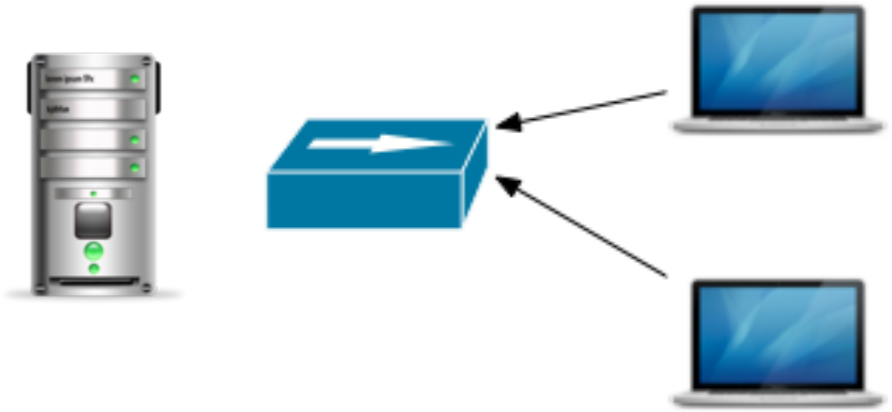
	Port 1	Port 2	Port 3	Port 4
00:01:23:45:67:A1	x			
00:01:23:45:67:B2		x		
00:01:23:45:67:C3			x	
00:01:23:45:67:D4				x

VLAN Hopping

- Attack on a network with multiple VLANs
- Two primary methods:
  - Switch spoofing – attacker initiates a trunking switch
  - Double tagging – packet is tagged twice.

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.

DHCP Attack Types

- Solution: enable DHCP snooping

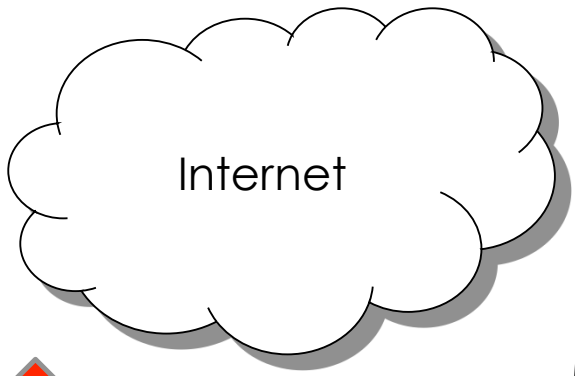
```
ip dhcp snooping (enable dhcp snooping globally)
ip dhcp snooping vlan <vlan-id> (for specific
  vlans)
ip dhcp snooping trust
ip dhcp snooping limit rate <rate>
```

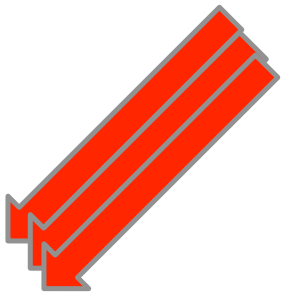
Layer 3 Attacks

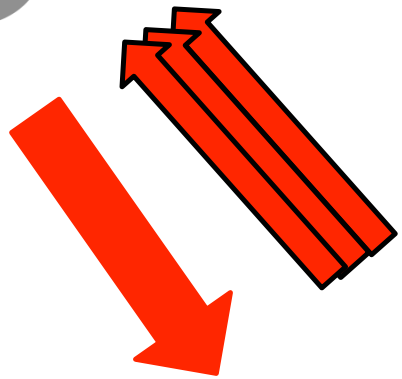
- ICMP Ping Flood
- ICMP Smurf
- Ping of death

