SECURE COMMUNICATIONS AND SECURITY AWARENESS 101

BY: DIMAS FEBRIAWAN, MTI, CEH

MAY 18, 2017

MEDAN, SUMATERA UTARA

*'The methods that will most effectively minimize the ability of intruders to compromise information security are **comprehensive user training and education**. Enacting policies and procedures simply won't suffice. My access to Motorola, Nokia, ATT, Sun depended upon the willingness of people to bypass policies and procedures that were in place for years before I compromised them successfully.'*

Kevin Mitnick - an American computer security consultant, author and hacker, best known for his high-profile 1995 arrest and later five years in prison for various computer and communications-related crimes

'The Coming Third Wave of Internet Attacks:

- *The first wave of attacks targeted the physical electronics.*
- *The second wave - syntactic attacks - targets the network's operating logic.*
- *The third wave of attacks - semantic attacks - will target data and it's meaning. This includes fake press releases, false rumors, manipulated databases.*

Semantic attacks are much harder to defend against because they target meaning rather than software flaws. ***They play on security flaws in people, not in systems.****'*

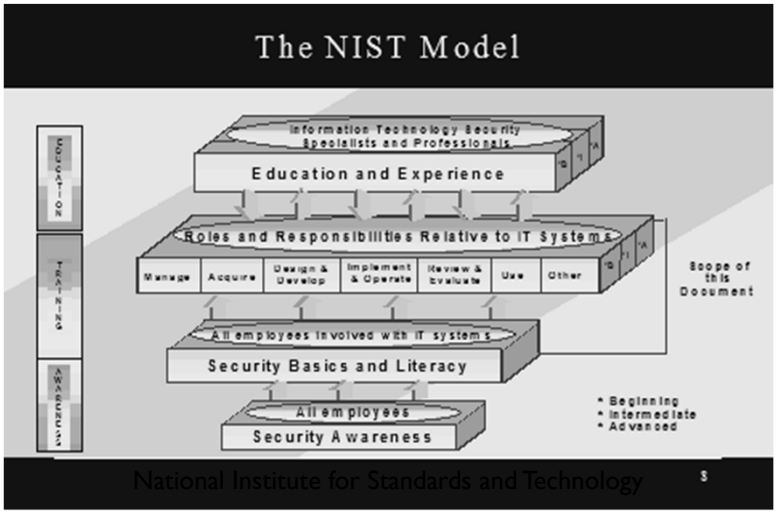
Bruce Schneier - an American cryptographer, computer security professional, privacy specialist and writer.

INTRODUCTION

About Me:

- IT Security Analyst at PT. Scan Nusantara (6 years)
  - Involved in various penetration testing, vulnerability assessment, and SIEM implementation projects
- IT Security Consultant at one of Indonesia's Private Banking Company (2 years)
  - Involved in developing and enforcing information security policies
- Present:
  - IT Lecturer at Universitas Muhammadiyah Prof. DR. Hamka
  - IT Security Auditor
  - Freelance IT Security enthusiast
- Website: http://dimz-it.com/
- Email: dimz_it@yahoo.com

AWARENESS…
TO FOCUS ATTENTION ON SECURITY



OVERVIEW

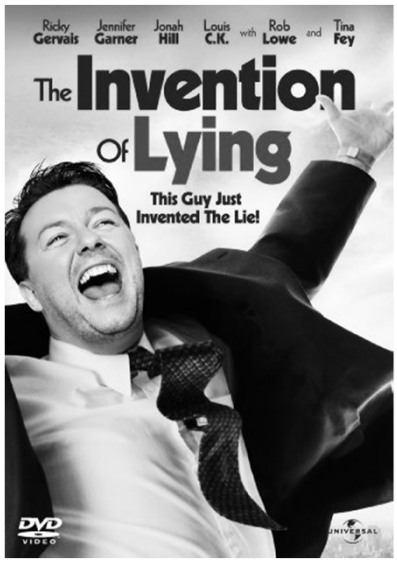
- Introduction
- Internet insecurity vs. Internet security
- Secure website
- Secure email
- Secure channel
- Wireless security
- Current trend in security threats
- Q & A

