Internet Security Introduction

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok

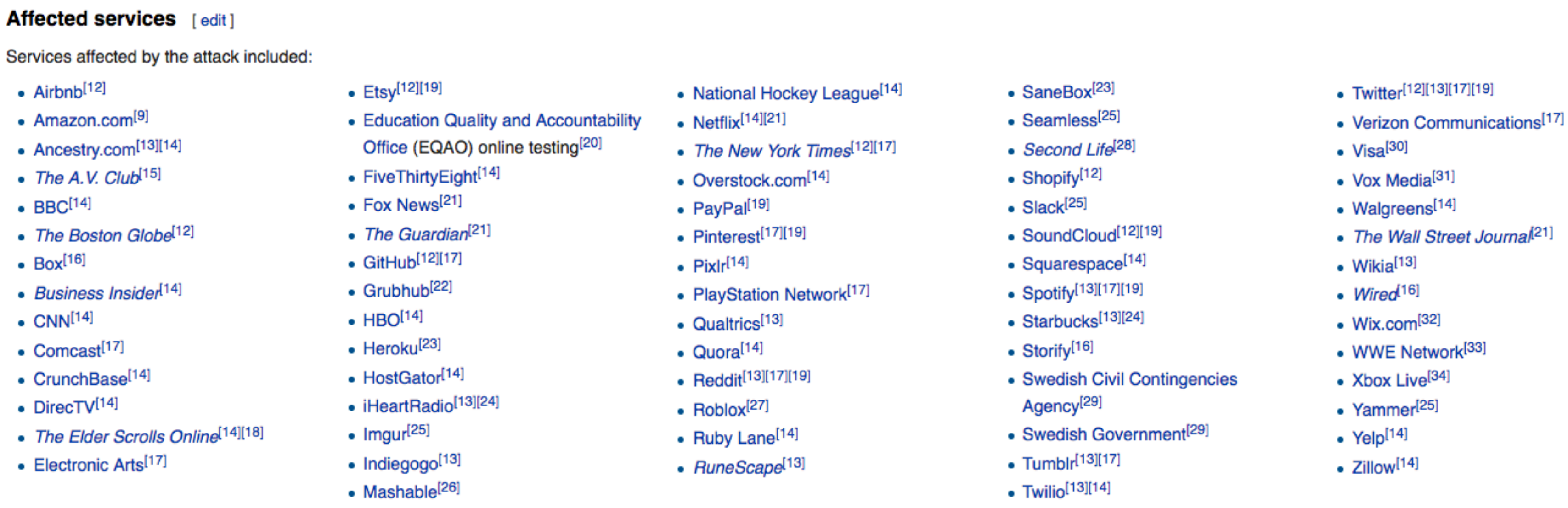
Last updated 29th April 2017

Internet Security Trend

It’s Global Issue

Recent Incidents

- **2016 Dyn cyberattack**
  - With an estimated throughput of **1.2 terabits per second**



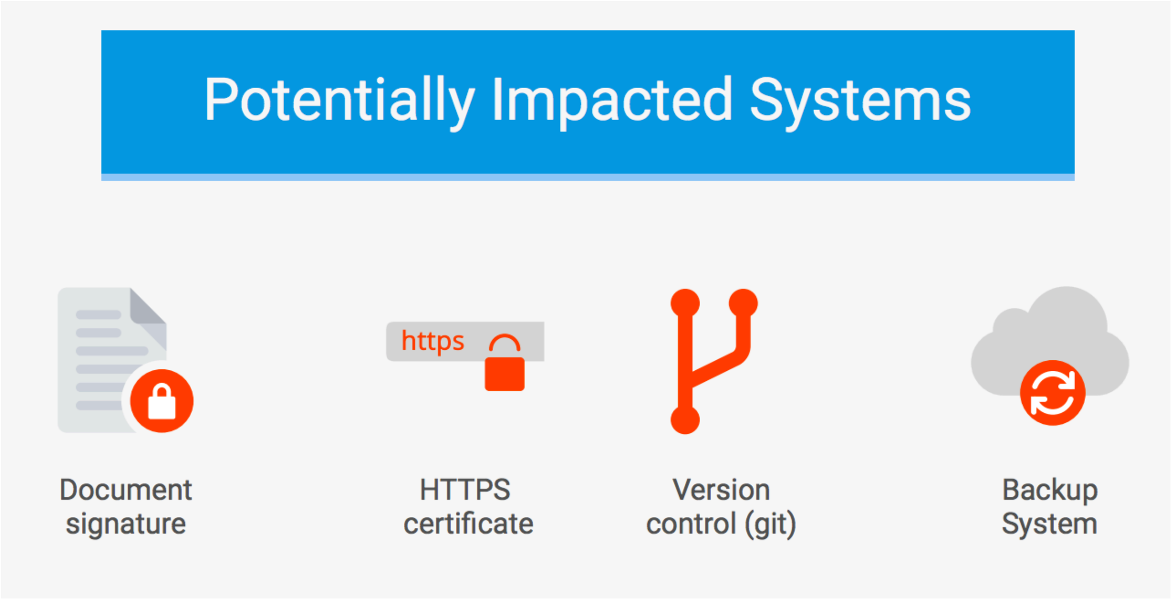
Affected services [edit]

Services affected by the attack included:

- Airbnb[12]
- Amazon.com[9]
- Ancestry.com[13][14]
- *The A.V. Club*[15]
- BBC[14]
- *The Boston Globe*[12]
- Box[16]
- *Business Insider*[14]
- CNN[14]
- Comcast[17]
- CrunchBase[14]
- DirecTV[14]
- *The Elder Scrolls Online*[14][18]
- Electronic Arts[17]
- Etsy[12][19]
- Education Quality and Accountability Office (EQAO) online testing[20]
- FiveThirtyEight[14]
- Fox News[21]
- *The Guardian*[21]
- GitHub[12][17]
- Grubhub[22]
- HBO[14]
- Heroku[23]
- HostGator[14]
- iHeartRadio[13][24]
- Imgur[25]
- Indiegogo[13]
- Mashable[26]
- National Hockey League[14]
- Netflix[14][21]
- *The New York Times*[12][17]
- Overstock.com[14]
- PayPal[19]
- Pinterest[17][19]
- Pixlr[14]
- PlayStation Network[17]
- Qualtrics[13]
- Quora[14]
- Reddit[13][17][19]
- Roblox[27]
- Ruby Lane[14]
- *RuneScape*[13]
- SaneBox[23]
- Seamless[25]
- *Second Life*[28]
- Shopify[12]
- Slack[25]
- SoundCloud[12][19]
- Squarespace[14]
- Spotify[13][17][19]
- Starbucks[13][24]
- Storify[16]
- Swedish Civil Contingencies Agency[29]
- Swedish Government[29]
- Tumblr[13][17]
- Twilio[13][14]
- Twitter[12][13][17][19]
- Verizon Communications[17]
- Visa[30]
- Vox Media[31]
- Walgreens[14]
- *The Wall Street Journal*[21]
- Wikia[13]
- *Wired*[16]
- Wix.com[32]
- WWE Network[33]
- Xbox Live[34]
- Yammer[25]
- Yelp[14]
- Zillow[14]