Ping Flood

Attacker

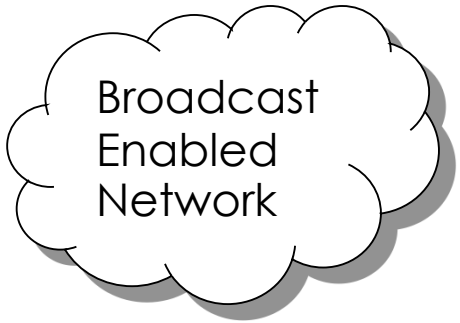






Victim

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

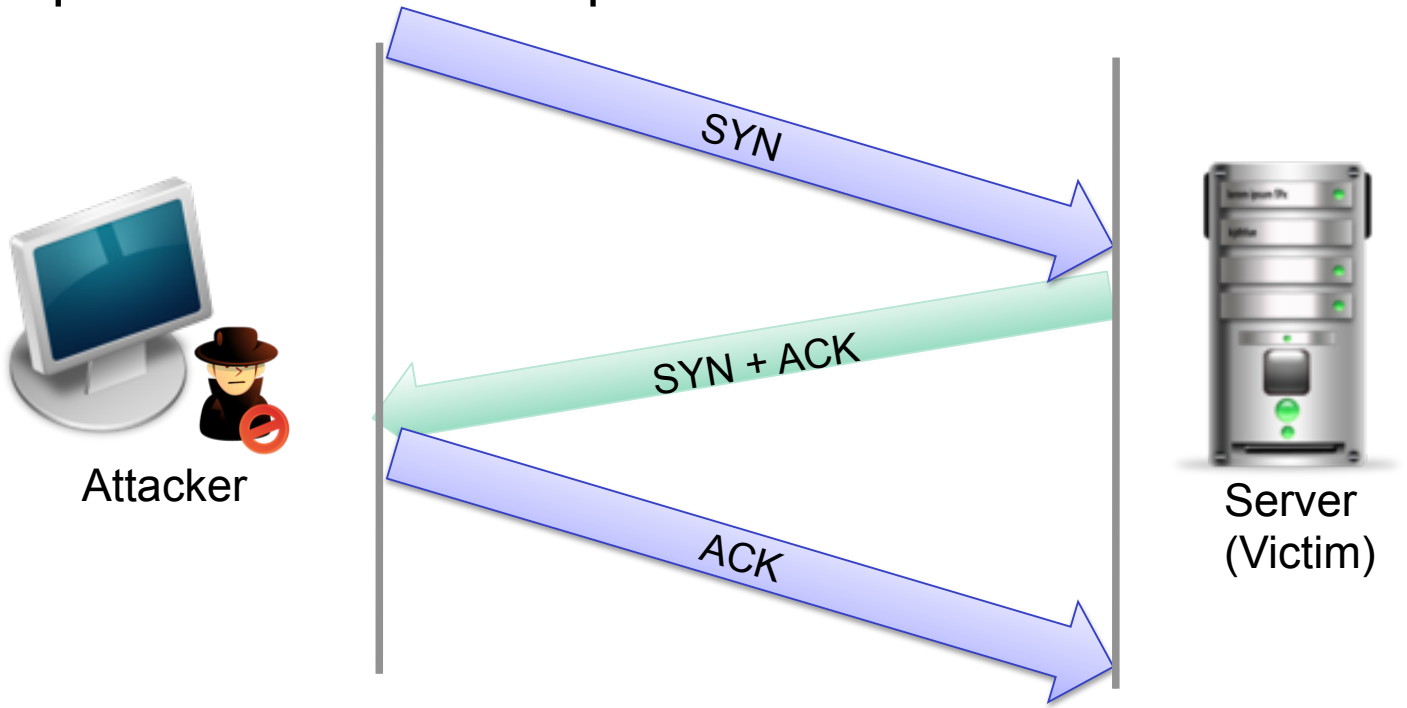


TCP Attacks

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



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

Application Layer Attacks

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

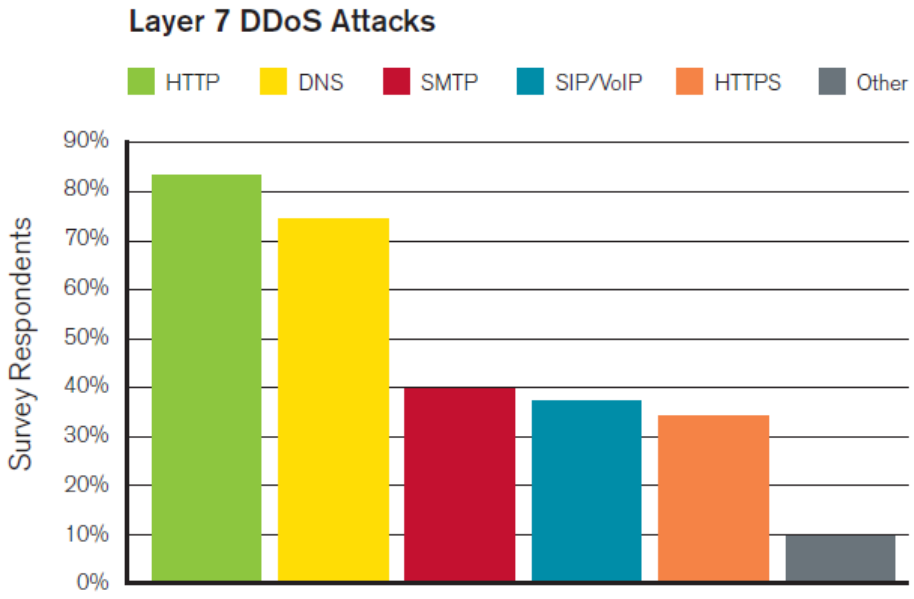


Figure 8
Source: Arbor Networks, Inc.

Application Layer Attacks

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

Server Side Scripting

- Server-side scripting – program is executed on the server and not on the user's browser or plugin.
- ASP.NET, PHP, mod_perl, CGI, Ruby, Python
- Benefits:
  - Cross-platform
  - No plugin required on user side
- Disadvantages:
  - Dynamic scripts create new security concern, exploiting code flaws