INTERNET INSECURITY

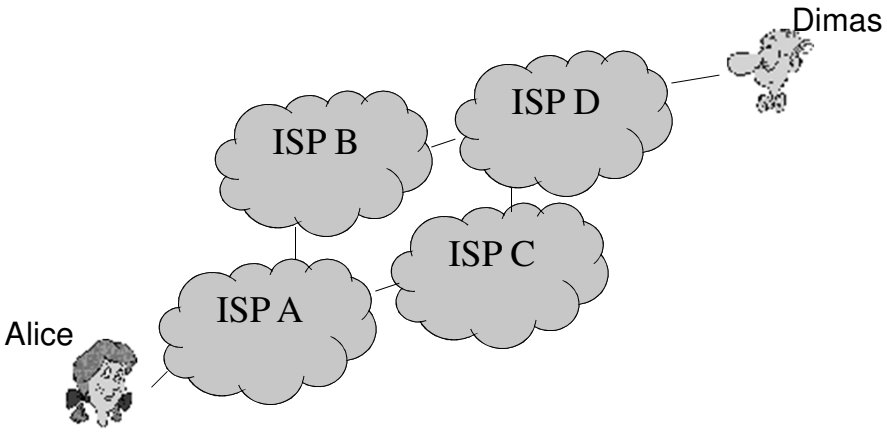
- Internet was not design with security in mind:
  - Originated as a small and cooperative network (U.S. DARPA)
  - Designed for simplicity, anyone can connect
  - "On by default" design

"Humans have natural tendency to trust on each other"

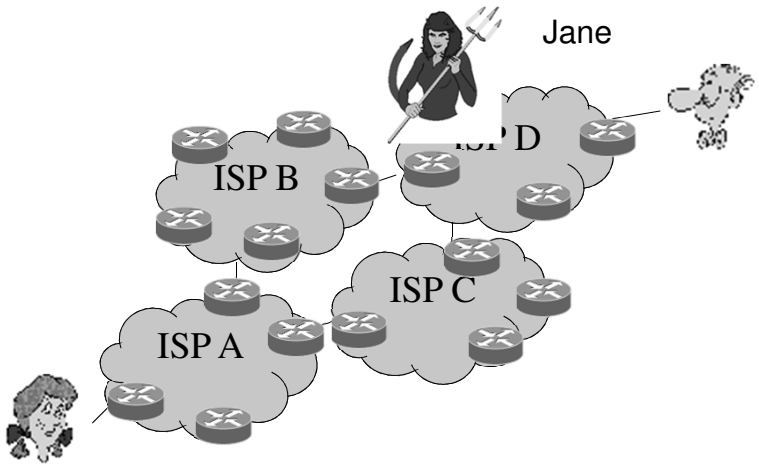
INTERNET INSECURITY



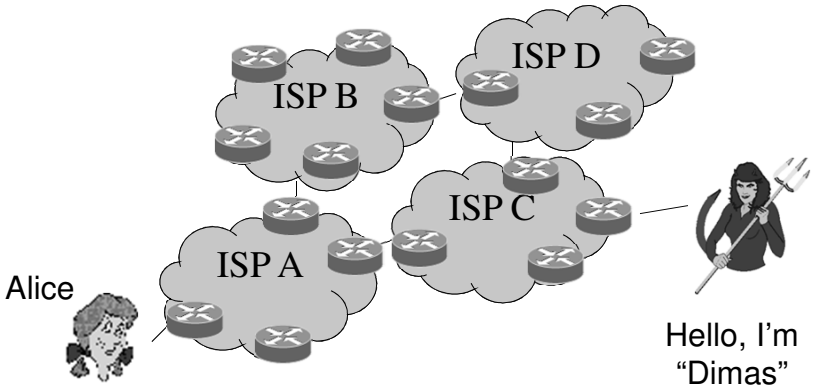
INTERNET INSECURITY



INTERNET INSECURITY



INTERNET INSECURITY



INTERNET SECURITY

- **Confidentiality:** concealment of information or resources.
- **Authenticity:** identification and assurance of the origin of information.
- **Integrity:** the trustworthiness of data or resources in terms of preventing improper and unauthorized changes.
- **Availability** the ability to use the information or resources as desired.
- **Non-repudiation:** offer of evidence that a party indeed is the sender or a receiver of certain information.

INTERNET SECURITY

- ***Security*** is a state of well-being of information and infrastructures in which the possibility of successful yet undetected theft, tampering, and disruption of information and services is kept low or tolerable

SECURE WEBSITE

SECURE WEBSITE

- Special characteristics of Web servers:
  - "Out there" accessible to anyone
  - Connected to corporate databases - dangerous if subverted
  - Application software developed quickly and often security-ignorant
- Special characteristics of Web users:
  - Often not security knowledgeable
  - Often not subject to corporate or other rules
  - Cannot be counted on to fulfill their part in a security protocol

WEB SECURITY THREATS

- Integrity
  - Modification of data on servers ("data-at-rest")
  - Modification of messages ("data-in-motion")
- Confidentiality
  - Theft of data from server, or from client
  - Eavesdropping on communication
  - Info on network configuration
  - Info on network traffic
- Availability
  - Denial of Service
- Authentication
  - Impersonation of legitimate users
  - Data forgery on server (or client)

HTTP VS. HTTPS

HTTP:

- All communications sent over regular HTTP connections are in 'plain text' and can be read by any hacker that manages to break into the connection between your browser and the website.
- This presents a clear danger if the 'communication' is on an order form and includes your credit card details or social security number.