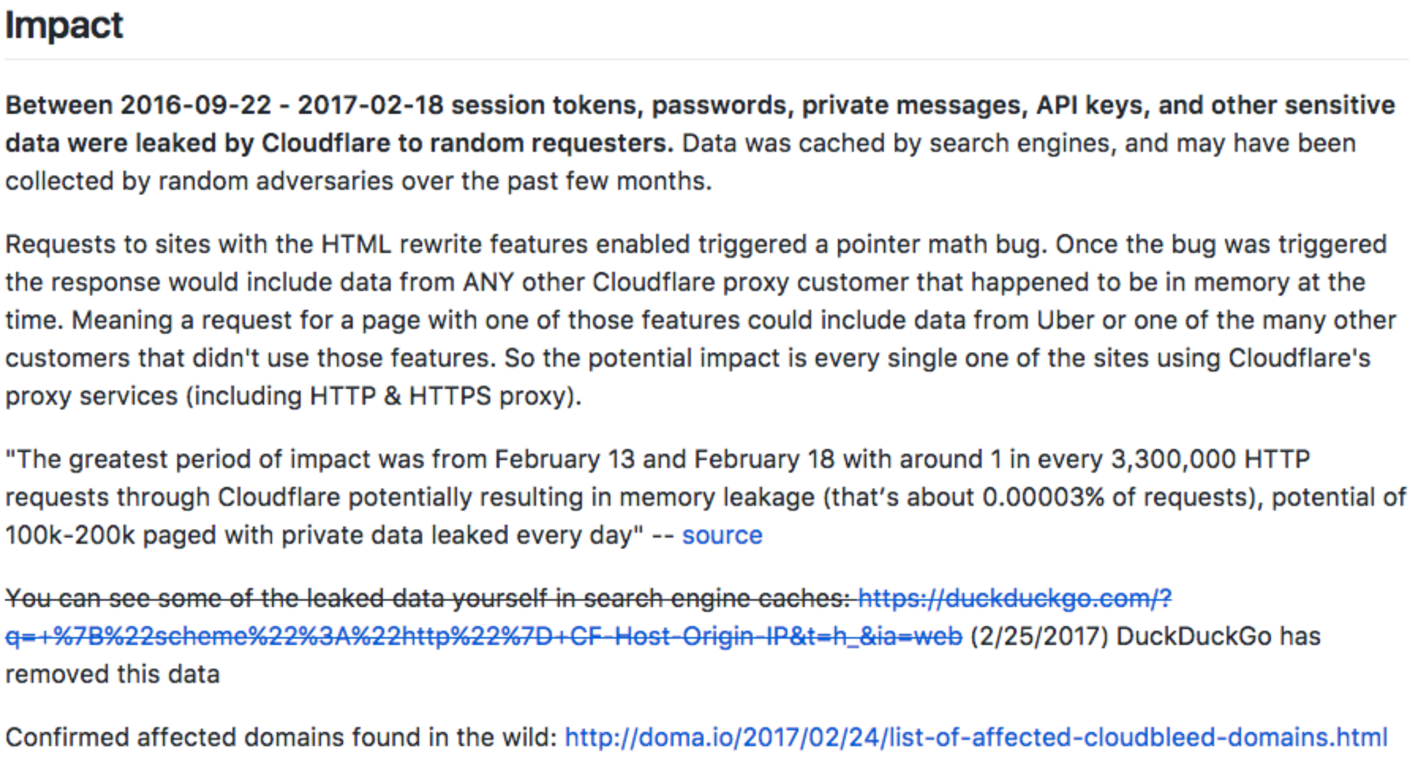
Recent Incidents

- **SHA-1 is broken**
  - It is now practically possible to craft two colliding PDF files and obtain a SHA-1 digital signature on the first PDF file which can also be abused as a valid signature on the second PDF file.



Recent Incidents

- **Cloudbleed**
  - https://github.com/pirate/sites-using-cloudflare



Impact

Between 2016-09-22 - 2017-02-18 session tokens, passwords, private messages, API keys, and other sensitive data were leaked by Cloudflare to random requesters. Data was cached by search engines, and may have been collected by random adversaries over the past few months.

Requests to sites with the HTML rewrite features enabled triggered a pointer math bug. Once the bug was triggered the response would include data from ANY other Cloudflare proxy customer that happened to be in memory at the time. Meaning a request for a page with one of those features could include data from Uber or one of the many other customers that didn't use those features. So the potential impact is every single one of the sites using Cloudflare's proxy services (including HTTP & HTTPS proxy).

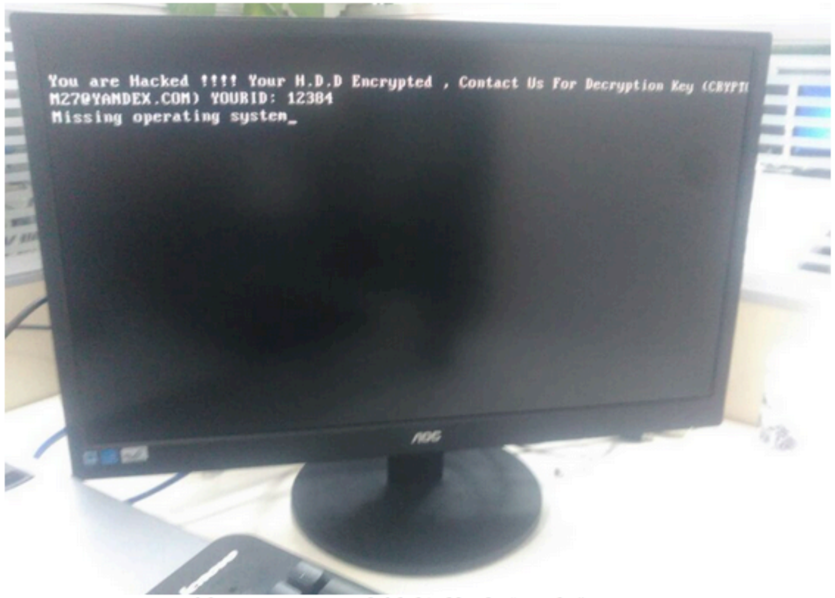
"The greatest period of impact was from February 13 and February 18 with around 1 in every 3,300,000 HTTP requests through Cloudflare potentially resulting in memory leakage (that's about 0.00003% of requests), potential of 100k-200k paged with private data leaked every day" -- source

~~You can see some of the leaked data yourself in search engine caches: https://duckduckgo.com/?q=+%7B%22scheme%22%3A%22http%22%7D+CF-Host-Origin-IP&t=h_&ia=web~~ (2/25/2017) DuckDuckGo has removed this data

Confirmed affected domains found in the wild: http://doma.io/2017/02/24/list-of-affected-cloudbleed-domains.html

Recent Incidents

- **San Francisco Rail System Hacker Hacked**
  - Ransomware attack on San Francisco public transit gives everyone a free ride