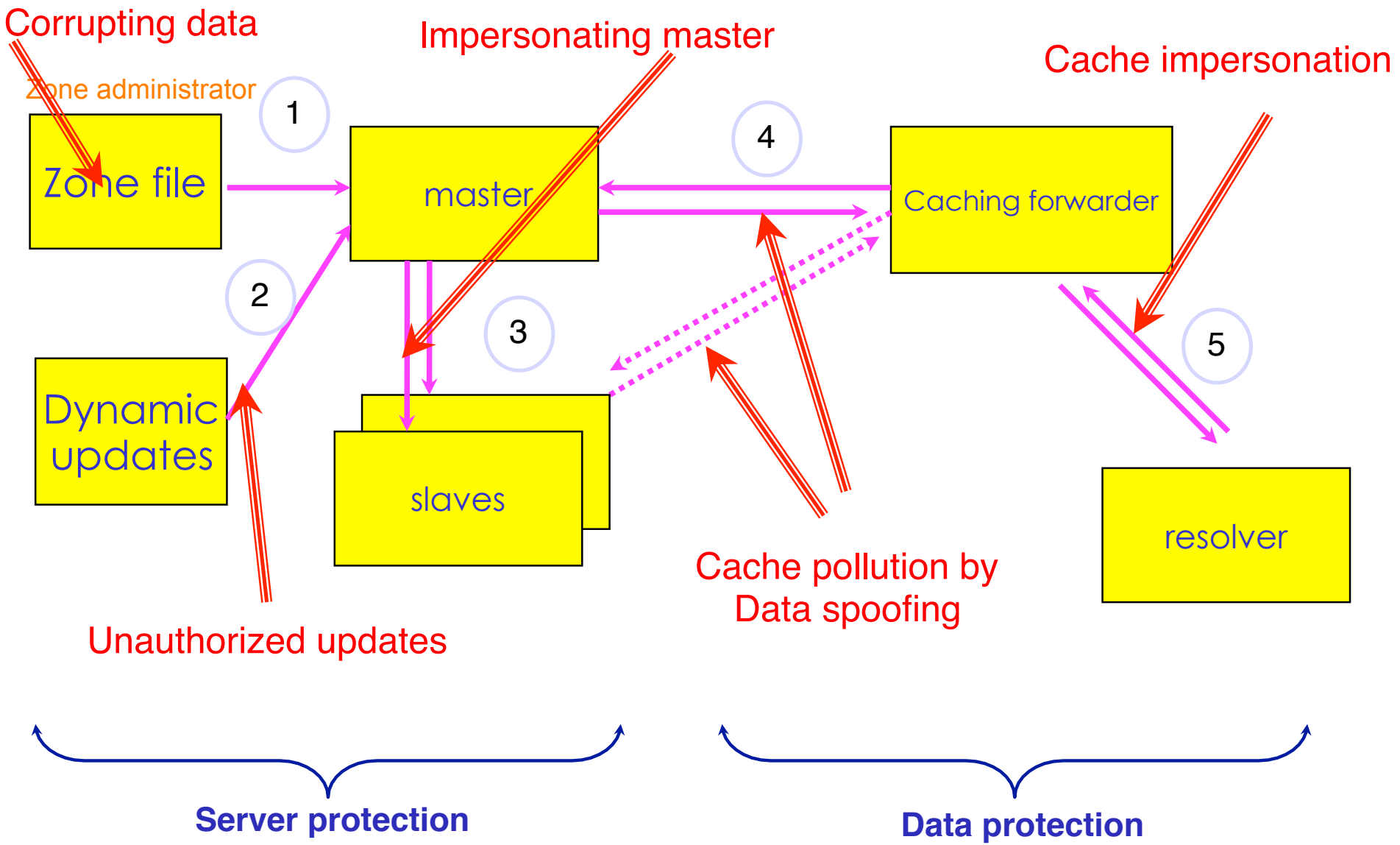
Cross-Site Scripting

- Cross-site scripting or XSS – enables attackers to inject scripts into webpages viewed by other users.
- Persistent XSS – more devastating
- Non-persistent XSS – more common
- Ex: BeEF (Browser Exploitation Framework)

SQL Injection

- SQL Injection – a subset of unverified user input vulnerability that injects malicious code (or SQL query) into strings. This code is executed when passed on to the SQL server.

