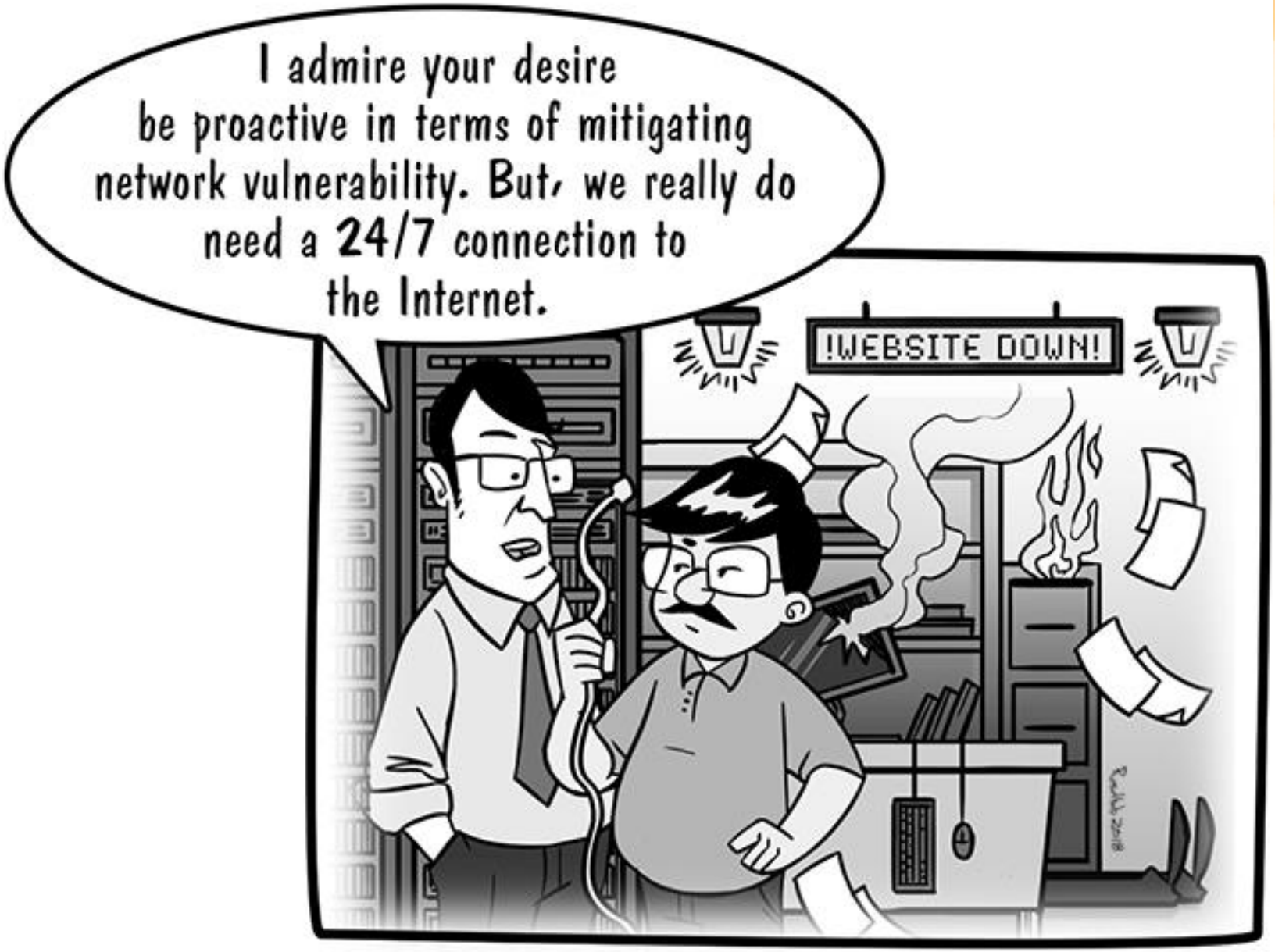
NETWORKS AND COMMUNICATIONS SECURITY

(ISC)²®


I admire your desire be proactive in terms of mitigating network vulnerability. But, we really do need a 24/7 connection to the Internet.
!WEBSITE DOWN!

