Network Attack and Defense

Based on Ross Andresson's "Security Engineering", Chapter 21

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."
- Gene Spafford

Lecturer : Roee Wodislawski

Seminar's Instructor: Professor Orr Dunkelman

University Of Haifa, Spring 2015

Content

- Network Protocols
- Malware
- Defensive Tools
- Network Topology
- Statistics

OSI Model

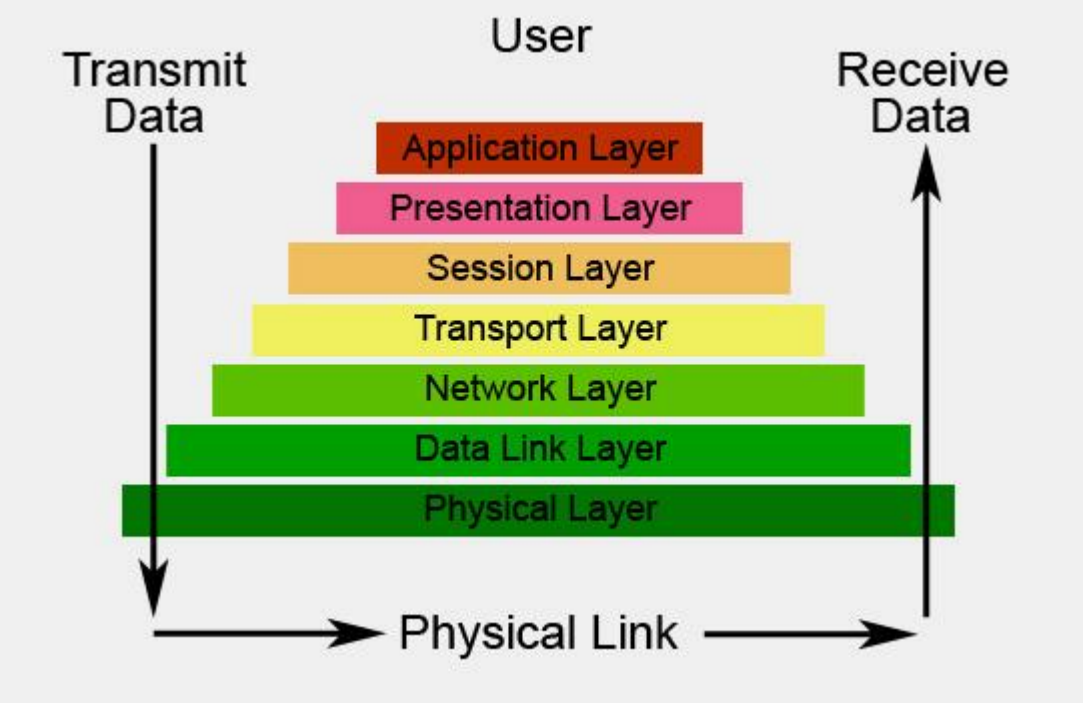


Image Source : http://www.windowsnetworking.com/

Network Protocols

- The Internet Protocol (IP)
- Transmission Control Protocol (TCP)
- Address Resolution Protocol (ARP)
- Dynamic Host Configuration Protocol (DHCP)
- The Domain Name System (DNS)
- Border Gateway Protocol (BGP)

Attacks on Local Networks

- **Packet sniffer**

  Capture and analyze network traffic in order to harvest sensitive information.

  Solution : Kerberos/SSH

- **Masquerade**

  Pretend to be other user's machine in the network, where the user has already logged on.

Images Sources : http://thumbs.dreamstime.com/ , http://blogs.lawyers.com/

Attacks on Local Networks

- **Address hijacking (ARP Spoofing)**

  Associate the attacker's MAC address with the IP address of another host by sending spoofed ARP replies.

  Solution : Static ARP entries and detection software.

- **Rogue access point**

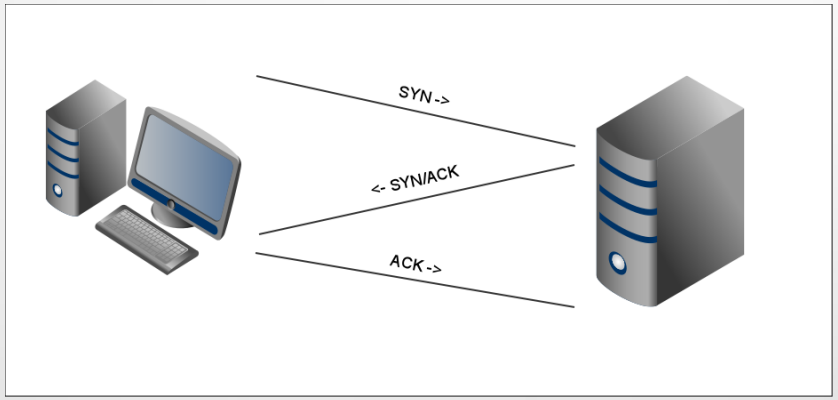
  - Maliciously deployed wireless access point.
  - Devices that employees have installed for their own convenience in defiance of corporate policy.