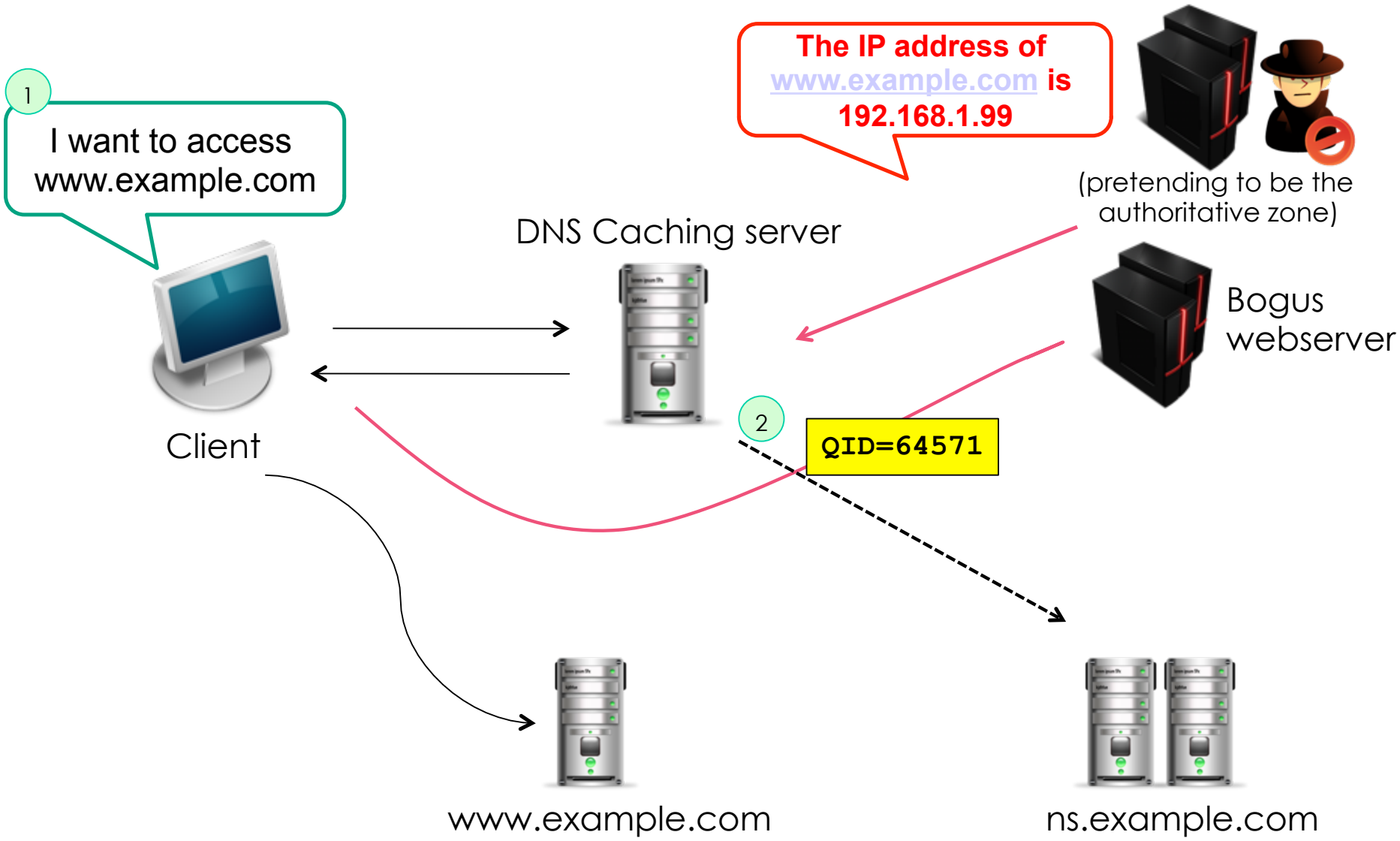
DNS Vulnerabilities



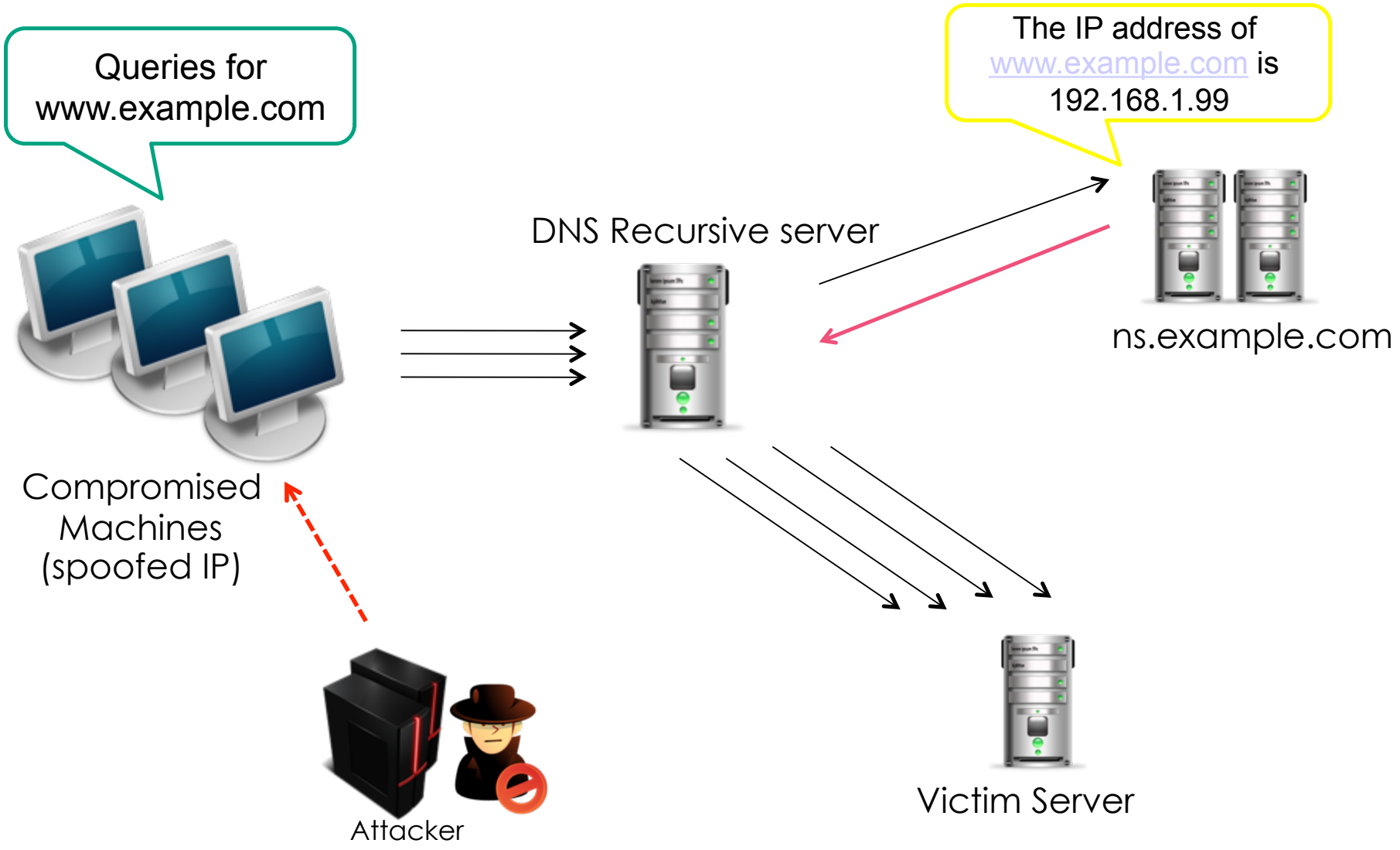
DNS Cache Poisoning

- 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



Common Types of Attack

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

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 attack were released to crack WEP more effectively and faster

Man in the Middle Attacks (Wireless)

- Creates a fake access point and have clients authenticate to it instead of a legitimate one.
- Capture traffic to see usernames, passwords, etc that are sent in clear text.

How to crash the Internet

By Steven J. Vaughan-Nichols | February 13, 2011, 10:39am PST

Summary

The Internet was designed to survive a nuclear war, but researchers claim they've found a way to take down the Internet.

Topics

Router, Attack, Max Schuchard, CXPST, CXPST Attack, BGP, Internet, Routers & Switches, Networking, Security, *more +*

Blogger Info

Steven J. Vaughan-Nichols

Bio Contact

Vendor HotSpot

We know you can take down Web sites with Distributed Denial of Service (DDoS) attacks. We know that a country, like Egypt, can knock down a country's entire Internet infrastructure. And, we thought we knew that you couldn't take down the entire Internet. It turns out we could be wrong.

In a report from New Scientist, Max Schuchard a computer science graduate student and his buddies claim they've found a way to launch DDoS attacks on Border Gateway Protocol (BGP) network routers that could crash the Internet.

BGP is an essential Internet protocol. It's the routing protocol used to exchange routing information across the Internet. Without it ISPs couldn't connect to each other and you couldn't connect Web sites and services outside of your local intranet. Because network connections and routers ar constantly changing, BGP routers and switches are constantly working to keep current route maps of the Internet. In short, you don't want to mess it.