OSI Model

APPLICATION LAYER Network-related application programs
PRESENTATION LAYER Standardization of data presentation to the applications
SESSION LAYER Management of sessions between applications
TRANSPORT LAYER End-to-end error detection and correction
NETWORK LAYER Management of connections across the network
DATA LINK LAYER Reliable data delivery Includes LLC and MAC sub-layers
PHYSICAL LAYER Physical characteristics of the network media

TCP/IP Reference Model

	OSI layer		TCP/IP layer
7	Application	4	Application
6	Presentation		
5	Session		
4	Transport	3	Transport
3	Network	2	Internet
2	Data Link	1	Network Access
1	Physical		

Internet Protocol (IP) Networking

- IP is responsible for sending packets from the source to the destination hosts
- Hosts are distinguished by the IP addresses of their network interfaces
- The address is expressed as four octets separated by a dot (.), for example, 216.12.146.140
- Each octet may have a value between 0 and 255

Network Classes

Class	Range of First Octet	Number of Network Octets	Number of Hosts in Network
A	1 – 127	1	16,777,214
B	128 – 191	2	65,534
C	192 – 223	3	254
D	224 – 239		
E	240 – 255		

IPv6

A much larger address field

Improved security

A more concise IP packet header

Improved quality of service

Transmission Control Protocol (TCP)

- The Transmission Control Protocol provides connection-oriented data management and reliable data transfer
- Port ranges:
  - Well-known Ports – (0 – 1023)
  - Registered Ports – (1024 – 49151)
  - Dynamic or Private Ports – (49152 – 65535)

ICMP Redirect Attack

- A router may send an ICMP redirect to a host to tell it to use a different, more effective default route
- However, an attacker can send an ICMP redirect to a host telling it to use the attacker's machine as a default route

Traceroute Exploitation

Traceroute is a diagnostic tool that displays the path a packet traverses between a source and destination host

Traceroute can be used maliciously to map a victim network and learn about its routing

Carrier Sense Multiple Access (CSMA)

- Access protocol that uses the absence/presence of a signal on the medium that it wants to transmit on as permission to speak
- Two variations:
  - Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - Carrier Sense Multiple Access with Collision Detection (CSMA/CD)

Token Ring (IEEE 802.5)

Token Ring uses a physical star topography

The logical topography, however, is a ring

Each device receives data from its upstream neighbor and transmits to its downstream neighbor

Token Ring uses ring passing to mediate which device may transmit


HERE'S YOUR PROBLEM. THE CONNECTION TO THE NETWORK IS BROKEN.
UH-OH. IT'S A "TOKEN RING" LAN. THAT MEANS THE TOKEN FELL OUT AND IT'S IN THIS ROOM SOMEPLACE.
S.Adams
5/2/96 © 1996 United Feature Syndicate, Inc.(NYC)
YOU ARE THE WIND BENEATH MY WINGS.
I'LL WAIT A WEEK THEN TELL HIM THE TOKEN MUST BE IN THE "ETHERNET."

Lightweight Directory Access Protocol (LDAP)

Commonly used for managing user information

Ports	389/TCP,389/UDP
RFC 1777 (Original)	

Network Basic Input Output System (NetBIOS)

Under TCP/IP, NetBIOS runs over TCP on ports 137 and 138 and over UDP on port 139

Ports	135/UDP 137/TCP 138/TCP 139/UDP
RFC 1001 RFC 1002	

Common Internet File System (CIFS)/Server Message Block (SMB)

CIFS/SMB is a file-sharing protocol prevalent on Windows systems

Ports	445/TCP
Definition Proprietary	

File Transfer Protocol (FTP)

Stateful protocol that requires two communication channels

Ports	20/TCP (data stream)
Definition RFC 959	

Hypertext Transfer Protocol (HTTP)

HTTP is the Layer 7 foundation of the World Wide Web (WWW)

Ports	80/TCP; other ports are in use especially for proxy services
Definition	
RFC 1945 (HTTP v1.0)	
RFC 2109	
RFC 2616 (HTTP v1.1)	