Image Source : http://www.bologna-airport.it/

Attacks Using Internet Protocols

- **SYN Flooding**

  The attacking device sends a series of SYN requests (without acknowledging any of the replies) with the goal of overwhelming the recipient.



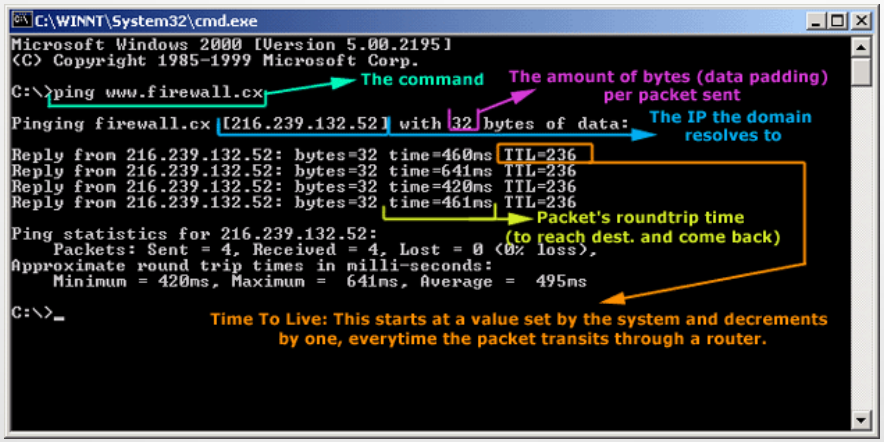
Moral : when you are designing a protocol that anyone can invoke, do not make it easy for malicious users to make honest ones consume resources.

Image Source : http://blogs.ixiacom.com/

Attacks Using Internet Protocols

- **Smurfing**

  The attacker sends a ping or an ICMP Echo Request to a broadcast address ("smurf amplifier") with the source address forged to be that of the victim.



Moral : when you are designing a network protocol, be careful to ensure that no-one who puts one packet in can get two packets out, and avoid feedback and loops.

Image Source : http://www.firewall.cx/

Attacks Using Internet Protocols

- **Distributed Denial Of Service**

  The attacker subverts a large number of machines ("botnet") over a period of time and, or on a given signal, these machines all start to bombard the target with traffic.

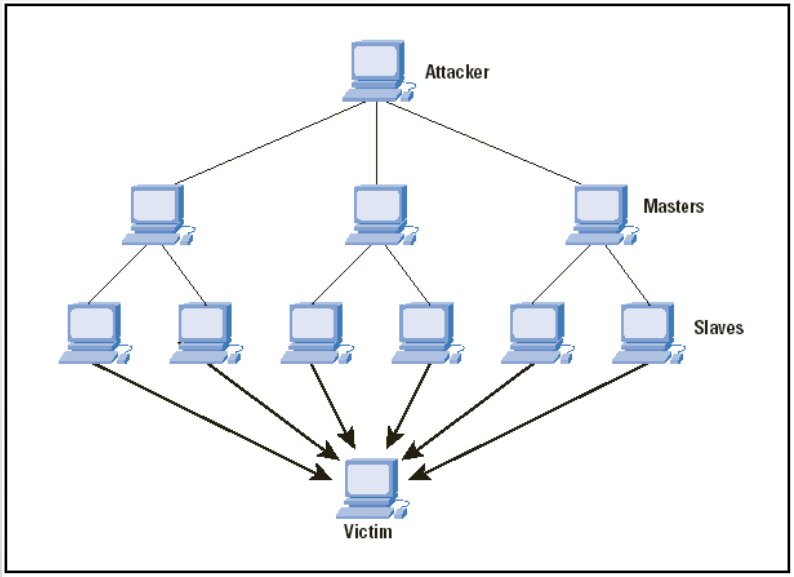


Image Source : http://www.webnethosting.net/

Attacks Using Internet Protocols

- **Spam**

  Floods of generally unwanted traffic sent out for the most part by botnets, and often with clear criminal intent.

Image Source : http://media.licdn.com/

Attacks Using Internet Protocols

- **DNS Security and Pharming**
  - Directing the user to a malicious DNS server (DNS pharming).
  - Feeding A DNS server with wrong information to drive clients to a wicked website (DNS cache poisoning).