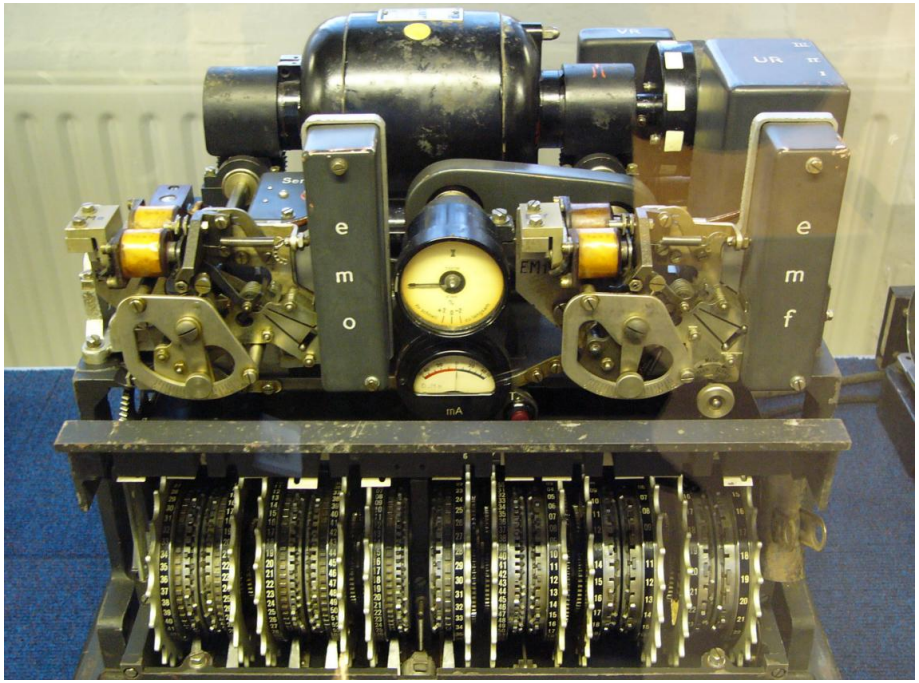
http://www.zdnet.com/blog/networking/how-to-crash-the-internet/680?

How do we protect our system?

Cryptography

Cryptography

- Has evolved into a complex science in the field of information security



What is Cryptography?

- Part of a field of study known as cryptology
- Cryptology includes:
  - Cryptography
    - Study of methods for secret writing
    - Transforming messages into unintelligible form
    - Recovering messages using some secret knowledge (key)
  - Cryptanalysis:
    - Analysis of cryptographic systems, inputs and outputs
    - To derive confidential information

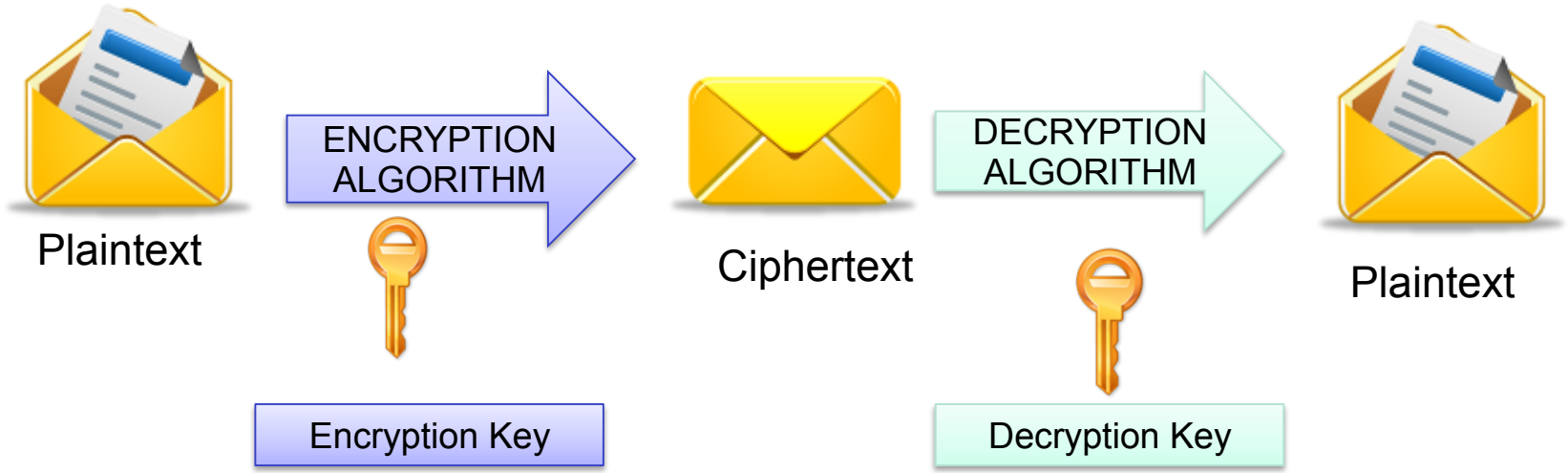
Cryptography

- Encryption – process of transforming plaintext to ciphertext using a cryptographic key
- Symmetric key cryptography – uses a single key to both encrypt and decrypt information. Also known as private key.
  - Includes DES, 3DES, AES, IDEA, RC5, Blowfish
- Asymmetric key cryptography – separate keys for encryption and decryption (public and private key pairs)
  - Includes RSA, Diffie-Hellman, El Gamal

Terminology of cryptography

- Cipher
  - Cryptographic technique (algorithm) applying a secret transformation to messages
- Plaintext / cleartext
  - Original message or data
- Encryption
  - Transforming plaintext, using a secret key, so meaning is concealed
- Ciphertext
  - Unintelligible encrypted plaintext
- Decryption
  - Transforming ciphertext back into original plaintext
- Cryptographic Key
  - Secret knowledge used by cipher to encrypt or decrypt message

Cryptography



Symmetric Key Algorithm

- Stream ciphers – encrypts bits of the message at a time
- Block ciphers – takes a block of bits and encrypts them as a single unit

Cryptography

- Digital Signature – sender encrypts message with own private key instead of encrypting with intended receiver's public key
- Message digests – produces a condensed representation of a message (hashing)
  - MD5
  - SHA-1
  - HMAC