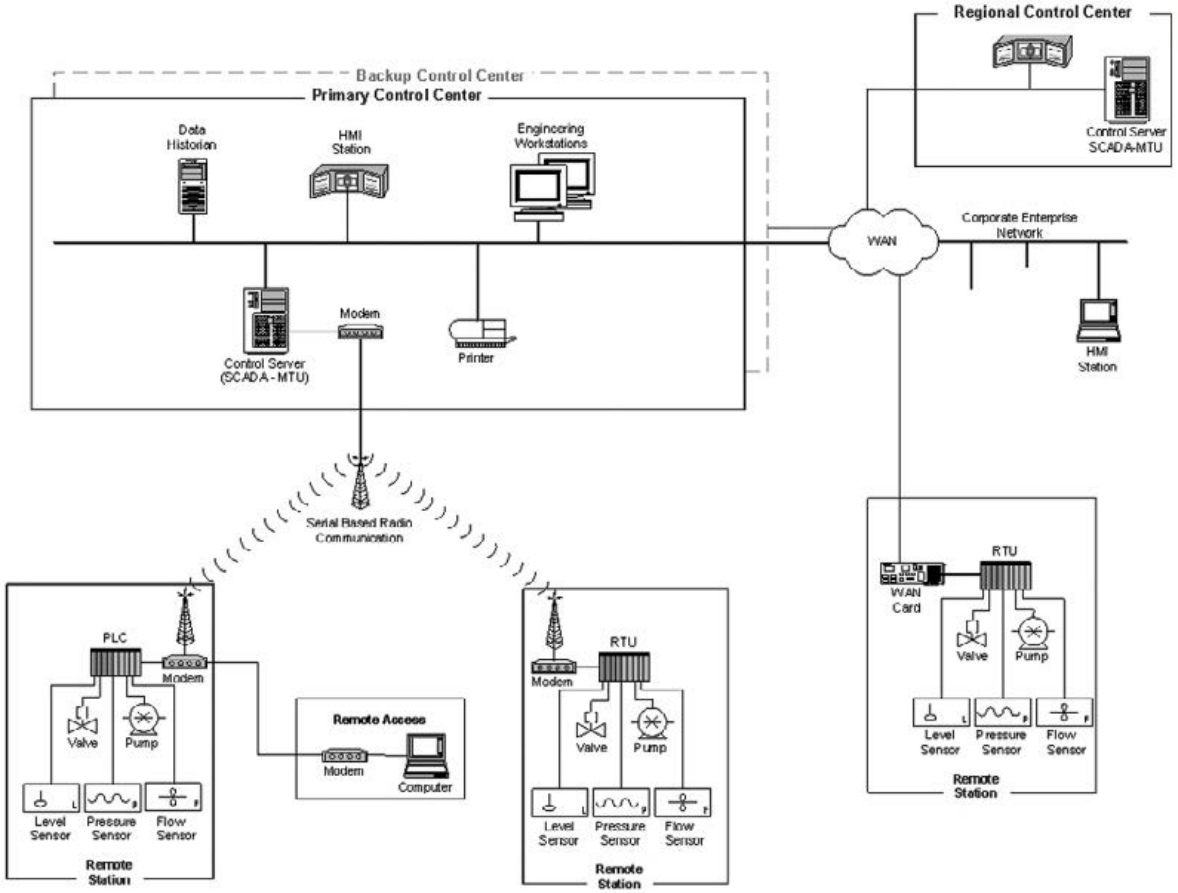
HTTP Tunneling

Applied by encapsulating outgoing traffic from an application in an HTTP request and incoming traffic in a response

Implication of Multilayer Protocols

SECURITY TOPIC	INFORMATION TECHNOLOGY	CONTROL SYSTEMS
Anti-virus/Mobile Code	Common Widely used	Uncommon/Impossible to deploy effectively
Support Technology Lifetime	2-3 Years Diversified vendors	Up to 20 years Single vendor
Outsourcing	Common Widely Used	Operations are often outsourced, but not diverse to various providers
Application of Patches	Regular Scheduled	Rare, Unscheduled Vendor specific
Change Management	Regular Scheduled	Highly managed and complex
Time Critical Content	Generally delays accepted	Delays are unacceptable
Availability	Generally delays accepted	24x7x365 (continuous)
Security Awareness	Moderate in both private and public sector	Poor except for physical
Security Testing/Audit	Part of a good security program	Occasional testing for outages
Physical Security	Secure (server rooms, etc.)	Remote/Unmanned Secure

Supervisory Control and Data Acquisition (SCADA)



POTS

Commonly found in the "last mile" of most residential and business telephone services

Attacks and Countermeasures

Attacks on telecommunications systems:

- Telecommunication DoS (TDoS) / Distributed DoS (DDoS)
- Denial of Service (DoS)
- DDoS for Hire
- SIP Flooding
  - Often takes place because attackers are running brute-force password guessing scripts that overwhelm the processing capabilities of the SIP device