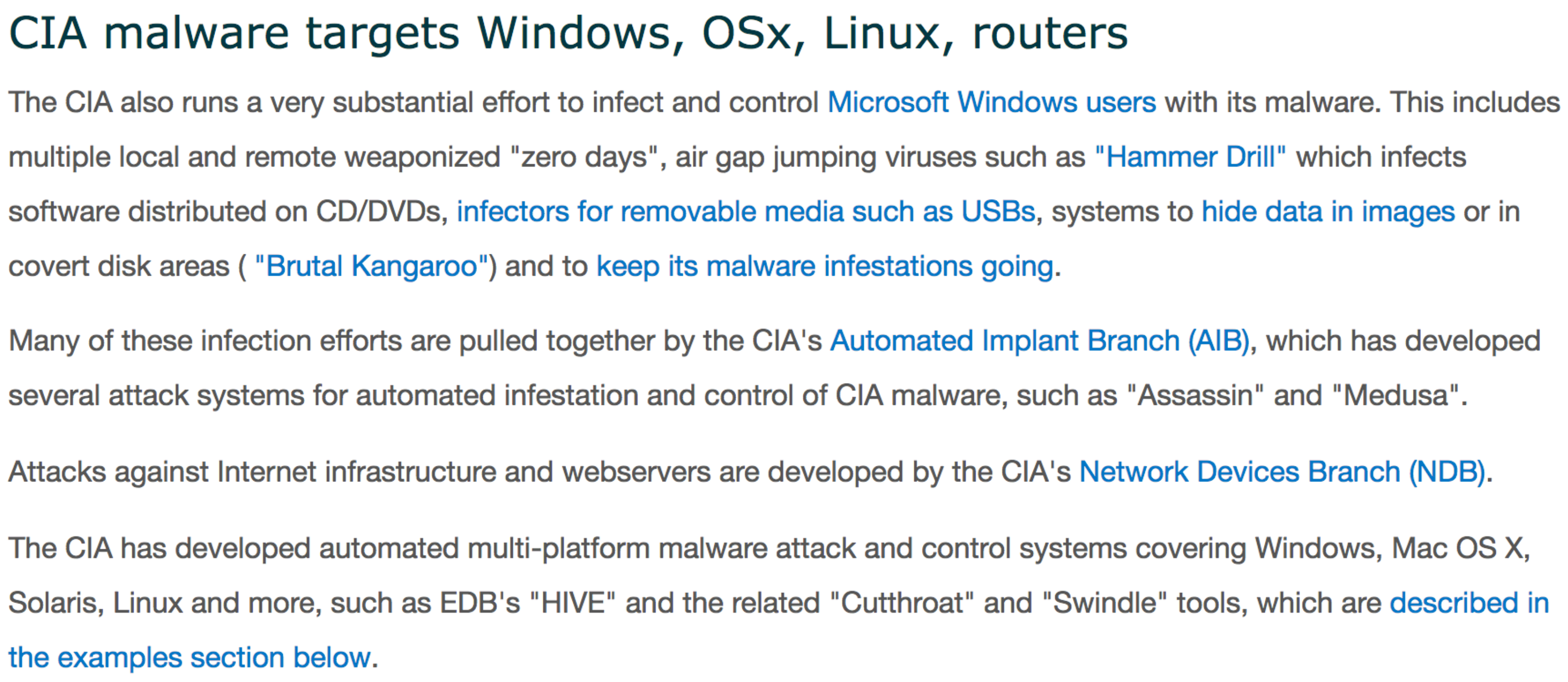


```
You are Hacked !!!! Your H.D.D Encrypted , Contact Us For Decryption Key (CRYPTI
M27@YANDEX.COM) YOURID: 12384
Missing operating systen_
```

A copy of the ransom message left behind by the "Mamba" ransomware.

Recent Incidents

- **Vault 7: CIA Hacking Tools Revealed**
  - https://wikileaks.org/ciav7p1/index.html



CIA malware targets Windows, OSx, Linux, routers

The CIA also runs a very substantial effort to infect and control Microsoft Windows users with its malware. This includes multiple local and remote weaponized "zero days", air gap jumping viruses such as "Hammer Drill" which infects software distributed on CD/DVDs, infectors for removable media such as USBs, systems to hide data in images or in covert disk areas ("Brutal Kangaroo") and to keep its malware infestations going.

Many of these infection efforts are pulled together by the CIA's Automated Implant Branch (AIB), which has developed several attack systems for automated infestation and control of CIA malware, such as "Assassin" and "Medusa".

Attacks against Internet infrastructure and webservers are developed by the CIA's Network Devices Branch (NDB).

The CIA has developed automated multi-platform malware attack and control systems covering Windows, Mac OS X, Solaris, Linux and more, such as EDB's "HIVE" and the related "Cutthroat" and "Swindle" tools, which are described in the examples section below.

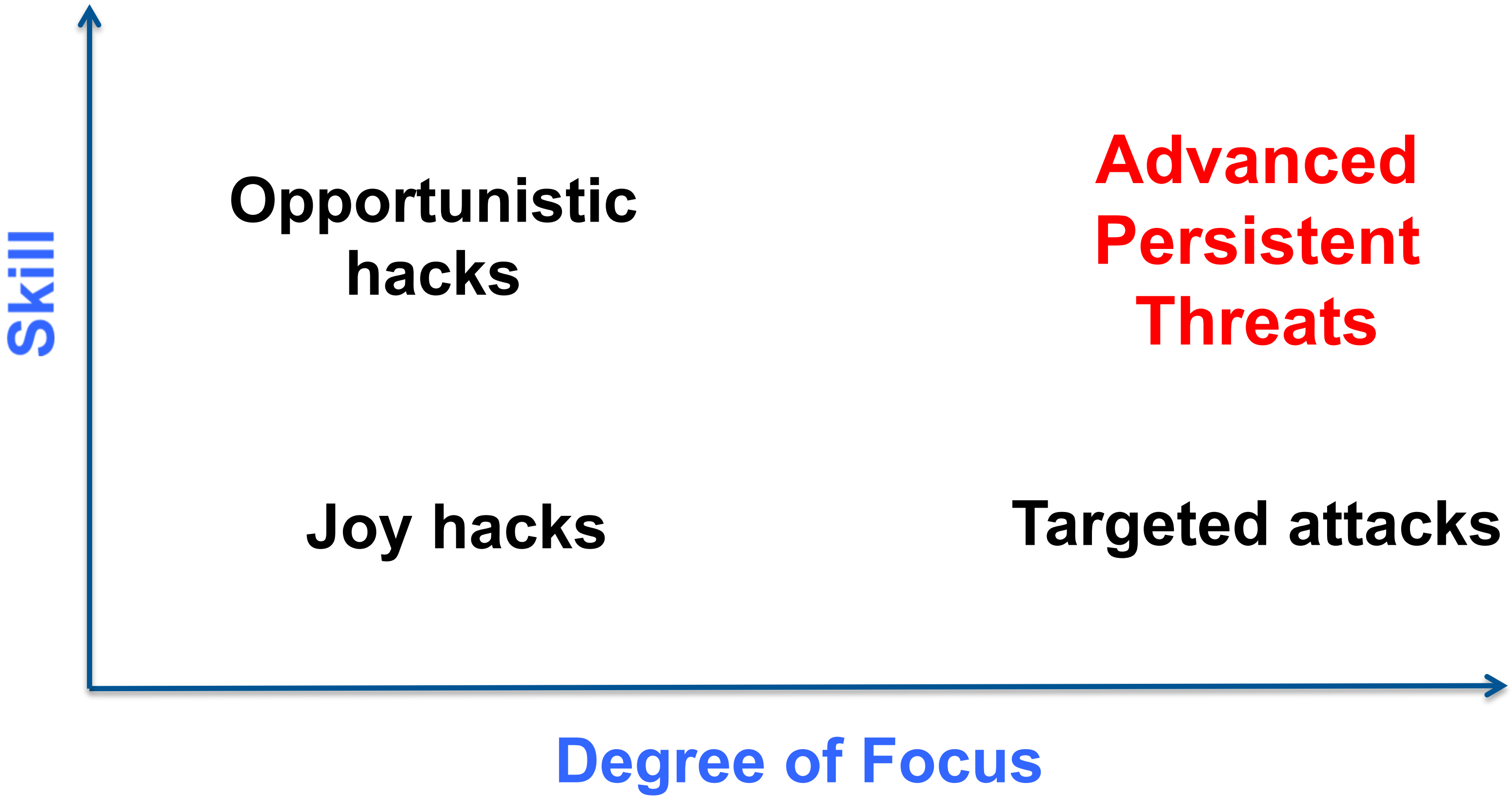
Overview

- Assets – What are we protecting?
- Attackers – From whom?
- Attacks – Common Attacks
- Defenses - Defenses

Who Are the Enemies?