Secret Key Algorithms

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

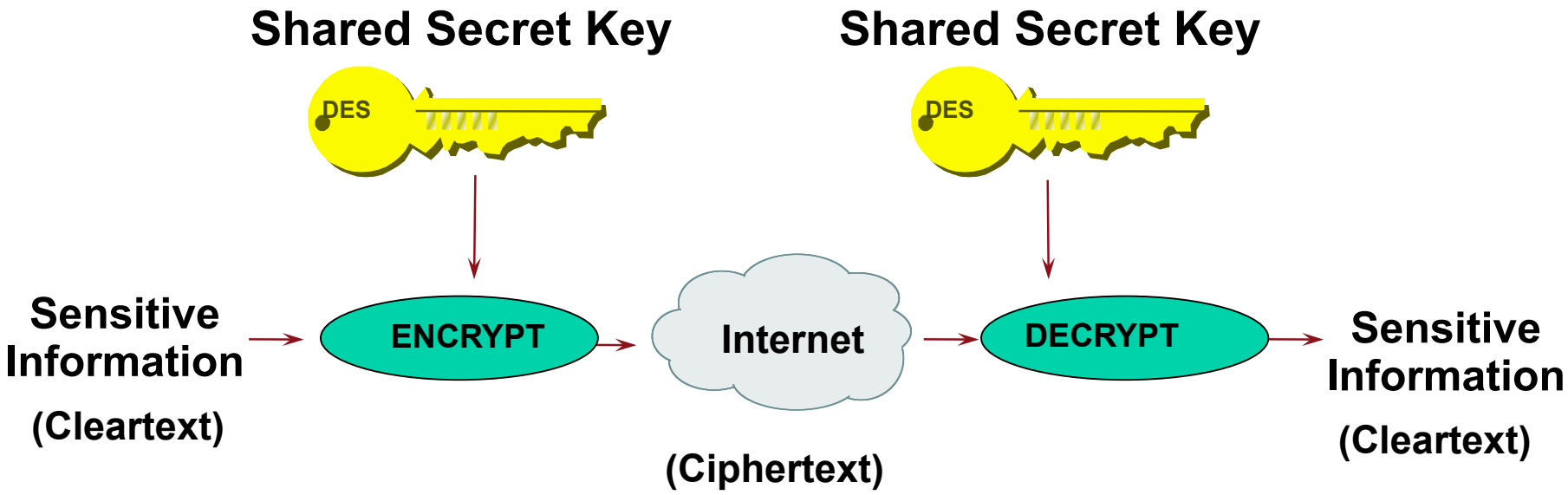
DES

- Data Encryption Standard
- Developed by IBM for the US government in 1973-1974, and approved in Nov 1976.
- Based on Horst Feistel's Lucifer cipher
- block cipher using shared key encryption, 56-bit key length
- Block size: 64 bits

Triple DES

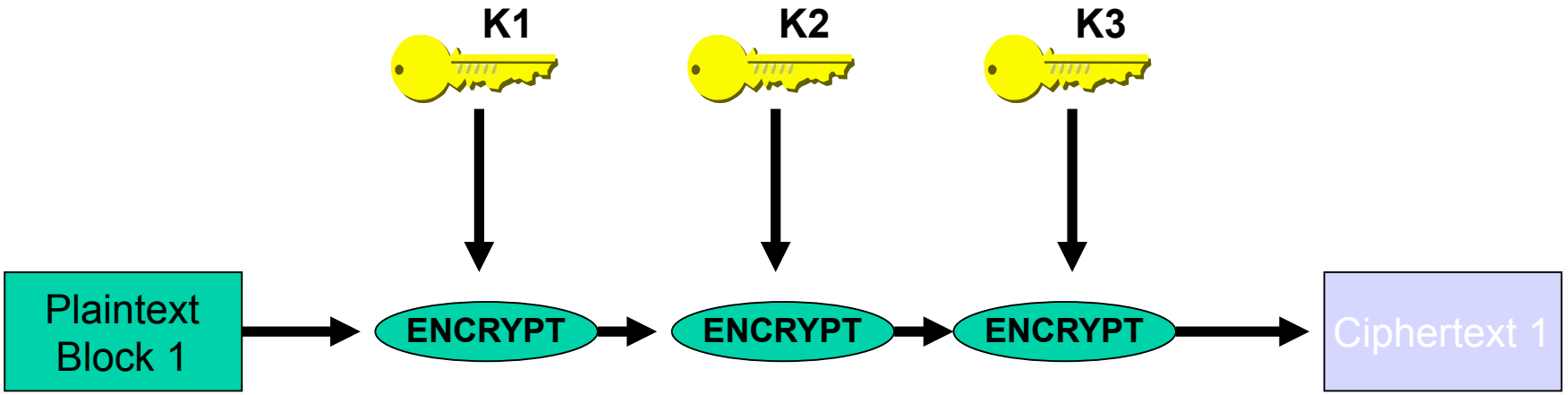
- 3DES (Triple DES) – a block cipher that applies DES three times to each data block
- Uses a key bundle comprising of three DES keys (K1, K2, K3), each with 56 bits excluding parity.
- DES encrypts with K1, decrypts with K2, then encrypts with K3
  - $C_i = E_{K1}(D_{K2}(E_{K1}(P_i)))$
- Disadvantage: very slow

Secret Key Encryption



Common Algorithms: DES, 3DES, AES, IDEA

Triple DES (3DES)



- Many applications use K3=K1, yielding a key length of 112 bits
- Interoperable with conventional DES if K1=K2=K3

AES

- Advanced Encryption Standard (AES) Cipher
- Published in November 2001
- Symmetric block cipher
- Has a fixed block size of 128 bits
- Has a key size of 128, 192, or 256 bits
- Based on Rijndael cipher which was developed by Joan Daemen and Vincent Rijmen

Hash Functions

A *hash function* takes an input message of arbitrary length and outputs fixed-length code. The fixed-length output is called the *hash*, or the *message digest*, of the original input message.