HTTPS:

- With a HTTPS connection, all communications are securely encrypted.
- This means that even if somebody managed to break into the connection, they would not be able decrypt any of the data which passes between you and the website.

DEMO – HTTP VS. HTTPS

- Attack method: eavesdropping
- Scenario:
  - A user is accessing a website using plain HTTP protocol
  - A user is accessing a website using secure HTTPS protocol

HTTP VS. HTTPS

- Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, which means all communications between your browser and the website are encrypted.
- HTTPS pages typically use one of two secure protocols to encrypt communications - SSL (Secure Sockets Layer) or TLS (Transport Layer Security).
- Both the TLS and SSL protocols use what is known as an 'asymmetric' Public Key Infrastructure (PKI) system.
  - An asymmetric system uses two 'keys' to encrypt communications, a 'public' key and a 'private' key.
  - Anything encrypted with the public key can only be decrypted by the private key and vice-versa.
- In the case of a website, the private key remains securely stored on the web server.
- Conversely, the public key is intended to be distributed to anybody and everybody that needs to be able to decrypt information that was encrypted with the private key.

HTTP VS. HTTPS

- When a trusted SSL Digital Certificate is used during a HTTPS connection, users will see a padlock icon in the browser address bar.
- When an Extended Validation Certificate is installed on a web site, the address bar will turn green.
- Other signs:
  - Secure
  - Info or Not secure
  - Not secure or Dangerous

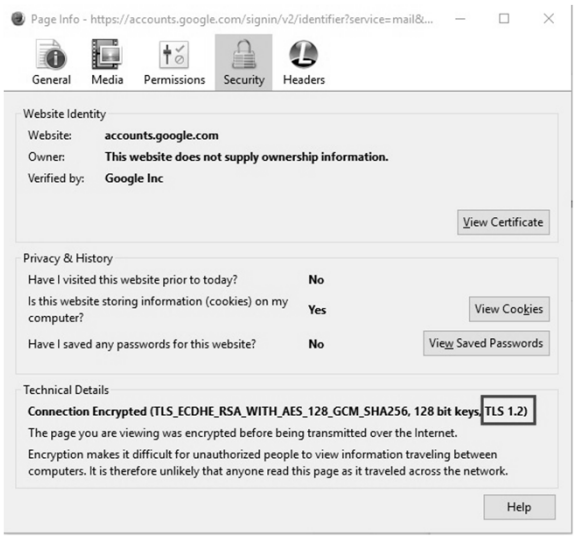
SSL VS. TLS

- TLS (Transport Layer Security) and SSL (Secure Sockets Layer) are protocols that provide data encryption and authentication between applications and servers in scenarios where that data is being sent across an insecure network,.
- The terms SSL and TLS are often used interchangeably or in conjunction with each other (TLS/SSL), but one is in fact the predecessor of the other — SSL 3.0 served as the basis for TLS 1.0.
- SSL Versions:
  - SSL version 1.0, 2.0, 3.0
- TLS Versions:
  - TLS version 1.0, 1.1, 1.2 (newest)
  - TLS version 1.3 (draft)

SSL VS. TLS

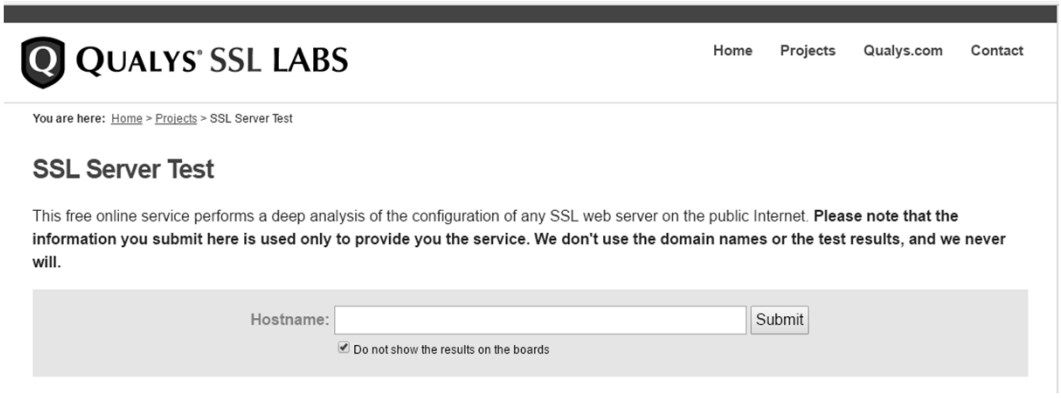
- SSL v3.0
  - Was exploited by the POODLE attack and is now obsolete
  - Vulnerable to BEAST attack
- TLS v1.0
  - Vulnerable to BEAST attack
- TLS v1.2
  - The newest, most widely-used TLS protocol
  - Enables better use of more secure ciphers
  - Features enhanced negotiation of the encrypted connections