- Script kiddies: Little real ability, but can cause damage if you're careless
- Money makers: Hack into machines; turn them into spam engines; etc.
- Government intelligence agencies, AKA Nation State Adversaries

The Threat Matrix



Opportunistic hacks

Advanced Persistent Threats

Joy hacks

Targeted attacks

Skill

Degree of Focus

Joy Hacks

- Hacks done for fun, with little skill
- Some chance for damage, especially on unpatched machines
- Targets are random; no particular risk to your data (at least if it's backed up)Ordinary care will suffice
- Most hackers start this way

Opportunistic Hacks

- Most phishers, virus writers, etc.
- Often quite skilled, but don’t care much whom they hit
- May have some “0-days” attacks
- The effects are random but can be serious
- Consequences: bank account theft, machines turned into bots, etc.

Targeted Attacks

- Attackers want you
- Sometimes, you have something they want; other times, it's someone with a grudge
- Background research—learn a lot about the target
- May do physical reconnaissance
- Watch for things like "spear-phishing" or other carefully-targeted attacks

Advanced Persistent Threats (APT)

- Very skillful attackers who are aiming at particular targets
- Sometimes—though not always—working for a nation-state
- Very, very hard to defend against them
- May use non-cyber means, including burglary, bribery, and blackmail
- Note: many lesser attacks blamed on APTs

Are You Targeted?

- If you’re big, someone is probably targeting you, especially if you’re unpopular
- If you have something someone wants - including money - you can be targeted
- Or it could be random chance

Defense Strategies

- Defense strategies depend on the class of attacker, and what you’re trying to protect
- Tactics that keep out teenagers won’t keep out an intelligence agency
- But stronger defenses are often much more expensive, and cause great inconvenience

Joy Hacks

- By definition, joy hackers use existing tools that target known holes
- Patches exist for most of these holes; the tools are known to A/V companies
  - The best defense is staying up to date with patches
  - Also, keep antivirus software up to date
- Ordinary enterprise-grade firewalls will also repel them

Opportunistic Hacks

- Sophisticated techniques used
  - Possibly even some 0-days
- You need multiple layers of defense
  - Up-to-date patches and anti-virus
  - Multiple firewalls
  - Intrusion detection
  - Lots of attention to log files
- Goal: contain the attack

Targeted Attacks

- Targeted attacks exploit knowledge; try to block or detect the reconnaissance
  - Security procedures matters a lot
  - How do you respond to phone callers?
  - What do people do with unexpected attachments?
  - USBs in the parking lot
- Hardest case: disgruntled employee or ex-employee

Advanced Persistent Threats (APT)

- Very, very hard problem!
- Use all of the previous defenses
- There are no sure answers—even air gaps aren't sufficient (see Stuxnet)
- Pay special attention to procedures
- Investigate all oddities

Varying Defenses

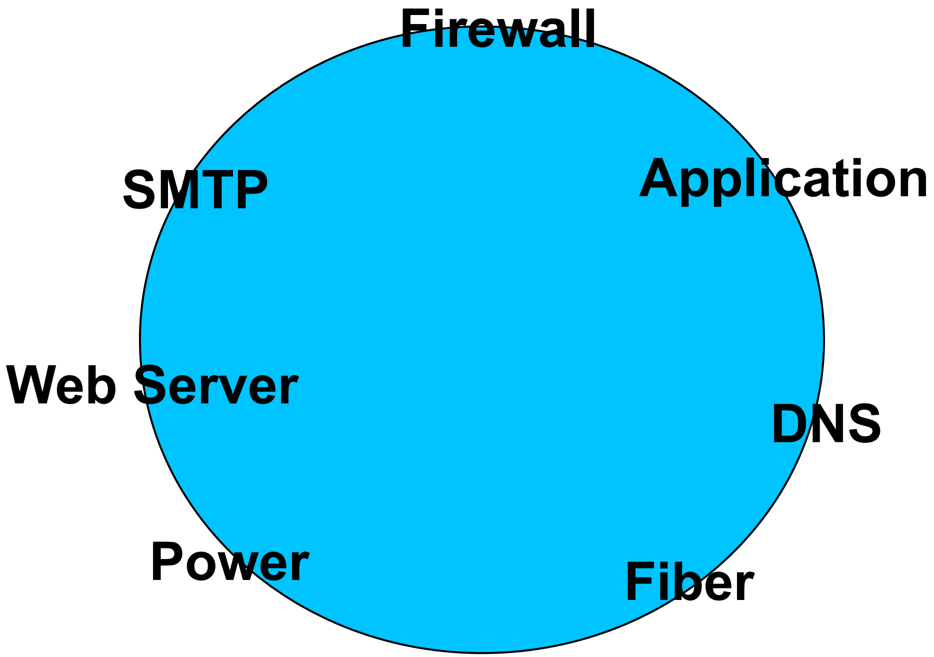
- Don’t use the same defenses for everything
- Layer them; protect valuable systems more carefully
- Maybe you can’t afford to encrypt everything
  - but you probably can encrypt all communications among and to/from your high-value machines

Uneven Playing Field

- The defender has to think about the entire perimeter, all the weakness
- The attacker has to find only one weakness
- This is not good news for defenders

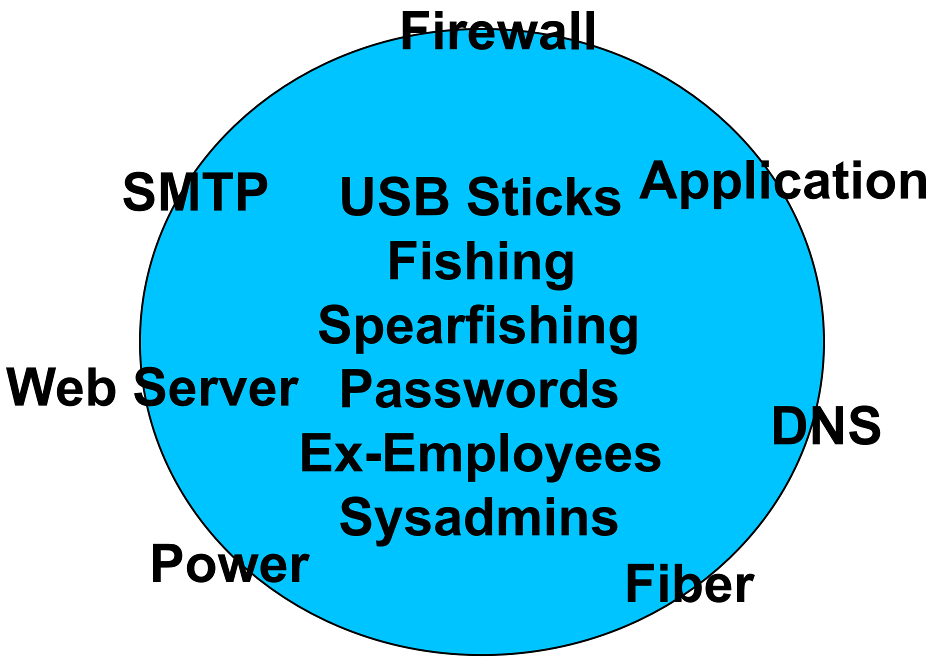
Attack Surface

Entire Perimeter you have to Defend



Attack Surface

But it is not just the perimeter!