Man-in-the-Middle Attack

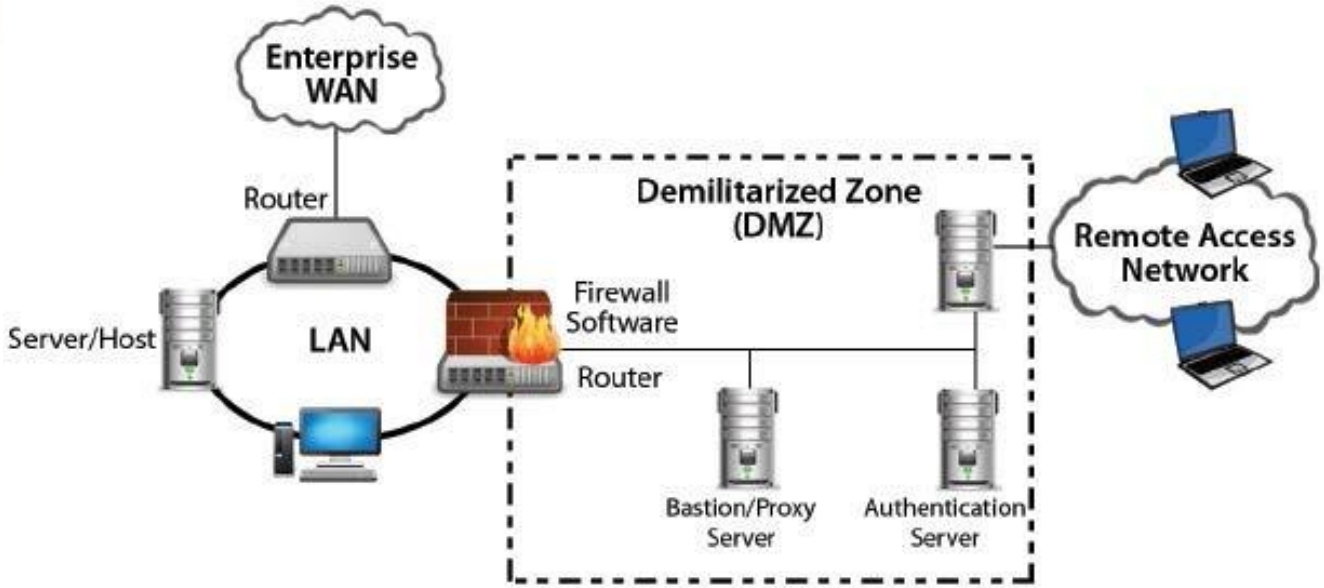
Malicious party:

- Intercepts a legitimate communication between two friendly parties
- Then controls the flow of communication
- Can eliminate or alter the information sent

Network Partitioning

- Segmenting networks into domains of trust is an effective way to help enforce security policies
- Controlling which traffic is forwarded between segments protects digital assets

Demilitarized Zone (DMZ)



Instant Messaging

Instant messaging systems can generally be categorized in three classes:

- Peer-to-peer networks
- Brokered communication
- Server-oriented networks

Extensible Messaging and Presence Protocol (XMPP) and Jabber

Jabber is an open instant messaging protocol for which a variety of open-source clients exist

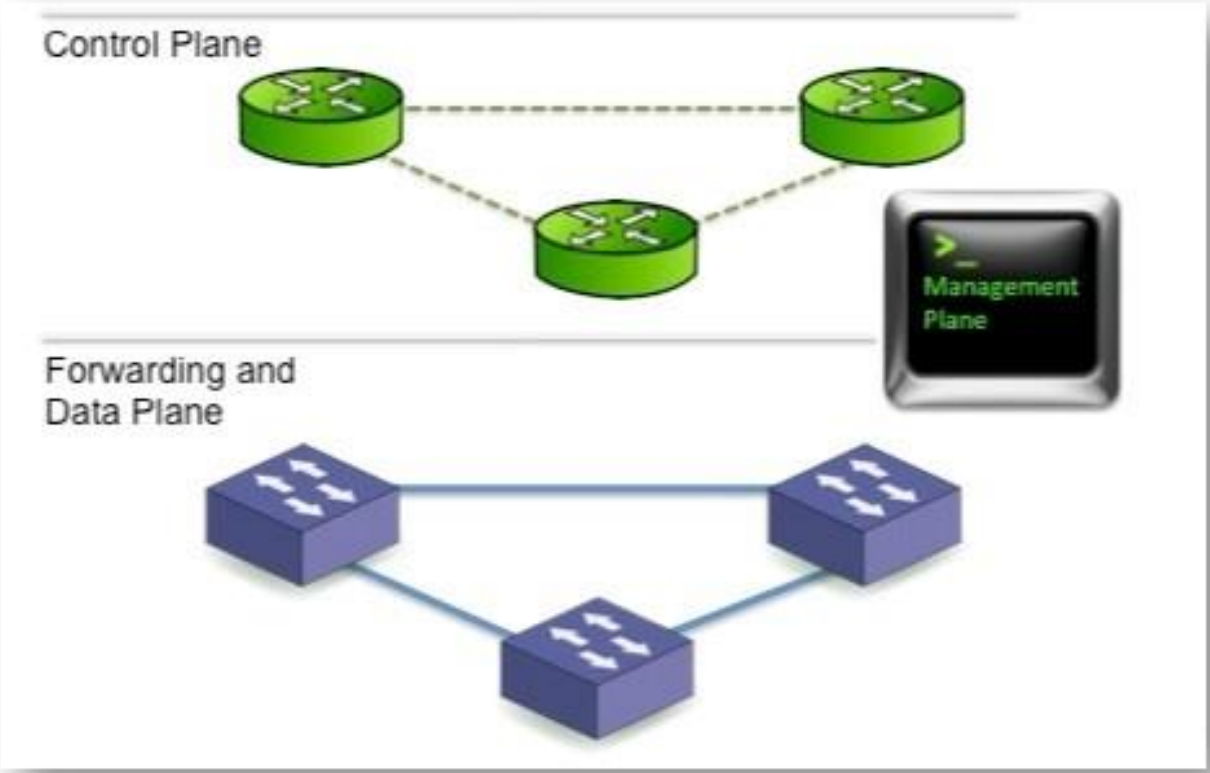
Tunneling Firewalls and Other Restrictions