Common Algorithms: MD-5 (128), SHA-1 (160)

Hashing

- Also called a digest or checksum
- A form of signature that represents the data.
- Uses:
  - Verifying file integrity - if the hash changes, it means the data is either compromised or altered in transit.
  - Digitally signing documents
  - Hashing passwords

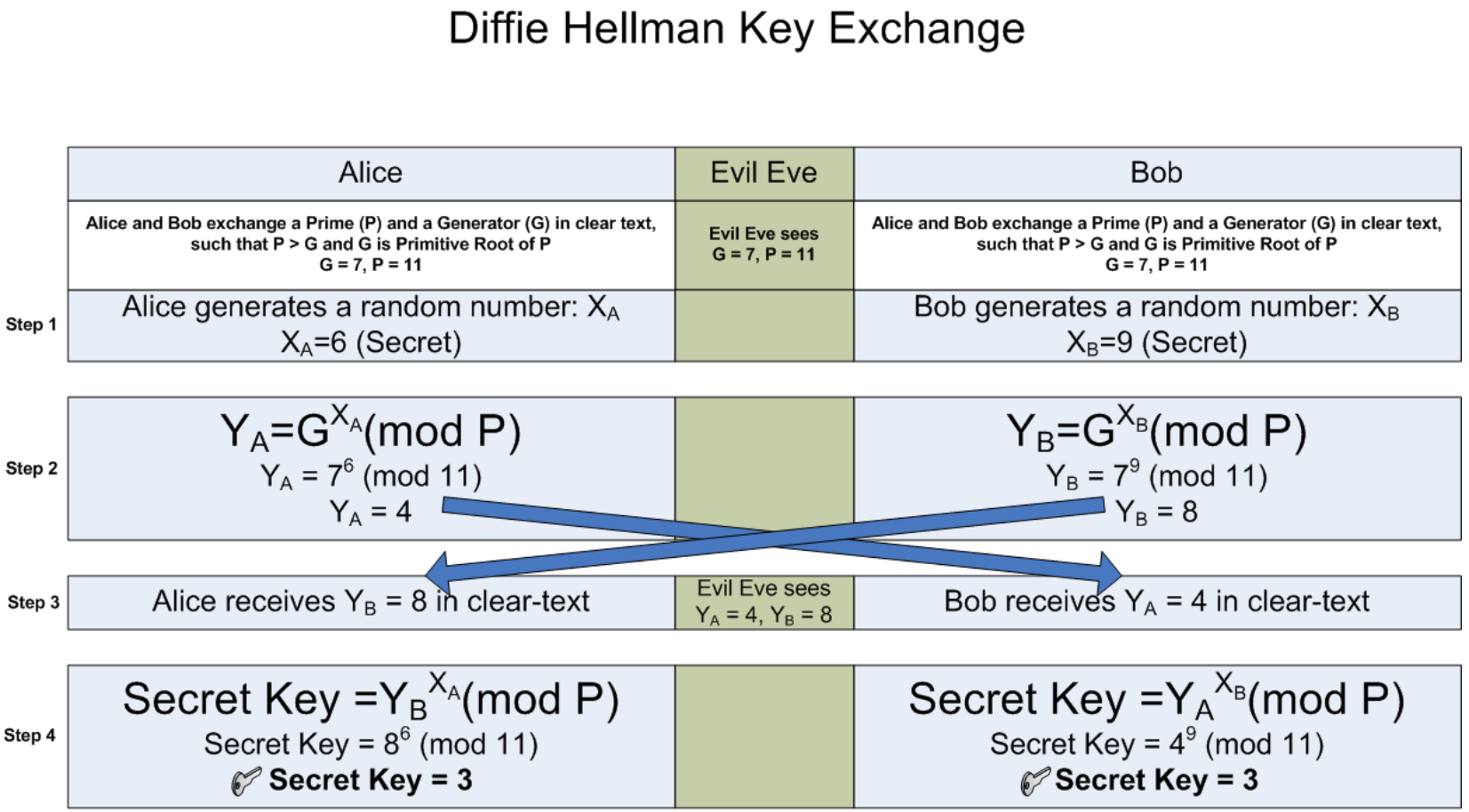
Hashing

- MD5 Message Digest Algorithm
  - Outputs a 128-bit fingerprint of an arbitrary-length input
- SHA-1 (Secure Hash Algorithm)
  - Outputs a 160-bit message digest similar to MD5
  - Widely-used on security applications (TLS, SSL, PGP, SSH, S/MIME, IPsec)

Diffie-Hellman

- Diffie-Hellman Protocol – requires that both the sender and recipient of a message have key pairs.
- Combining one's private key and the other's public key, both parties can compute the same shared secret number.

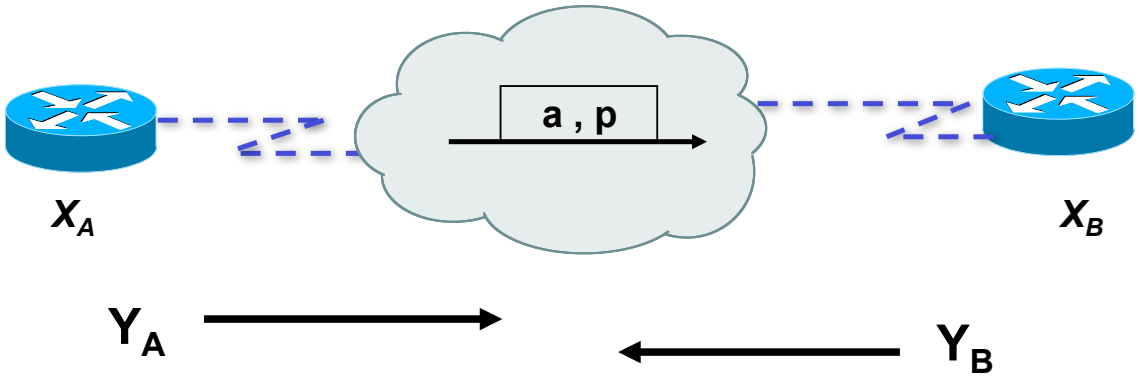
Diffie-Hellman



http://en.wikipedia.org/wiki/File:DiffieHellman.png

DH Man-in-the-Middle Attack

- Diffie-Hellman is subject to a man-in-the-middle attack
- Digital signatures of the ‘public values’ can enable each party to verify that the other party actually generated the value



=> DH exchanges need to be authenticated!!