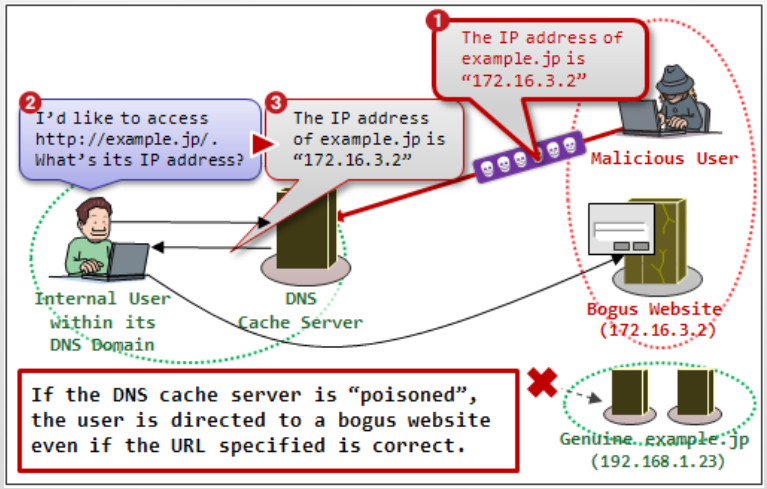


Image Source : https://www.ipa.go.jp/

Malware

- **Worms**

  Self-propagating malicious programs.

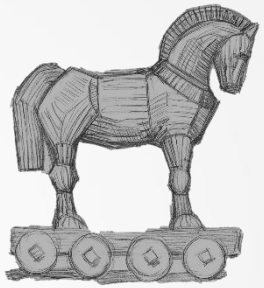
- **Viruses**

  A worm which replicates by attaching itself to other programs and data files.

  Two main components : **Replication mechanism** and **Payload**

Images Sources : http://www.vir.us.com/

Malware



- **Trojan Horses**

  Malicious program that disguise itself as a/as part of legitimate program in order to persuade victims to install them on their computers.

- **Rootkits**

  A piece of software that once installed on a machine hide the existence of itself and other certain processes or programs from standard tools of detection and enable remote control.

Images Sources : http://www.simon-hohberg.de/

Malware History

- 1960's – 1970's
  - Machines were slow and their CPU cycles were carefully rationed between different groups of users (The "worm" program).
- 1980's
  - "On Trusting Trust" (1984) - you can not trust a system you didn't build completely yourself.
  - Studies and experiments about malicious code are being made and after short time, real "live" viruses start appearing in the "wild" - alarm and consternation ('Christma' virus prank , The Internet Worm).

Malware History

- 1990's
  - Whole industry of anti-virus software writers and consultants rises.
  - Exploitation of java and macro languages.
  - The main transmission mechanism - the Internet.
- 2000's
  - Worms using various ways to persuade people to click on (The "Love Bug" Virus).
  - "Flash worms" - scanning the Internet for vulnerable machines (Code Red, Slammer).
  - Spyware and Adware.

Image Source : http://superuser.com/

Malware History

- 2000's - continue
  - A significant change in the nature of the environment.
  - Manually-controlled and limited attacks.
  - Large botnet networks (the "Storm network").
  - The "clicking" routine of users.

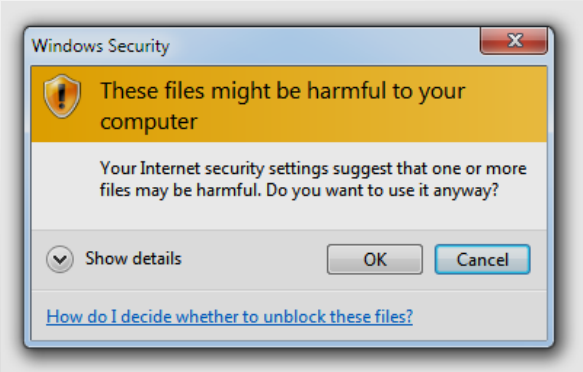
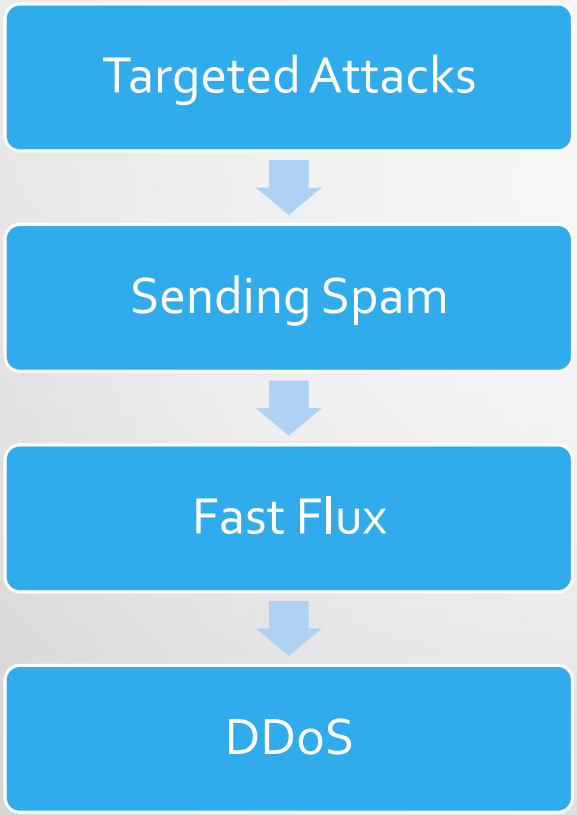


Image Source : http://motherboard-images.vice.com/

Compromised Machines Market

Value chain of compromised machine :



- People who specialize in hacking machines can sell their product to people who specialize in herding them and extracting value.
- The vendors even install up-to-date antivirus software to stop any competing botnet from taking the machine over, and provide after-sales service.
- The compromised machines are rented out to spammers, phisher-men and extortionists.