SSL/TLS DETECTION – FOR USERS



SSL/TLS DETECTION – FOR SERVERS

- Free online SSL Server Test: https://www.ssllabs.com/ssltest/index.html

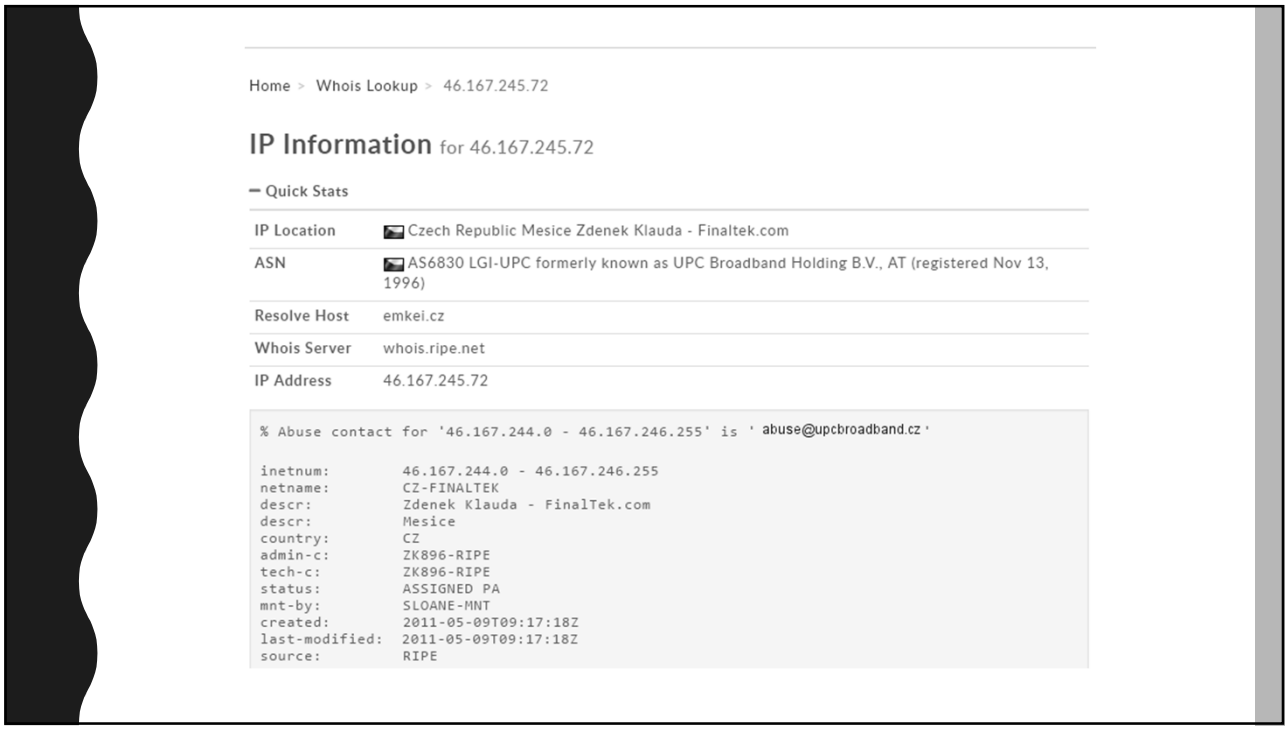


SECURE EMAIL

DEMO - EMAIL PHISHING

```
X-Apparently-To: dimz_it@yahoo.com; Tue, 16 May 2017 18:03:58 +0000
Return-Path: <jokowi@presidenri.go.id>
Received-SPF: none (domain of presidenri.go.id does not designate permitted sender hosts)
X-YMail-ISG: LH1q6cYWLD53X23gzmALAf5f2ZfcUHmLuTZKGeSeaqaw1vRZ
 PnNzLQ3mOdB2B6f2DaV7xlhS7PG5KX0cQV57VZ6pXrXS5Ey7ibsXm7vQ.EXV
 X9HQFaz041E1Juen_eWxVb8jHJpRvyL6IhGJ5Om_HUctzN2tuMcrwtwOGHOP
 7U5klm_2j1We30TkY13hxGZQ_T172o0npzs29BfPeNZ_.lm5obx4Qze3B.Xb
 p1jjLagqJ07Vo1kJGd26d0F0LjEzAsUeMfGkTgnRACL4uQrHCBHYSznAMBms
 Jf9KaRuX5xuiHA_rBoaCTVZajI6E6skNIiRJsWeIxWgIhShmHOXdI0Rq5wl6
 cx2uXzS_k0Sjz5Y3JW_vdfKQa1vfCLR4j4FW5hdTFFBX079cvhpV08i3SwYB
 7YTevAv26npNfhiGPHIiYLIhSv4ktoaUEkiWTpe4PnBhIE_RF57fbLy9qvFF
 UcHY0y4iDyN8HGnKawDJDpWevd2979caw9UnpePnUYCWw2Fyaie4aHQ_I6r1
 VyFz628U2hJQLI55bSbqc47H5Cn3llIzvpzb.zZEKpEIsjThkcIKuEMpHqRUE
 wKCeH6isbOCZzl35pn0cDrCyu4rMOxqm__FlzA91gRKwU45qsmPqIBndY8xc
 z1n1xlAApQOtnfvrcx5dNj1iAd.ZnydInvvyZaM40PZcQZ6uPwpIy06Vc02x
 M.QU82.XX_xYMOpZPSS3pOagkd.rCUrhM1B5pZqSdkQ_HmAz3KMFa04Br84p
 UCeyidWliBbvgAmEkcfgLN8JSPZaSZwSjJfC1xdU.zcDd6E.4BiD7Ua0AJLO
 IYAae1vlQCL8v2RyxQYPqJZM3Qj0h9ZVsKX7aiW2xdyc5xuCbOUaTS0Z3BIJ
 IL62z7Z18JjSNukcdslsWSiQ.AIIx8e0VVM1Ec52m4hk4vRWxUhozx330b0i
 f9Hkvt2c_9np.5ioz4vZVJwQjjy1p9fKmDIUvEREtBnxBqFhUG_qASVkihR7
 3ChL5icpZd1XuxT0VNrtZr9003jbrNTl7jBTwPTMqk4TKUqZmL5Np.2d6pzw
 DCnkl3JQSpWLXszI..BZyWnHj17QzvtEs.r3SCvzLyn1Wmf_bP96lmDkHx7W
 DNQXZRgpiDIR7nDg551uG8C8zWwyIxv1pTR774bpFUtDPqk9b0pfRnZ9OHFe