Trusted Network

- Standard defensive-oriented technologies
  - Firewall
  - Intrusion Detection
- Build TRUST on top of the TCP/IP infrastructure
  - Strong authentication
  - 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

Public Key Infrastructure

Public Key Infrastructure

- Framework that builds the network of trust
- Combines public key cryptography, digital signatures, to ensure confidentiality, integrity, authentication, nonrepudiation, and access control
- Protects applications that require high level of security

PKI Components

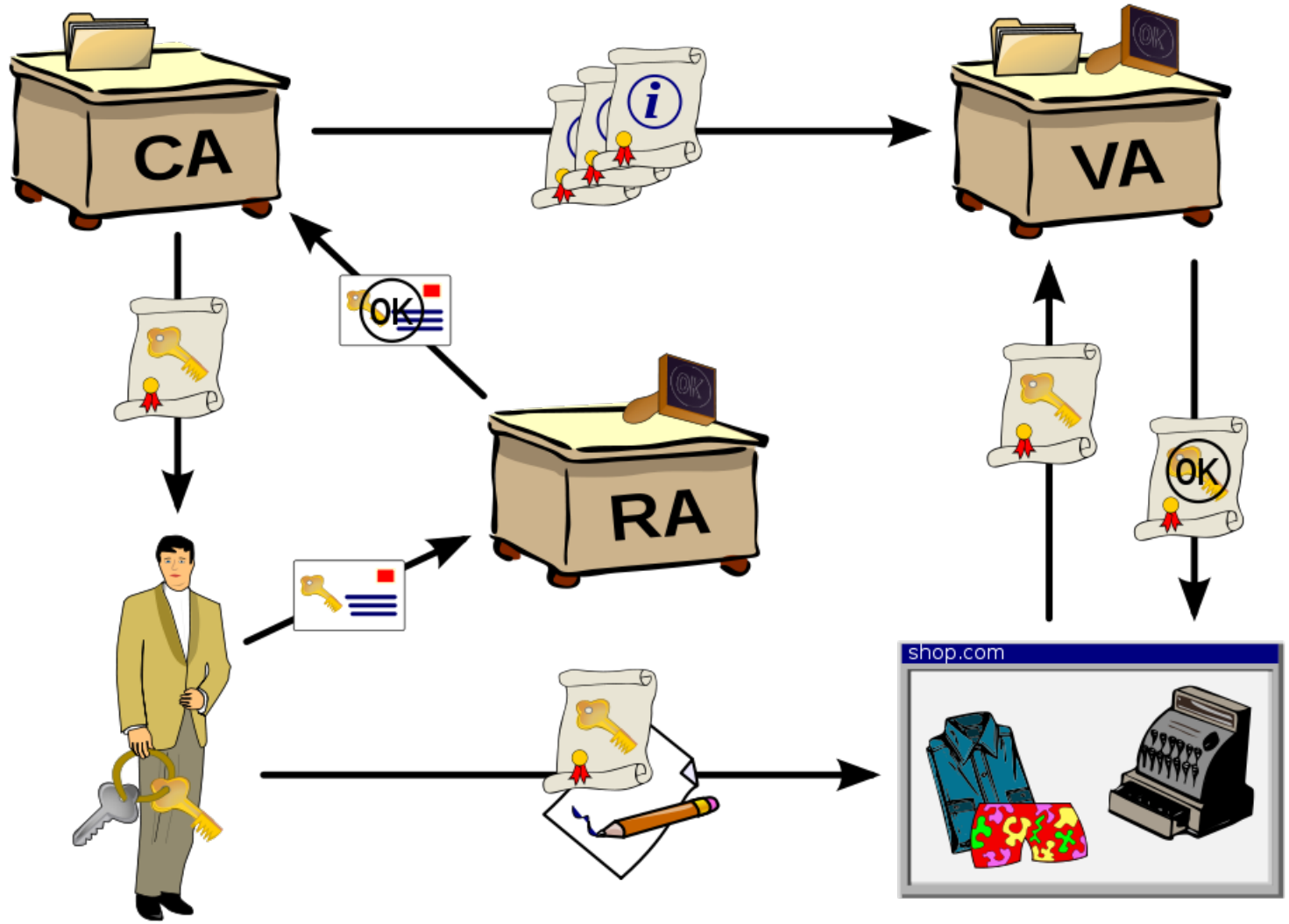
- Certificate Authority (CA) – a trusted third party
  - Trusted by both the owner of the certificate and the party relying upon the certificate
- Registration Authority (RA) – binds keys to users
  - Users who wish to have their own certificate registers with the RA
- Validation Authority (VA) – validates the user is who he says he is

Certificate Authority

- Components:
  - Certificate Authority – a trusted third party

    Trusted by both the owner of the certificate and the party relying upon the certificate.
  - Validation Authority
  - Registration Authority

PKI Process



Source: http://commons.wikimedia.org

Digital Certificate

- Digital certificate – basic element of PKI; secure credential that identifies the owner
- Also called public key certificate

Digital Certificates

- Digital certificates deal with the problem of
  - Binding a public key to an entity
  - A major legal issue related to eCommerce
- A digital certificate contains:
  - User's public key
  - User's ID
  - Other information e.g. validity period
- Certificate examples:
  - X509 (standard)
  - PGP (Pretty Good Privacy)
  - Certificate Authority (CA) creates and digitally signs certificates

Digital Certificates

- To obtain a digital certificate, Alice must:
  - Make a certificate signing request to the CA
  - Alice sends to CA:

    Her identifier Id_A

    Her public key K_{A_PUB}

    Additional information
- CA returns Alice's digital certificate, cryptographically binding her identity to public key:
  - $Cert_A = \{ID_A, K_{A\_PUB}, info, Sig_{CA}(ID_A, K_{A\_PUB}, info)\}$

X.509

- An ITU-T standard for a public key infrastructure for single-sign-on and Privilege Management Infrastructure (PMI)
- Assumes a strict hierarchical system of Certificate Authorities (CAs)
- Structure of a Certificate