Countermeasures

- **Antivirus software**
  - Scanners - searches executable files for a sign of malicious code.
    Virus writers response - polymorphism.
  - Checksummers - keep a list of all the authorized executables on the system.
    Virus writers response - stealth.
- **Medical Lessons**
  - Epidemic threshold.
  - Using immune system models to develop strategies for malware detection.
  - Prevention versus cure.

Image Source : http://coreo.staticworld.net/

Defensive Tools

- Configuration Management
- Filtering
- Intrusion Detection
- Encryption

Configuration Management

- The importance of installing patches fast ("patch Tuesday")
- Unsafe defaults
- Reduce the attack surface
- Overnight Reinstallation
- Know your network's topology
- Training staff

Filtering

- **Packet Filtering (IP level)**
  - Preventing IP spoofing, denial-of-service, censorship mechanisms.
  - Can be defeated by overwritten fragment, fast-flux.
- **Circuit Gateways (TCP level)**
  - The functionality of virtual private network (VPN), DNS filtering.
  - Can't inspect things at the application level.
  - May often be programmed to direct certain types of traffic to specific application filters.

Image Source : http://smartecart.com/

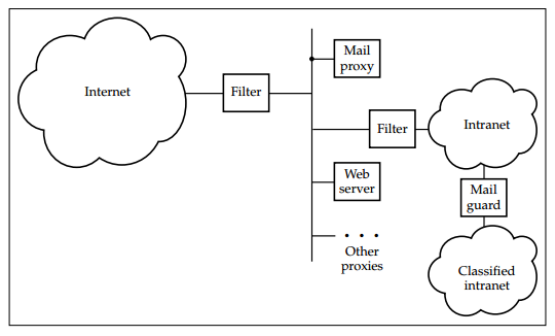
Filtering

- **Application Relays (application level)**
  - Acts as a proxy for one or more services.
  - The three-headed arms race : the firewall vendors, the spammers, and people trying to circumvent controls to get their work done.
  - Breaking Encryption.
  - Possible problems : bottleneck, the trailing behind of the firewall vendors.

Images Sources : http://www.bccc.edu/, http://stmarkfestival.com.au/, http://digitalfirm.net/, http://sobolsoft.com/

Filtering

- **Architecture**
  - Demilitarized zone (DMZ) - a screened subnet inserted as a "neutral zone" between a company's private network and the outside public network. Can contain a number of application servers or proxies to filter mail, web and other services.
  - Separating networks operating at different clearance levels.
  - Deperimiterization - it is steadily becoming harder to put all the protection at the perimeter.



Intrusion Detection

- It's often cheaper to prevent some attacks and detect the rest
- Intrusion detection systems - "boxes" that sit on your network and look for signs of an attack in progress or a compromised machine.
- Examples : Detecting mobile phone cloning/bank fraud, suspect lists at airports.

Types of Intrusion Detection

- **Using threshold** - sound an alarm when a threshold of red flags is passed.
- **Misuse Detection** - using a model of the likely behavior of an intruder (searching for a "signature").

- **Anomaly detection** - detect attacks that have not been previously recognized and cataloged.

Image Source : http://www.blueviolet networks.com/

Problems Detecting Network Attacks

- Noisy environment
- “The guards get tired”
- Large and constantly changing library of attack signatures
- Encrypted traffic
- Locally and globally intrusion detection

Encryption

- **SSH**

  Provides encrypted links between Unix and Windows hosts - log into another computer over a network, to execute commands in a remote machine.

  Each machine has a public-private keypair.

  Vulnerabilities : man in the middle attacks, each character gets sent in its own packet, keys are stored in the clear.

- **WiFi**

  Local area wireless computer networking technology which allows connecting electronic devices to a network.

  Security systems : WEP, WPA/WPA2

Image Source : http://www.jjc.edu/

Encryption

- **Bluetooth**

  Protocol used for short-range wireless communication (personal area networks).

  Vulnerabilities : PIN (brute-force), man-in-the-middle attack.

- **IPsec**

  Encryption and/or authentication at the IP layer.
  It defines a "security association" as the combination of keys, algorithms and parameters used to protect a particular packet stream.
  IKE protocol being used to set up keys and negotiate parameters.

  Two modes : transport mode and tunnel mode. The latter could be used to set up virtual private network.