Firewall

SMTP

USB Sticks

Application

Fishing

Spearfishing

Web Server

Passwords

DNS

Ex-Employees

Sysadmins

Power

Fiber

Layers of Protection

- Firewalls (though there are laptops on the inside)
- Intrusion Detection Systems
- Logging Systems and Analysis
- Protecting the Firewalls, IDSs, and Logging Systems

- **And what do you have?**

Why Security?

- The Internet was initially designed for connectivity
  - Trust is assumed, no security
  - Security protocols added on top of the TCP/IP
- Fundamental aspects of information must be protected
  - Confidential data
  - Employee information
  - Business models
  - Protect identity and resources
- The Internet has become fundamental to our daily activities (business, work, and personal)

Internet Evolution

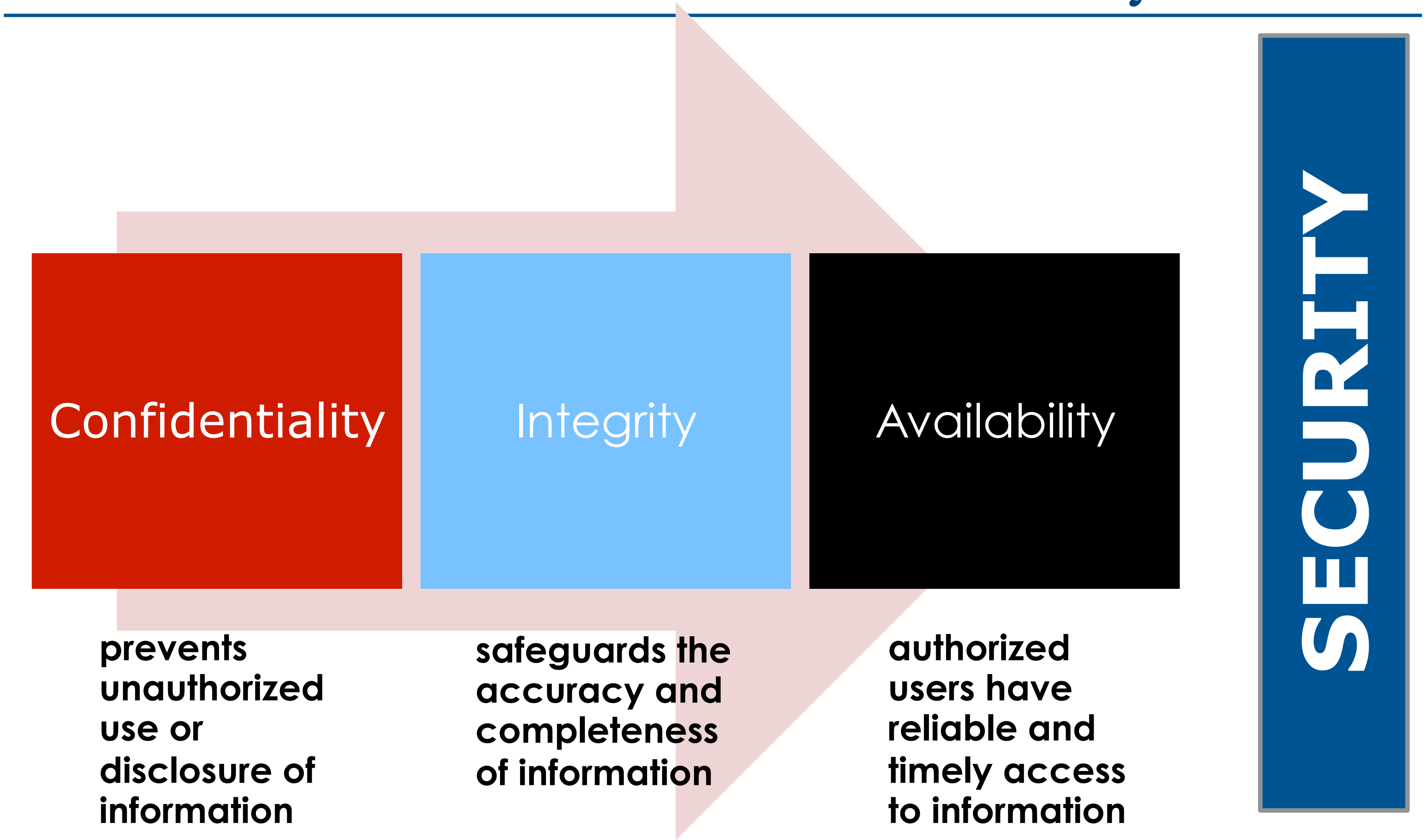
LAN connectivity

Application-specific
More online content

Application/data
hosted in the “cloud”

Different ways to handle security as the Internet evolves

Goals of Information Security



prevents unauthorized use or disclosure of information

safeguards the accuracy and completeness of information

authorized users have reliable and timely access to information

Access Control

- The ability to permit or deny the use of an object by a subject.

- It provides 3 essential services:
  - Authentication (identification of a user)
  - Authorisation (who is allowed to use a service)
  - Accountability (what did a user do)

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)