 a5.4F6hFR1bXbBA8GncNg0--
X-Originating-IP: [46.167.245.72]
Authentication-Results: mta1167.mail.ne1.yahoo.com  from=presidenri.go.id; domainkeys=neutral (no sig);  from=presidenri.go.id; dkim=neutral (no sig)
Received: from 127.0.0.1  (EHLO emkei.cz) (46.167.245.72)
  by mta1167.mail.ne1.yahoo.com with SMTPS; Tue, 16 May 2017 18:03:57 +0000
Received: by emkei.cz (Postfix, from userid 33)
        id 65D00D606A; Tue, 16 May 2017 20:03:55 +0200 (CEST)
To: dimz_it@yahoo.com
Subject: Undangan Makan Siang
From: "Joko Widodo" <jokowi@presidenri.go.id>
X-Priority: 3 (Normal)
Importance: Normal
Errors-To: jokowi@presidenri.go.id
Reply-To: jokowi@presidenri.go.id
Content-Type: text/plain; charset=utf-8
Message-Id: <20170516180355.65D00D606A@emkei.cz>
Date: Tue, 16 May 2017 20:03:55 +0200 (CEST)
Content-Length: 119

Dear Dimas,
```



Home > Whois Lookup > 46.167.245.72

IP Information for 46.167.245.72

− Quick Stats

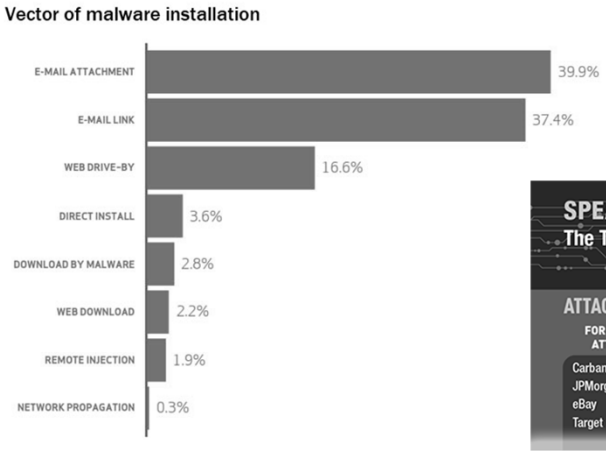
IP Location	Czech Republic Mesice Zdenek Klauda - Finaltek.com
ASN	AS6830 LGI-UPC formerly known as UPC Broadband Holding B.V., AT (registered Nov 13, 1996)
Resolve Host	emkei.cz
Whois Server	whois.ripe.net
IP Address	46.167.245.72

```
% Abuse contact for '46.167.244.0 - 46.167.246.255' is ' abuse@upcbroadband.cz '

inetnum:        46.167.244.0 - 46.167.246.255
netname:        CZ-FINALTEK
descr:          Zdenek Klauda - FinalTek.com
descr:          Mesice
country:        CZ
admin-c:        ZK896-RIPE
tech-c:         ZK896-RIPE
status:         ASSIGNED PA
mnt-by:         SLOANE-MNT
created:        2011-05-09T09:17:18Z
last-modified:  2011-05-09T09:17:18Z
source:         RIPE
```