Image Source : http://cdn.afterdawn.com/

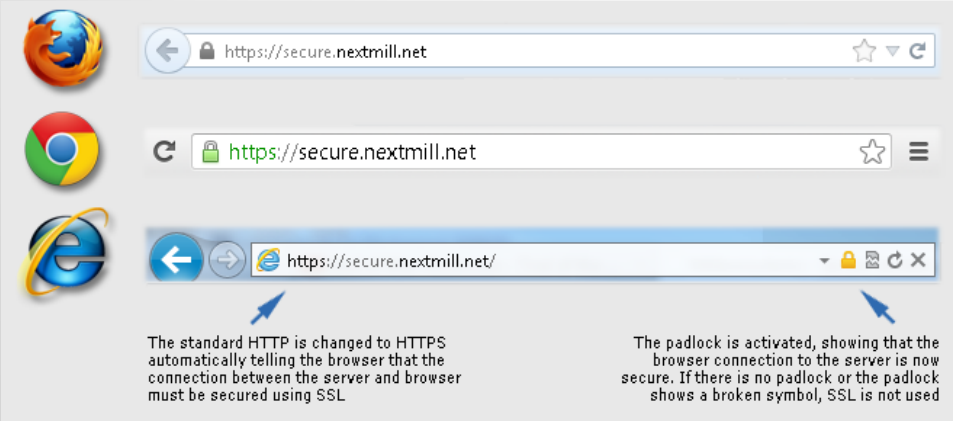
Encryption

- **TLS/SSL**

  Supports encryption and authentication in both directions, allowing http requests and responses can be protected against both eavesdropping and manipulation, using public key encryption.

  Minimizing the load on the browser first - **wrong design decision**.

  Other applications : Medical privacy, Windows Authentication, mail servers.



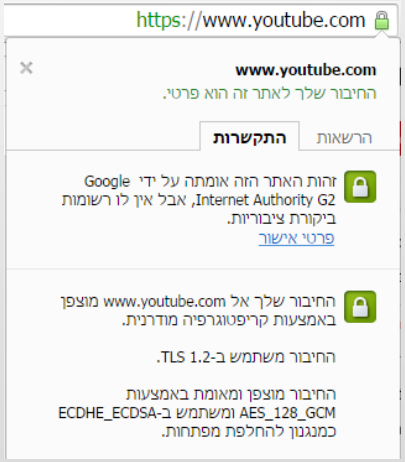
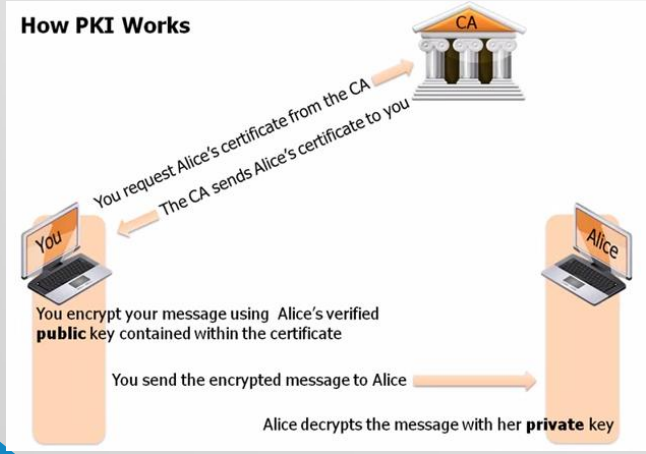
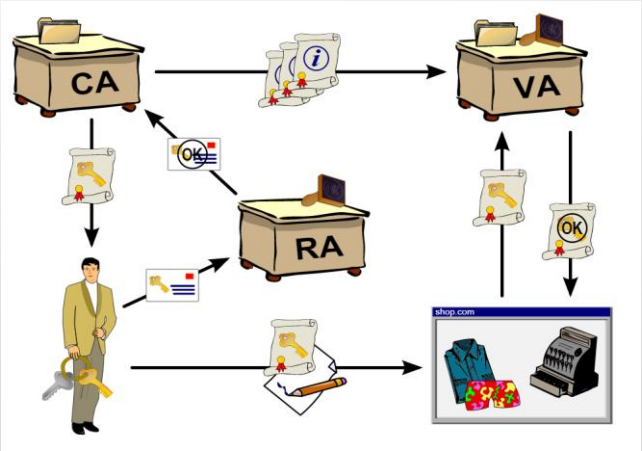