Authentication - 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

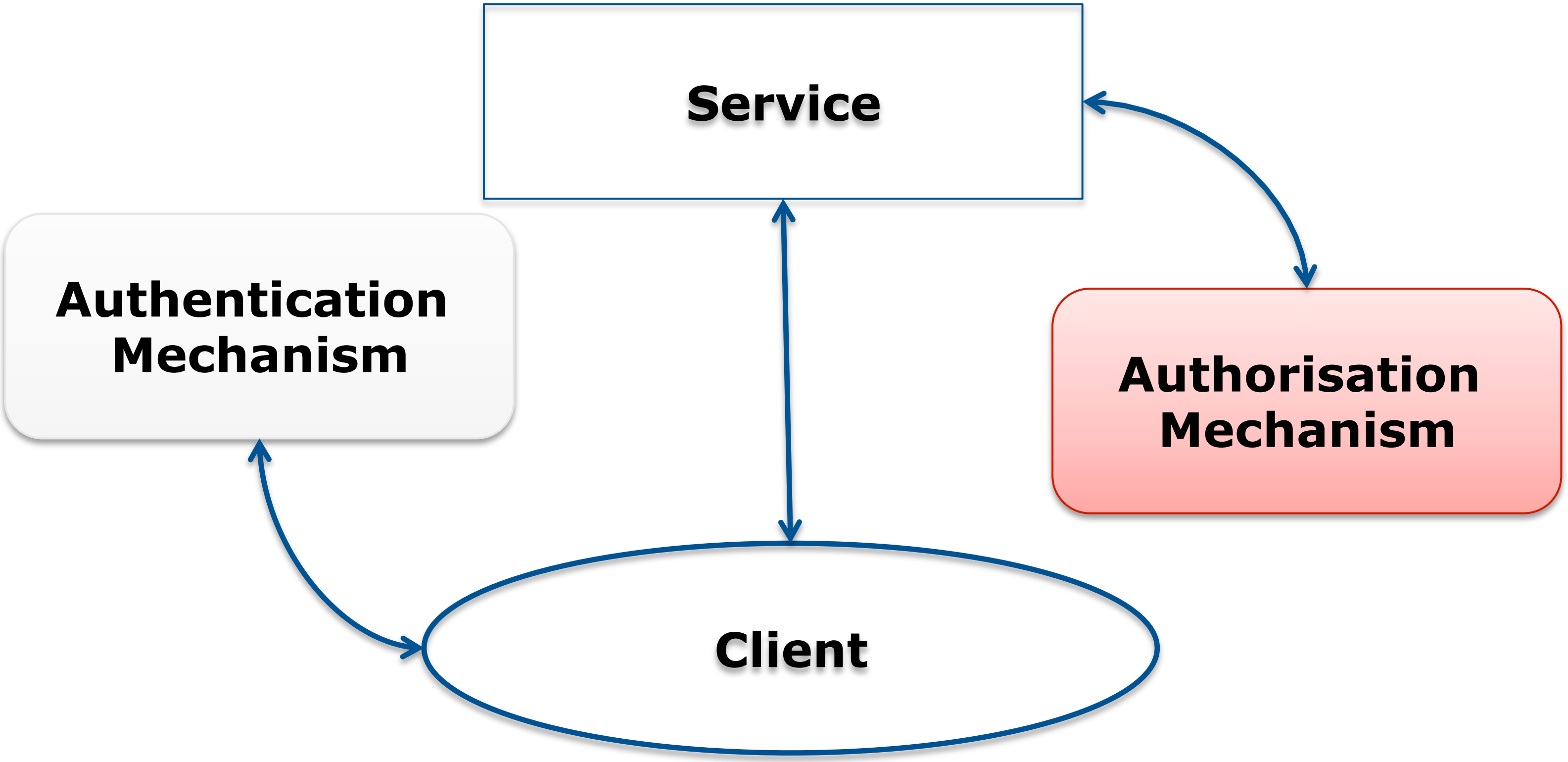
Two-factor Authentication

- 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

Authorisation

- 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. Authorisation



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

Authorisation Concepts

- Authorisation Creep
  - When users may possess unnecessarily high access privileges within an organization
- Default to Zero
  - Start with zero access and build on top of that
- Need to Know Principle
  - Least privilege; give access only to information that the user absolutely need
- Access Control Lists
  - List of users allowed to perform particular access to an object (read, write, execute, modify)

Authorisation - Single Sign On

- Property of access control where a user logs in only once and gains access to all authorized resources within a system.
- Benefits:
  - Ease of use
  - Reduces logon cycle (time spent re-entering passwords for the same identity)
- Common SSO technologies:
  - Kerberos, RADIUS
  - Smart card based
  - OTP Token
  - Shibboleth / SAML
  - OpenID
- Disadvantage: Single point of attack

Authorisation – Types of Access Control

- Centralized Access Control
  - Radius
  - TACACS+
  - Diameter
- Decentralized Access Control
  - Control of access by people who are closer to the resources
  - No method for consistent control

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

Risk, Threats, and Vulnerability

- Threat
  - Any circumstance or event with the potential to cause harm to a networked system
- 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

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

Risk = Threat * Vulnerability * Impact

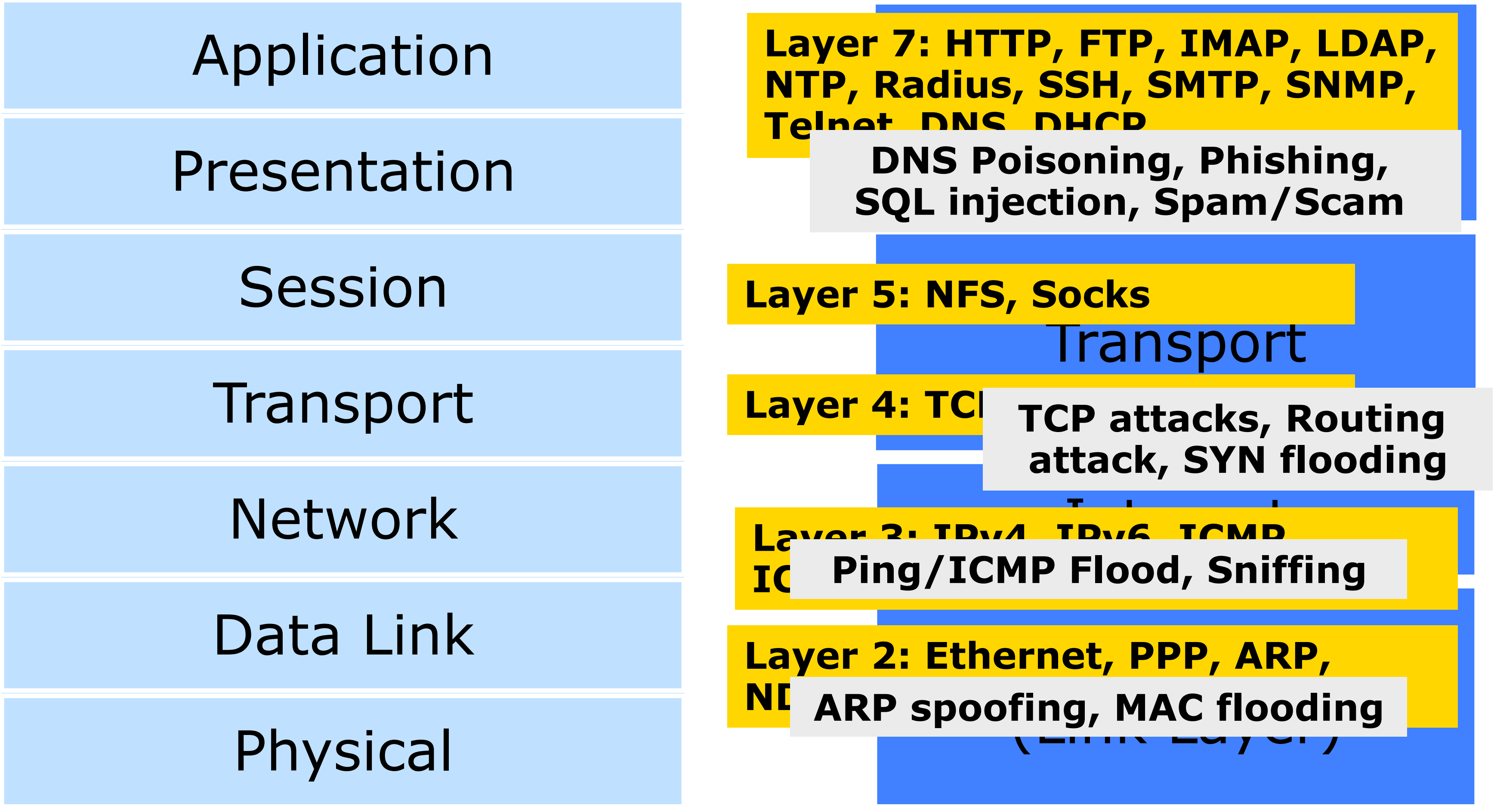
Target

- Many sorts of targets:
  - Network infrastructure
  - Network services
  - Application services
  - User machines
- What’s at risk?

What Are You Protecting?

- Identify Critical Assets
  - Hardware, software, data, people, documentation
- Place a Value on the Asset
  - Intangible asset – importance or criticality
  - Tangible asset – replacement value, training costs and/or immediate impact of the loss
- Determine Likelihood of Security Breaches
  - What are threats and vulnerabilities ?