Control of HTTP tunneling can happen on the firewall or the proxy server

Virtual Private Network (VPN)

An encrypted tunnel between two hosts that allows them to securely communicate over an untrusted network

Logical Design for Control Planes



Segmentation

- VLAN is a set of workstations within a LAN that can communicate with each other as though they were on a single, isolated LAN
- The basic reason for splitting a network into VLANs is to reduce congestion on a large LAN

Advantages of Using VLANs

- Performance
- Formation of virtual workgroups
- Greater flexibility
- Ease of partitioning off resources

Common Attacks Against the Data-Link Layer

- MAC Flooding Attack
- 802.1Q and Inter-Switch Link Protocol (ISL) Tagging Attack
- Double-Encapsulated 802.1Q/Nested VLAN Attack
- ARP Attacks
- Multicast Brute-Force Attack
- Spanning-Tree Attack
- Random Frame Stress Attack

Secure Shell (SSH)

Secure Shell (SSH) services:

- Include remote logon, file transfer, and command execution
- Support port forwarding

Simple Network Management Protocol (SNMP)

Allows the manager to retrieve “get” values of variables from the agent, as well as “set” variables

Ports	Definition
161/TCP | UDP 162/TCP | UDP	RFC 1157

DNSSEC

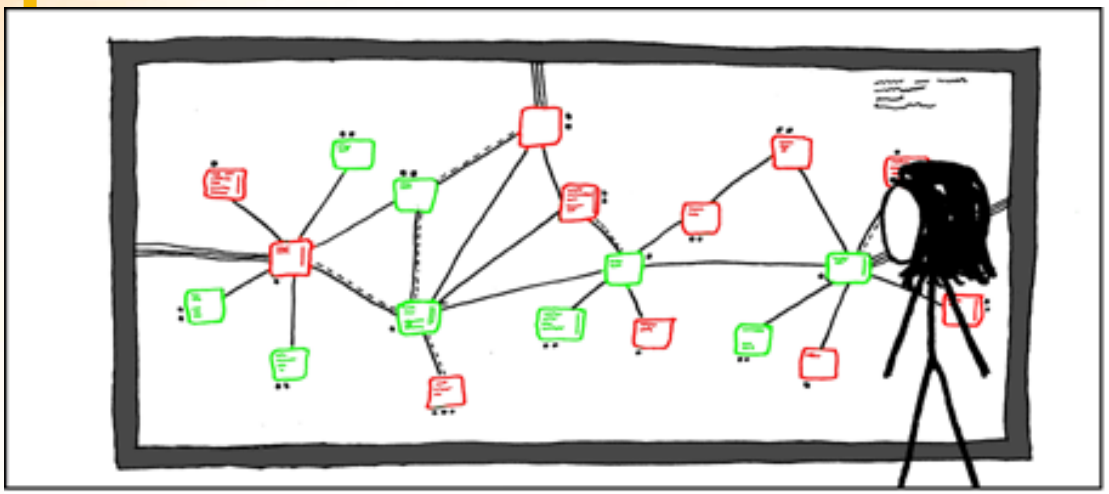
- The security extensions to DNS add protection for DNS records and allow the resolvers and applications to authenticate the data received
- The point of DNSSEC is to provide a way for DNS records to be trusted by whoever receives them

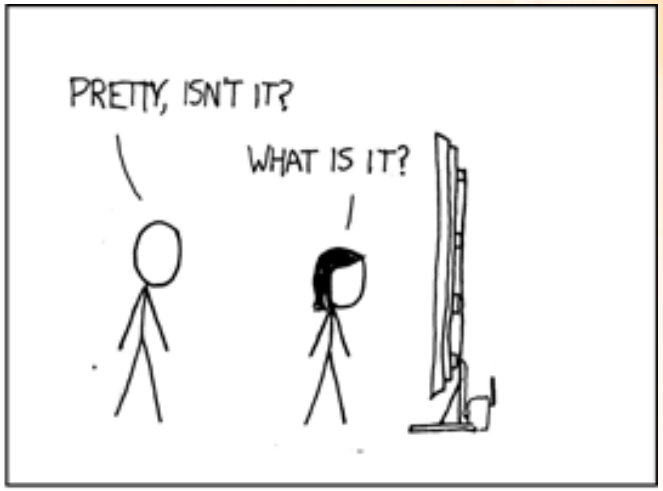
The Network as a Bastion of Defense

Definition of Security Domains

Segregation of Security Domains

Incident Response Capability





I'VE GOT A BUNCH OF VIRTUAL WINDOWS MACHINES NETWORKED TOGETHER, HOOKED UP TO AN INCOMING PIPE FROM THE NET. THEY EXECUTE EMAIL ATTACHMENTS, SHARE FILES, AND HAVE NO SECURITY PATCHES.