EMAIL PHISHING

EMAIL PHISHING



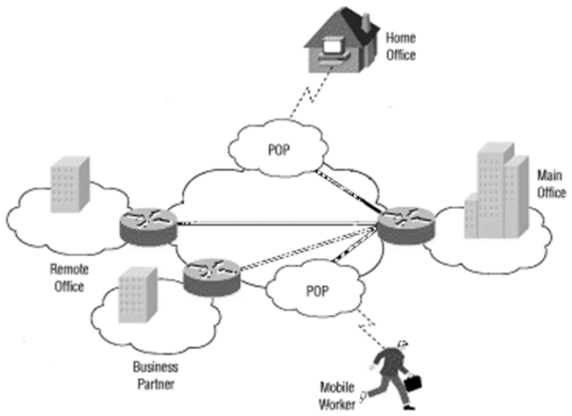
SECURE EMAIL

- Strong email account password
  - Minimum of 8 characters, contains at least: 1 small letter, 1 capital letter, 1 number and 1 special characters
- Secure protocol:
  - SMTPS (port 465 or 587)
  - POP3S (port 995) / IMAPS (port 993)
  - MS Exchange Encryption and Authentication (Oauth or NTLM Authentications)
- Secure format:
  - S/MIME (Secure/Multipurpose Internet Mail Extensions) is a standard for public key encryption and signing of MIME data. MIME standard was created to allow messages to have multiple parts and structure, to carry type information about individual parts, and to be able to carry non-text data.
- Encryption and digital certificate:
  - Free and powerful: OpenPGP (http://openpgp.org/) or ProtonMail (https://protonmail.com/)
- Disable email relaying for mail servers

SECURE CHANNEL

VPN

- Typical usage scenario for VPN



VPN

- A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.
- It creates a secure, encrypted connection, which can be thought of as a tunnel, between your computer and a server operated by the VPN service.
- VPNs may allow employees to securely access a corporate intranet while located outside the office.
- The VPN security model provides:
  - **Confidentiality** such that even if the network traffic is sniffed at the packet level an attacker would only see encrypted data
  - **Sender authentication** to prevent unauthorized users from accessing the VPN
  - **Message integrity** to detect any instances of tampering with transmitted messages

VPN

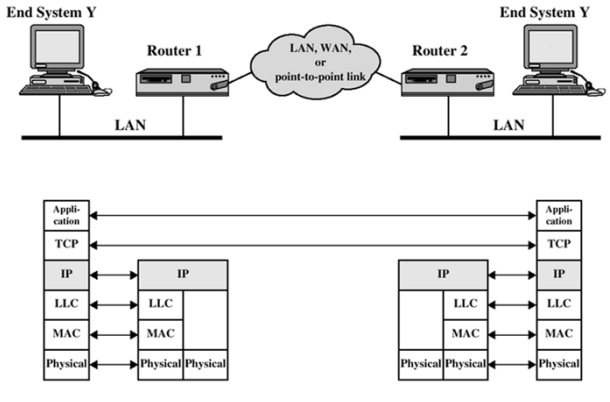
- Secure VPN protocols include the following:
  - Internet Protocol Security (IPsec) uses encryption, encapsulating an IP packet inside an IPsec packet. De-encapsulation happens at the end of the tunnel, where the original IP packet is decrypted and forwarded to its intended destination.
  - Transport Layer Security (SSL/TLS) can tunnel an entire network's traffic or secure an individual connection.
  - Datagram Transport Layer Security (DTLS) – used in Cisco AnyConnect VPN and in OpenConnect VPN to solve the issues SSL/TLS has with tunneling over UDP.
  - Microsoft Point-to-Point Encryption (MPPE) works with the Point-to-Point Tunneling Protocol and in several compatible implementations on other platforms.
  - Microsoft Secure Socket Tunneling Protocol (SSTP) tunnels Point-to-Point Protocol (PPP) or Layer 2 Tunneling Protocol traffic through an SSL 3.0 channel.
  - Multi Path Virtual Private Network (MPVPN). Developed by Ragula Systems Development Company.
  - Secure Shell (SSH) VPN – OpenSSH offers VPN tunneling to secure remote connections to a network or to inter-network links.

IPSEC

- IPsec is a piece of software that modified the IP stack so that all layers below IP can be encrypted (TCP, UDP, etc) and even Layer 2 can be encrypted using a tunneling daemon.