Image Source : http://www.millsysinc.com/

Encryption

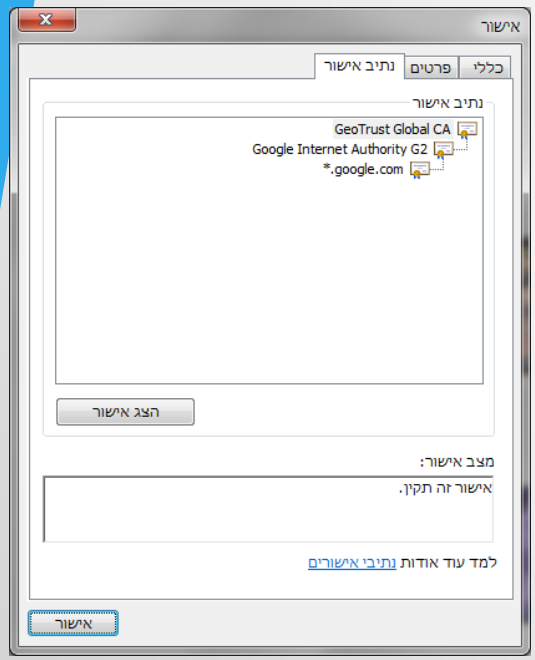
- **PKI (Public Key Infrastructure)**
  - System for the creation, storage, and distribution of digital certificates.
  - **Certificate authority (CA)** - responsible for issuing, revoking and distributing digital certificates.
  - **Registration authority (RA)** - responsible for accepting requests for digital certificates and verifies the prospective key owner's identify and sends it to the CA to issue a certificate.
  - **Validation authority (VA)** - an entity that provides services used to validate a certificate.