Attacks on Different Layers



Application

Presentation

Session

Transport

Network

Data Link

Physical

Layer 7: HTTP, FTP, IMAP, LDAP, NTP, Radius, SSH, SMTP, SNMP, Telnet, DNS, DHCP

DNS Poisoning, Phishing, SQL injection, Spam/Scam

Layer 5: NFS, Socks

Transport

Layer 4: TCI

TCP attacks, Routing attack, SYN flooding

Layer 3: IPv4, IPv6, ICMP

IC

Ping/ICMP Flood, Sniffing

Layer 2: Ethernet, PPP, ARP,

ND

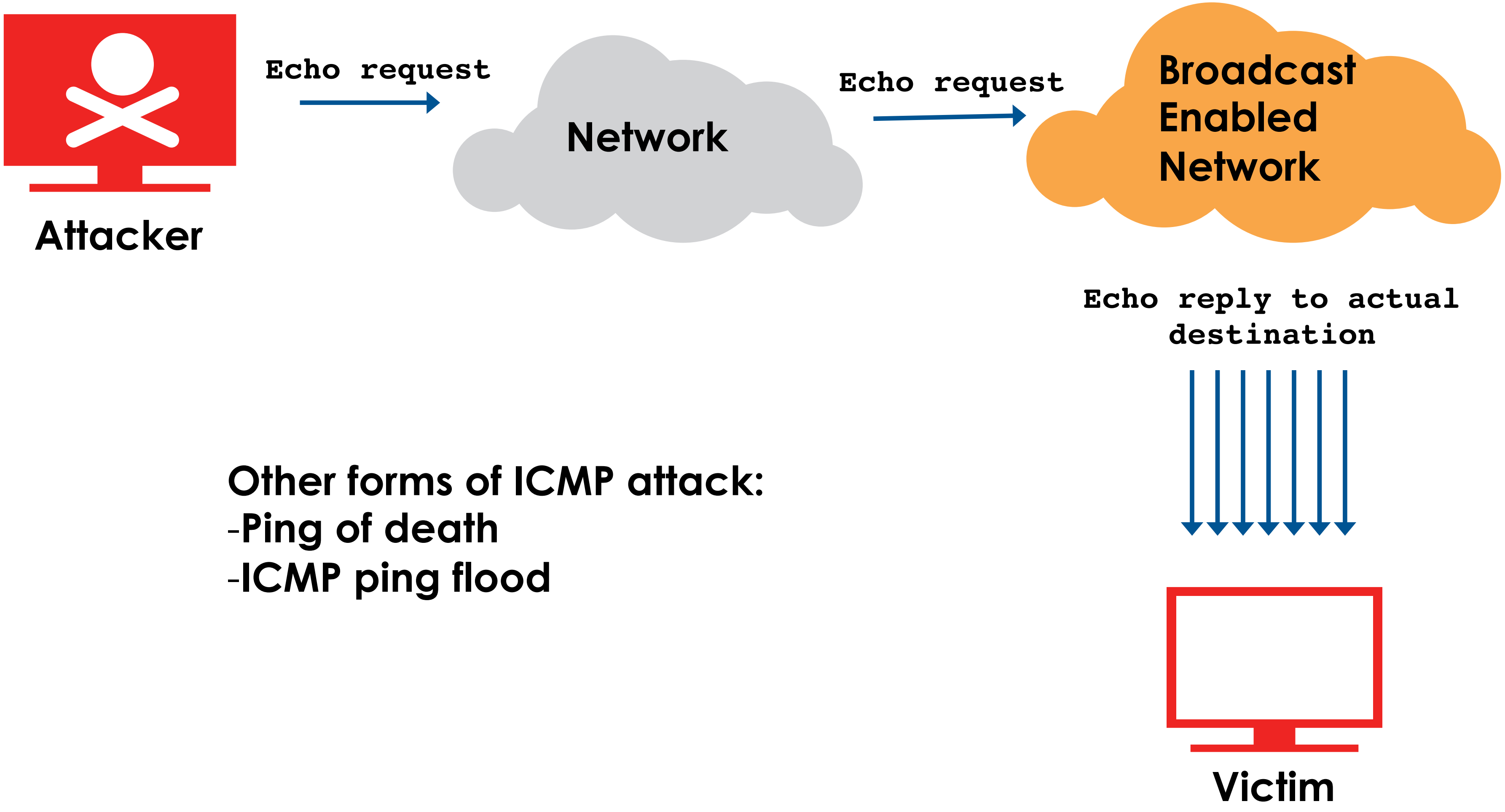
ARP spoofing, MAC flooding

OSI Reference Model **TCP/IP Model**

Layer 3 Attacks

- ICMP Ping Flood
- ICMP Smurf
- Ping of death

Ping Flood



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

Routing Attacks

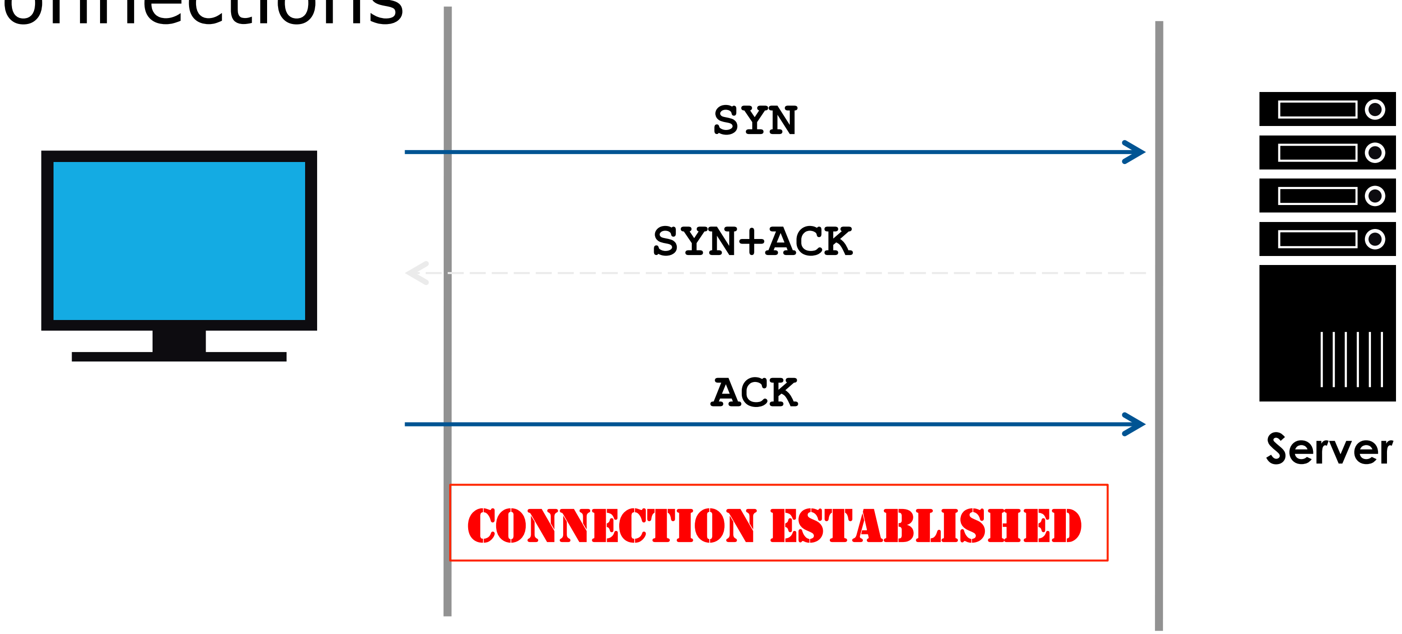
- Attempt to poison the routing information
- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP attacks
  -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