THERE ARE MAIL TROJANS, WARHOL WORMS, AND ALL SORTS OF EXOTIC POLYMORPHICS. A MONITORING SYSTEM ADDS AND WIPES MACHINES AT RANDOM. THE DISPLAY SHOWS THE VIRUSES AS THEY MOVE THROUGH THE NETWORK.

Network Security Objectives and Attack Modes

Perimeter defense

Defense in depth

Confidentiality

- An eavesdropping computer can be a legitimate client on the network or an unauthorized one
- Advantageous for an attacker to remain invisible on the network

Integrity

- The property association with corruption or change (intentional or accidental)
- A network needs to support and protect the integrity of its traffic

Availability

- The property of a network service related to its uptime, speed, and latency
- Availability of the service is commonly the most obvious business requirement

Domain Litigation

Domain names are subject to trademark risks, related to a risk of temporary unavailability or permanent loss of an established domain name

Open Mail Relay Servers

An SMTP service that allows inbound SMTP connections for domains it does not serve

Generally considered a sign of bad system administration

Firewalls

Firewalls are devices that enforce administrative security policies by filtering incoming traffic based on a set of rules

Filtering

- Firewalls filter traffic based on a rule set
- Each rule instructs the firewall to block or forward a packet based on one or more conditions
- Two important conditions used to determine if a packet should be filtered are:
  - By Address
  - By Service

Network Address Translation (NAT)

- Firewalls can change the source address of each outgoing packet to a different address
- Non-routable address
- Anonymity

Stateful Inspection or Dynamic Packet Filtering

Stateful inspection examines each packet in the context of a session

Allows dynamic adjustments to the rules

Proxies

A proxy firewall mediates communications between untrusted end-points and trusted end-points

- Circuit-level Proxy
- Application-level Proxy
- Web Proxy servers

Personal Firewalls

Following the principle of security in depth, personal firewalls should be installed on workstations, which protect the user from all hosts on the network

Port Scanning

The act of probing for TCP services on a machine

FIN, NULL, and XMAS Scanning

In FIN scanning, a stealth scanning method, a request to close a connection is sent to the target machine

TCP Sequence Number Attacks

- TCP attaches a sequenced number to each data packet that is transmitted
- If a transmission is not reported back as successful, a packet will be retransmitted.
- Eavesdropping allows a third party to predict the correct sequence number and introduce fake packets into the data stream.

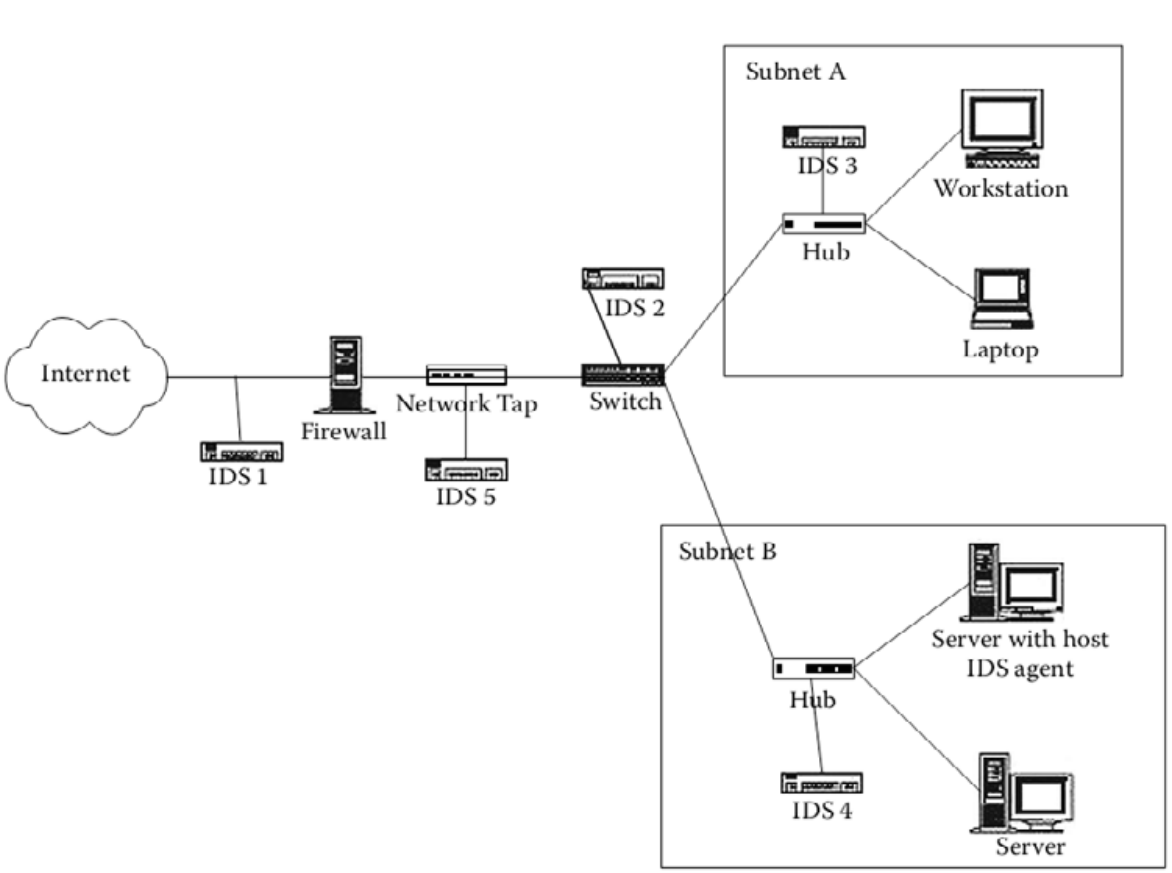
Intrusion Detection Systems (IDS)