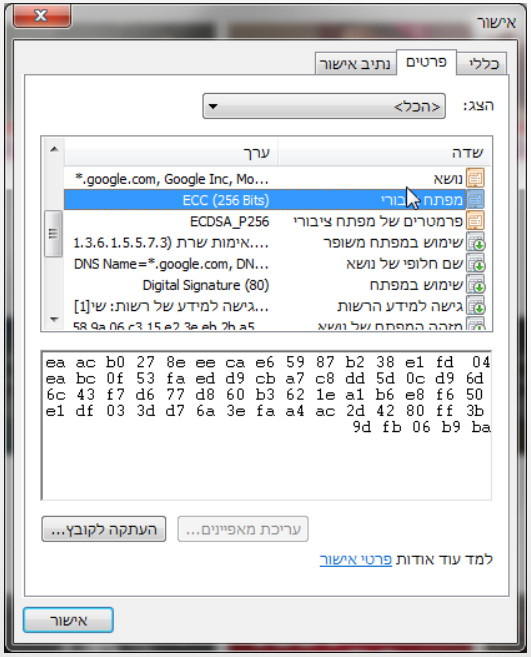


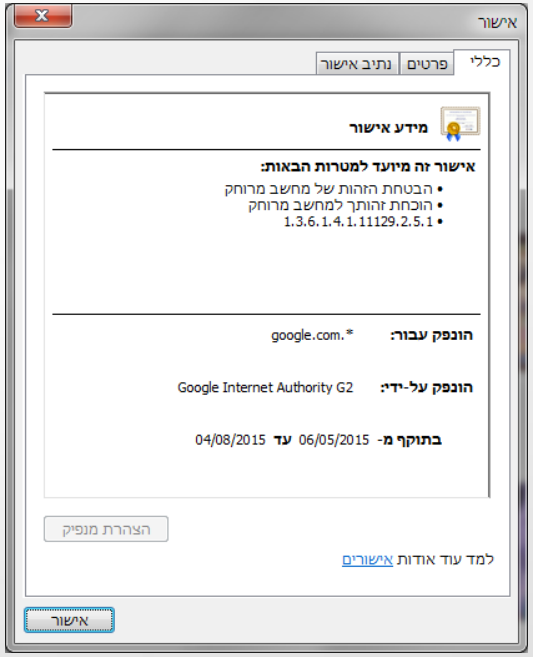


Images Sources : http://he.wikipedia.org, http://www.trainsignal.com/

Digital Certificate



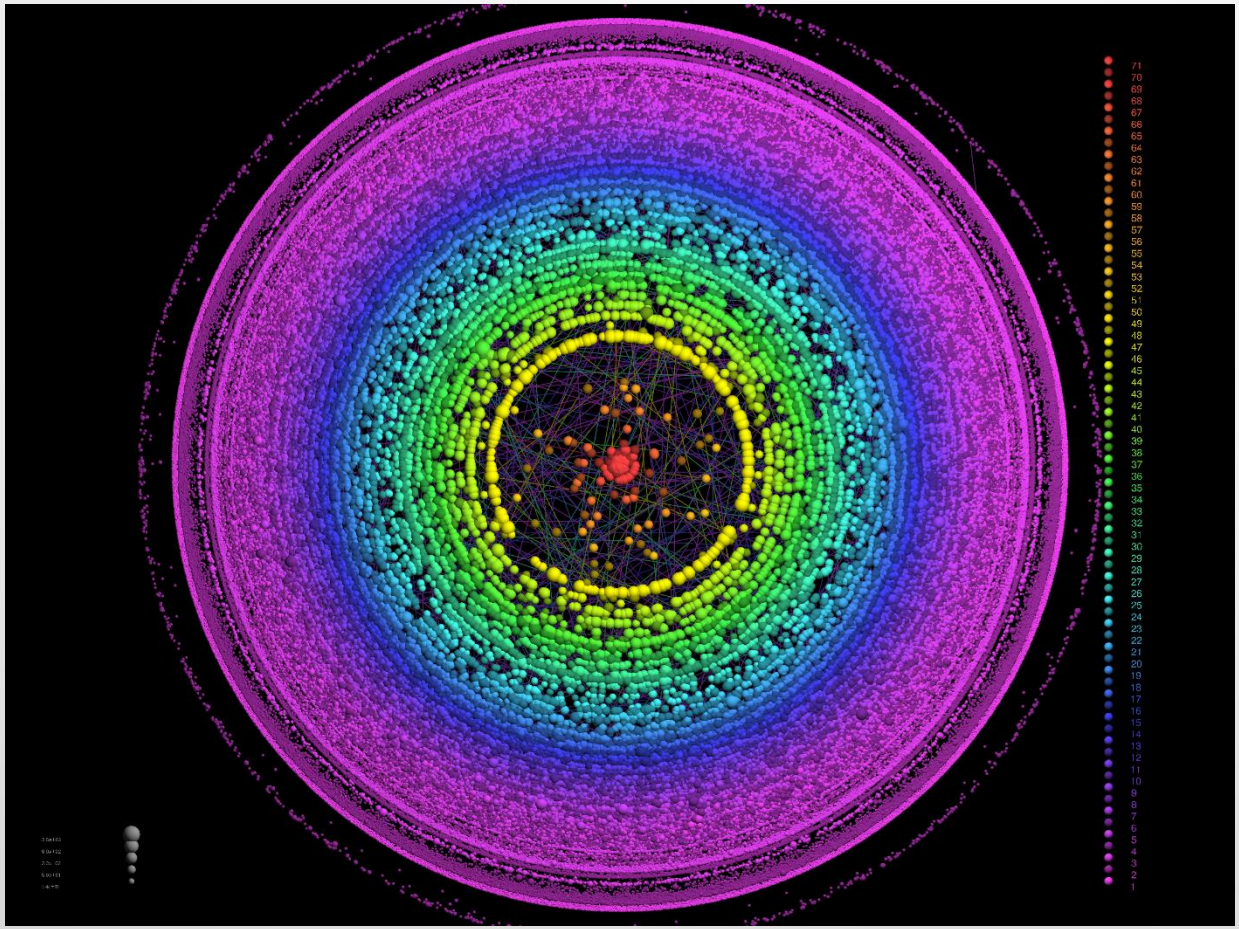




Topology

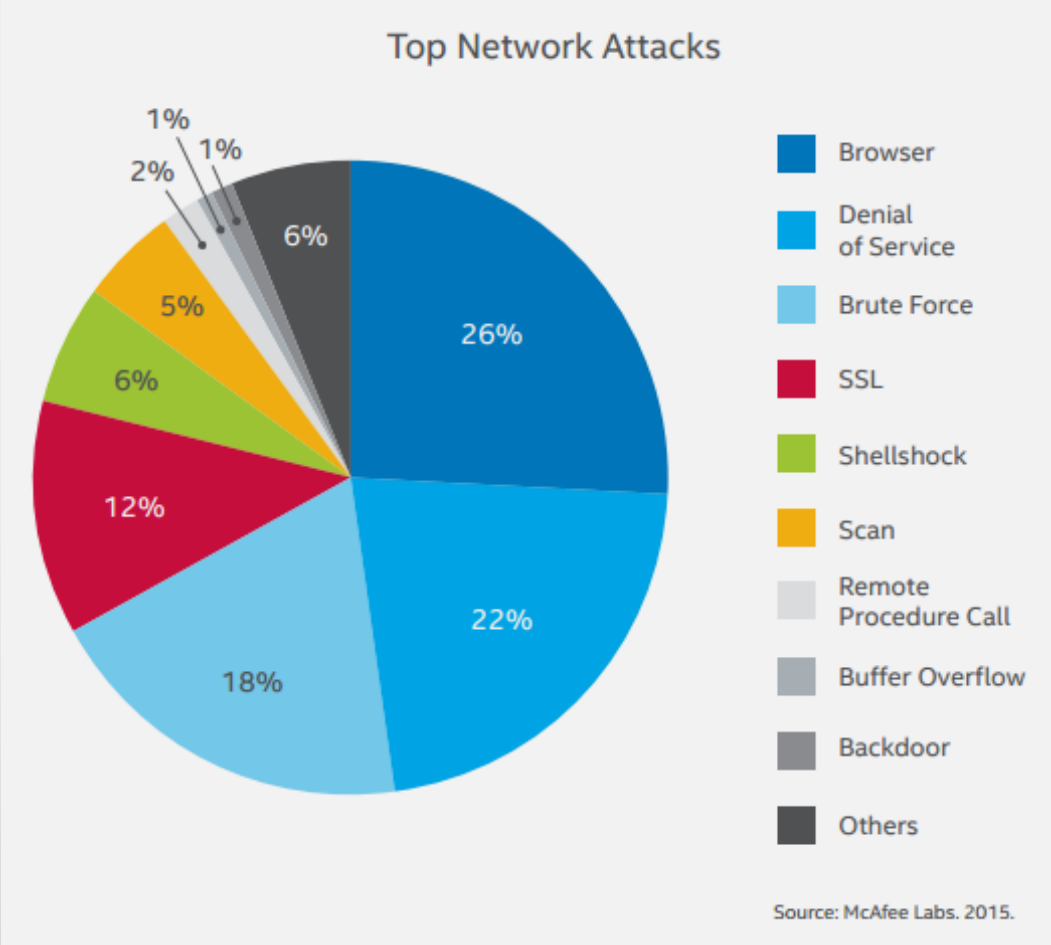
- The pattern in which its node are connected.
- Internet - classically is thought as a cloud to which all machines are attached, so in effect every machine is (potentially) in contact with every other one (fully connected graph).
- However, in many networks each node communicates with only a limited number of others.
- The topology of network is important in service denial attacks.
- Cell structure as a defense.