- Features that IPsec attempts to provide:
  - Encryption (optional)
  - Authentication (optional)
  - Confidentiality
  - Integrity
  - Availability

IPSEC

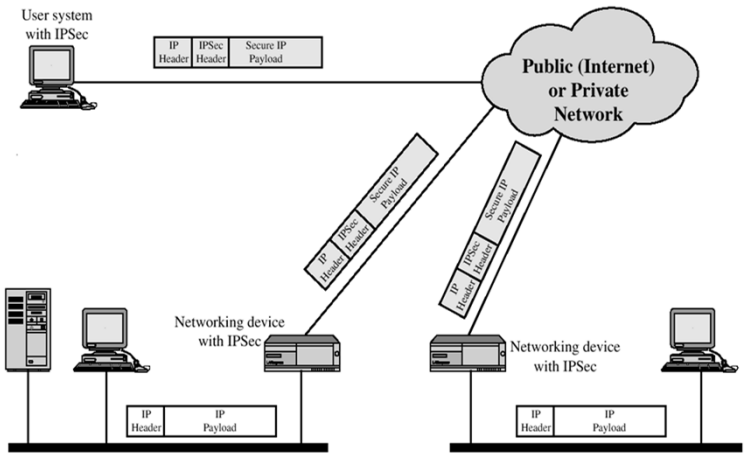


Application
Presentation
Session
Transport
Network (IP)
Data Link
Physical

OSI 7 layers

IPSEC

- Vulnerabilities:
  - IPSec-Tools (2015)
  - Logjam Attack (2015)



OTHER SECURE METHODS

- Teamviewer
- VNC (Virtual Network Computing)
- Secure Remote Desktop (RDP)
- Secure Shell (SSH)
- Secure File Transfer Protocol (SFTP) / Secure Copy (SCP)

WIRELESS SECURITY

WIRELESS NETWORKS

- Bluetooth – short range (10m), Personal Area Network, low voltage
- 802.11 – IEEE Standard for wireless LANs
- 802.11b (WiFi) – Direct Sequencing Spread Spectrum (DSSS), and increases bit rates to 11Mbps
- 802.11a – 5GHz frequency, 54Mbps, addresses some security concerns
- 802.11g – provides 54Mbps at 2.4GHz and compatible with 802.11b
- 802.11n – substantial increase in speed/range (MIMO technology)
- 802.11i – security standard for wireless networks

WIRED EQUIVALENT PRIVACY (WEP)

- Wireless communication is point-to-multipoint
  - Adversary can simply intercept packets, without having to intrude or impersonate
- Ratified in 1997, WEP security services:
  - Confidentiality
  - Integrity of messages
  - No key management, and no robust authentication
- WEP mechanisms
  - Challenge response (encryption) to authenticate
  - RC4 used to encrypt packets, based on a 40-bit key shared between mobile unit and access point, concatenated with 24 bit IV (link encryption)
  - Integrity Check Vector (ICV) is appended to the packets, to ensure that they were not modified

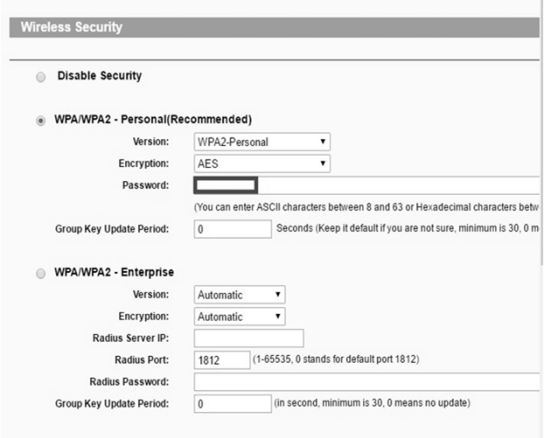
WIRED EQUIVALENT PRIVACY (WEP)

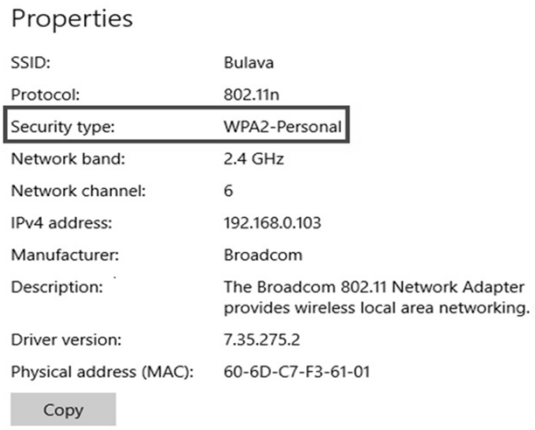
- Weaknesses:
  - Same hand-configured 40-bit key is shared by all mobile devices that connect to same access point
  - Lack of key management services results in infrequent change of above keys
  - Attacks take advantage of small IV size
  - Until 2003, WEP was only security standard in 802.11b
  - And (if this is not enough)…most devices are shipped with WEP turned OFF