IDS monitor activity and send alerts when they detect suspicious traffic

Two broad classifications:

- Host-based IDS
- Network-based IDS

Architecture of an Intrusion Detection System (IDS)



SEM/SEIM

A solution that involves harvesting logs and event information from a variety of different sources on individual servers or assets and analyzing it as a consolidated view with sophisticated reporting

Scanners

Discover devices and services on a network

Test compliance with a given policy

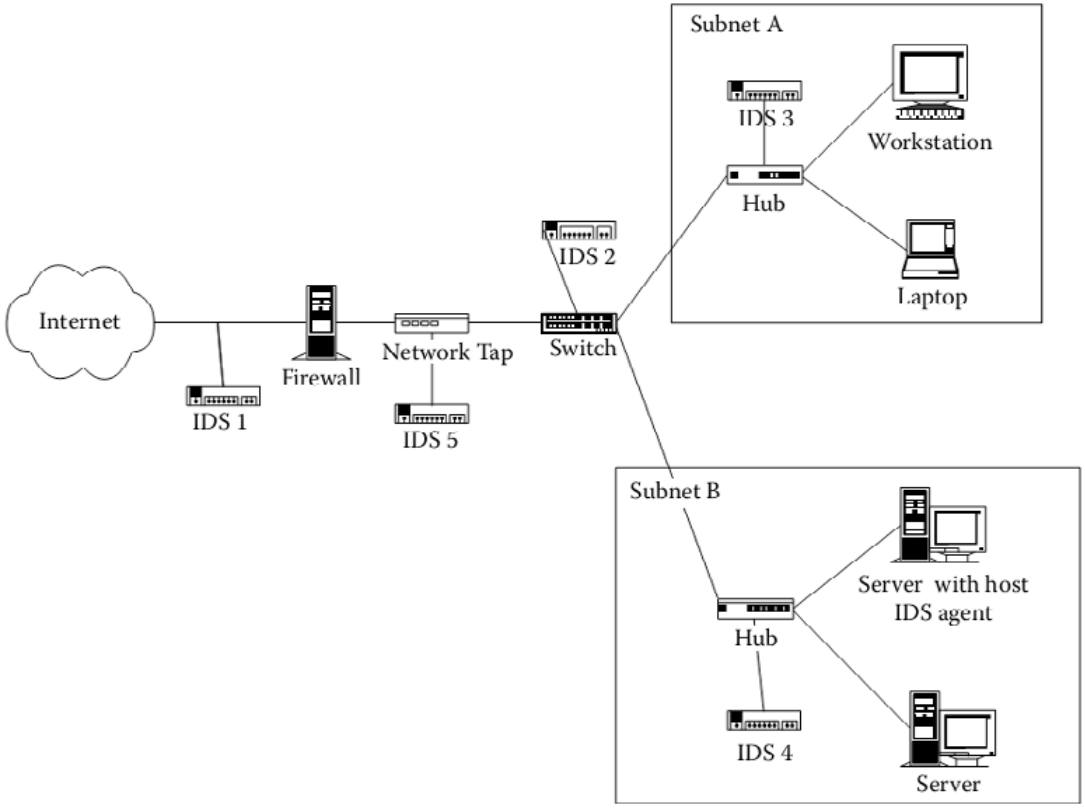
Test for vulnerabilities

Scanning Tools

Nessus

Nmap

Network Taps



IP Fragmentation Attacks and Crafted Packets

- Teardrop
- Overlapping Fragment
- Source Routing Exploitation
- Smurf and Fraggle