Internet Topology



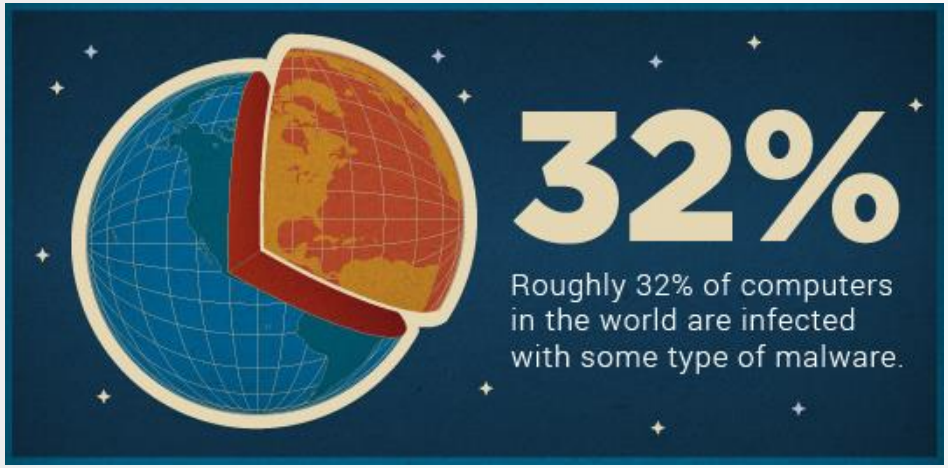
Source : http://www.netdimes.org/ipmap.png

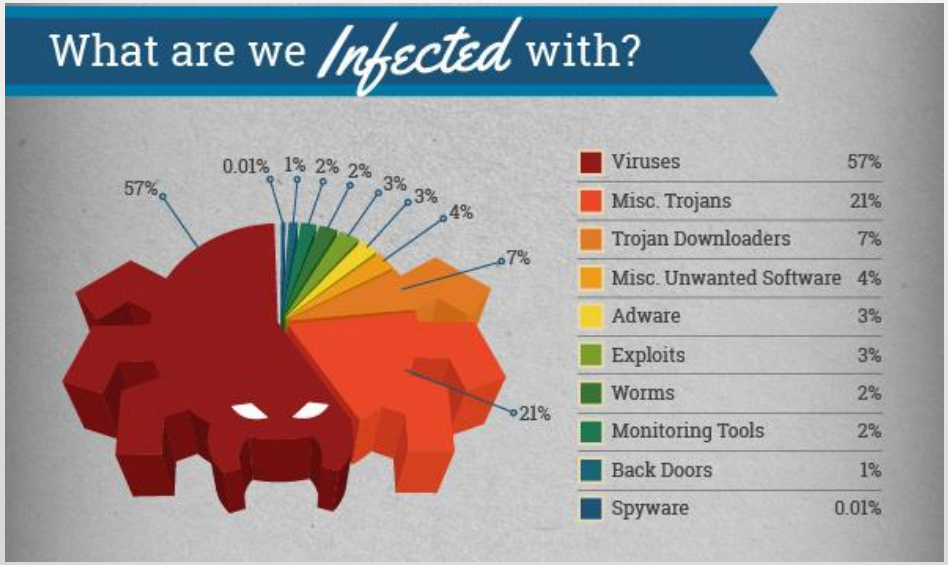
Statistics



Source : http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q4-2014.pdf

Statistics





Source : http://anti-virus-software-review.toptenreviews.com/how-infected-are-we.html

Summary

- Preventing and detecting attacks on networks is probably the most newsworthy aspect of security engineering.
- The problem is unlikely to be solved any time soon.
- The human element - “Amateurs hack systems, professionals hack people” (Bruce Schneier).
- Despite all the above, the Internet is **not** a disaster.

QUESTIONS?