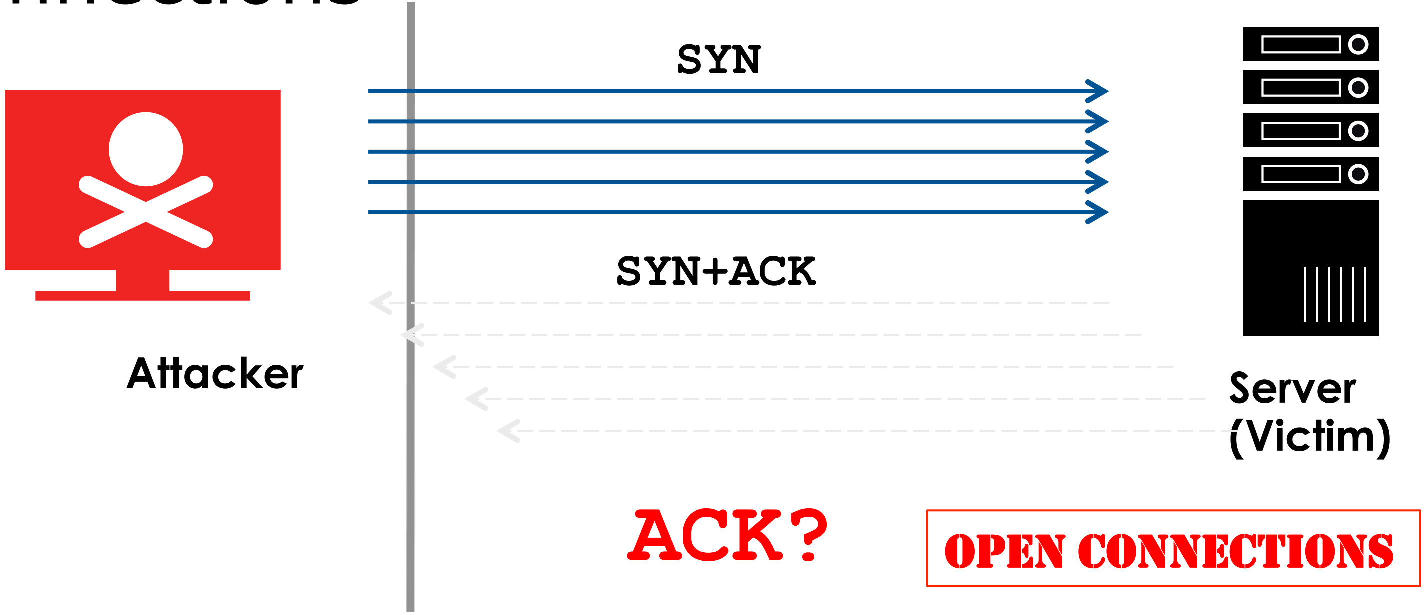
TCP Attacks

- 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

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

Layer 7 DDoS Attack

- Traditional DoS attacks focus on Layer 3 and Layer 4
- In Layer 7, a DoS attack is targeted towards the applications disguised as legitimate packets
- The aim is to exhaust application resources (bandwidth, ports, protocol weakness) rendering it unusable
- Includes:
  - HTTP GET
  - HTTP POST
  - Slowloris
  - LOIC / HOIC
  - RUDY (R-U-Dead Yet)

Layer 7 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

Amplification Attacks

- Exploiting UDP protocol to return large amplified amounts of traffic / data
- Small request, large reply
- Examples:
  - DNS
  - NTP
  - SMTP
  - SSDP

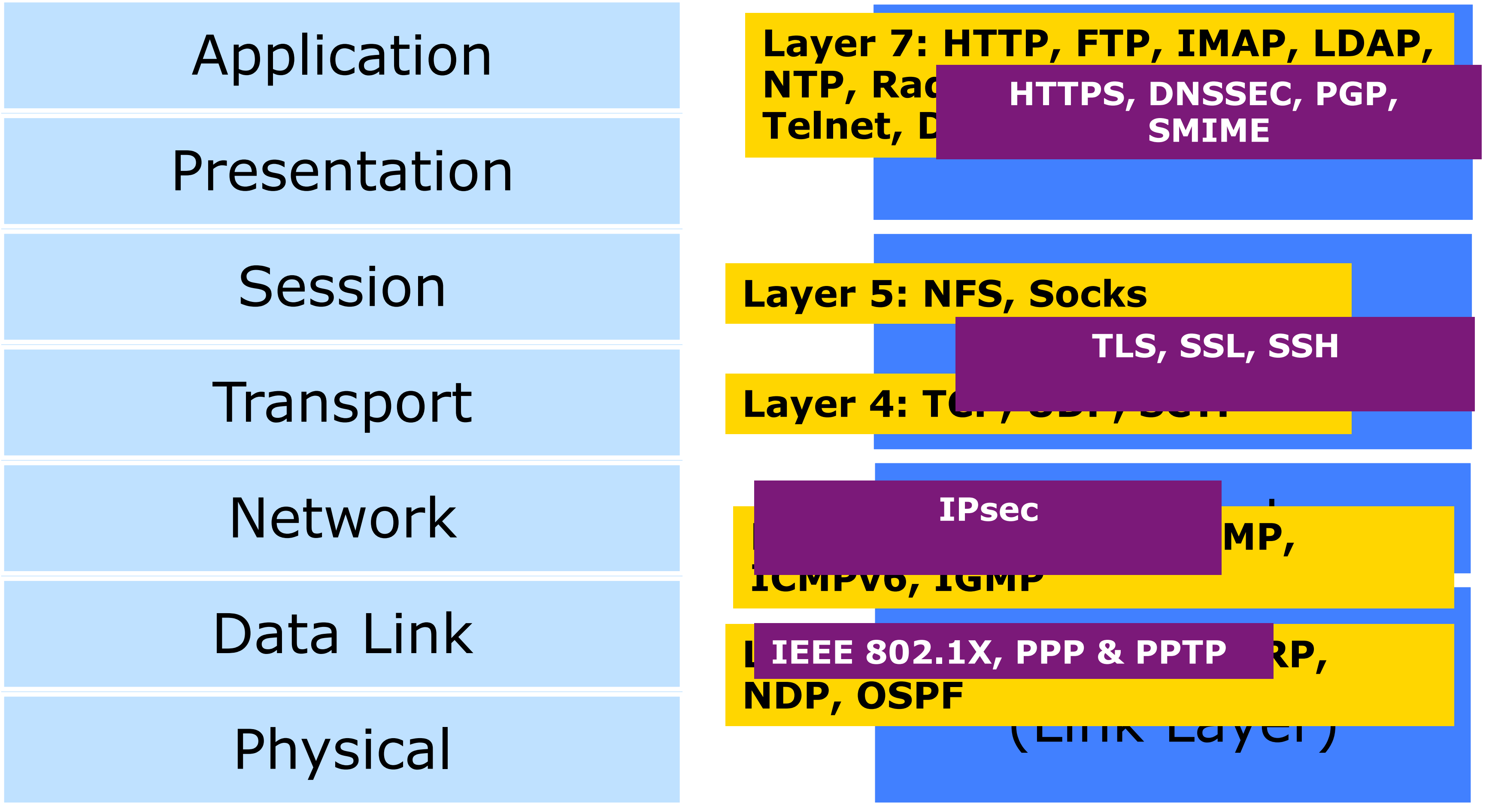
DNS Amplification Attack

- 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

NTP Amplification

- Network Time Protocol (NTP)
- Port 123/UDP
- Exploits NTP versions older than v4.2.7
  - monlist
- Several incidents in 2014

Attacks on Different Layers



Application

Presentation

Session

Transport

Network

Data Link

Physical

Layer 7: HTTP, FTP, IMAP, LDAP, NTP, Rad Telnet, D

HTTPS, DNSSEC, PGP, SMIME

Layer 5: NFS, Socks

TLS, SSL, SSH

Layer 4: TC

IPsec

MP, ICMPv6, IGMP

IEEE 802.1X, PPP & PPTP

L RP, NDP, OSPF

(Link Layer)

OSI Reference Model

TCP/IP Model

Questions

Internet Security Introduction

ITU/APNIC/MICT IPv6 Security Workshop

8th – 12th May 2017

Bangkok