WI-FI PROTECTED ACCESS (WPA / WPA2)

- New standard (part of 802.11i), approved 6/2004
- In Enterprise mode:
  - Key management services
  - Central RADIUS authentication server (otherwise Pre-Shared Key)
- RC4 enhanced with:
  - 48-bit IV and smart IV sequencing algorithms
  - New Message Integrity Code (MIC)
  - Key based on initial exchange of random numbers
  - Ongoing generation of per-packet keys
- In 2006 WPA replaced by WPA2:
  - Replaces RC4 with AES
  - CCMP = Counter-Mode Encryption + Cipher Block Chaining + Message Authentication Code
  - Requires new hardware
  - Michael algorithm shuts off network for 1 min when detecting an unauthorized message

WIRELESS SECURITY DETECTION





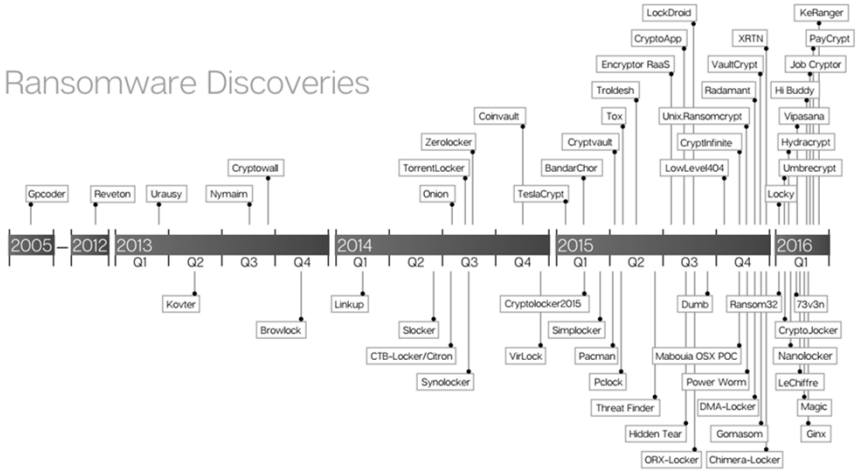
WIRELESS SECURITY TIPS

- For access point security:
  - Use strong passphrase / password
  - Don't broadcast your SSID
  - Use WPA2
  - Restrict access by MAC Address
  - Shut down when it is not being used
  - Monitor your network for intruders
  - Limit coverage based on necessity only
- For users:
  - Don't connect to FREE Wi-Fi
  - Only connect to Wi-Fi with WPA2 protection

WIRELESS SECURITY TIPS

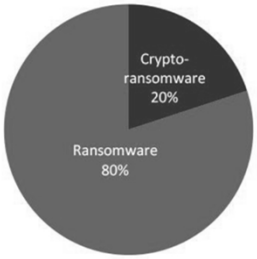
CURRENT TREND IN IT SECURITY THREATS

RANSOMWARE

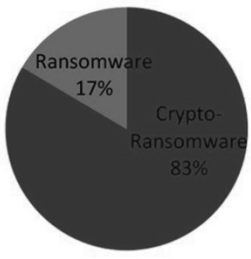


CRYPTO RANSOMWARE

2014 Ratio of Ransomware vs. Crypto-ransomware



2015 Ratio of Ransomware vs. Crypto-ransomware



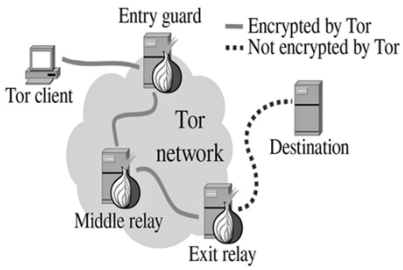
CRYPTO RANSOMWARE

CRYPTO RANSOMWARE

CRYPTO RANSOMWARE

- *Ransomware* is a type of malware that prevents or limits users from accessing their system, either by locking the system's screen or by locking the users' files unless a ransom is paid.
- More modern ransomware families, collectively categorized as *crypto-ransomware*, encrypt certain file types on infected systems and forces users to pay the ransom through certain online payment methods to get a decrypt key.
- *Crypto-ransomware* uses encryptions such as:
  - AES
  - RSA
- Uses *TOR network* to communicate with it's command center.

TOR NETWORK



- **Tor (The Onion Router)** is free software for enabling anonymous communication.
- Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.
- Using Tor makes it more difficult for Internet activity to be traced back to the user: this includes "visits to Web sites, online posts, instant messages, and other communication forms".
- Tor's use is intended to protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.
- Tor's domains are generally opaque, non-mnemonic, 16-character alpha-semi-numeric hashes which are automatically generated based on a public key ending with **.onion**

SECURITY TIPS

Q & A

Any Questions?

THANK YOU