Network Time Protocol (NTP)

- **NTP:**
  - Synchronizes computer clocks in a network
- **Simple Network Time Protocol (SNTP):**
  - Less resource intensive
  - Less exact form of synchronization

Denial-of-Service Attack (DoS)

Overload it through excessive traffic or traffic that has been "crafted" to confuse the network into shutting down or slowing to the point of uselessness

Distributed Denial-of-Service Attack (DDoS)

Using a network of remote-controlled hosts known as "botnets" the target is subjected to traffic from a wide range of sources that are very hard to block

SYN Flooding

A denial-of-service attack against the initial handshake in a TCP connection

IP Address Spoofing and SYN-ACK Attacks

- Packets are sent with a bogus source address so that the victim will send a response to a different host
- Spoofed addresses can be used to abuse the three-way handshake that is required to start a TCP session

DNS Vulnerabilities

Two principal vulnerabilities here:

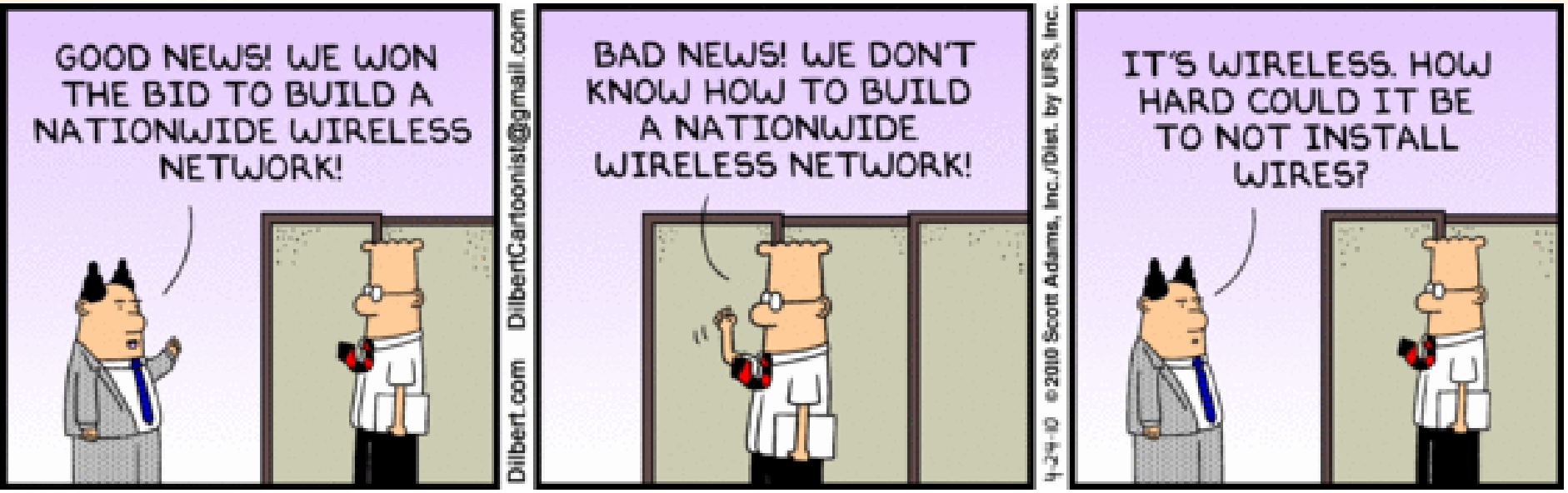
- It is possible for a DNS server to respond to a recursive query with information that was not requested.
- The DNS server will not authenticate information

Information Disclosure

Although knowing a server name will not enable anyone to access it, this knowledge can aid and facilitate preparation of a planned attack

Namespace-Related Risks

- **Session hijack**
  - IP spoofing
  - Man-in-the-middle attack
- **SYN scanning**


GOOD NEWS! WE WON THE BID TO BUILD A NATIONWIDE WIRELESS NETWORK!
BAD NEWS! WE DON'T KNOW HOW TO BUILD A NATIONWIDE WIRELESS NETWORK!
IT'S WIRELESS. HOW HARD COULD IT BE TO NOT INSTALL WIRES?
Dilbert.com DilbertCartoonist@gmail.com
4-24-10 ©2010 Scott Adams, Inc./Dist. by UFS, Inc.

Types of Wireless Technologies

Wi-Fi

Bluetooth

WiMAX

Types of Wireless Networks

- Wireless PAN
- Wireless LAN
- Wireless mesh network
- Wireless MAN
- Wireless WAN
- Cellular network
- Spread spectrum

Open System Authentication

- **The default authentication protocol for the 802.11 standard**
- **Consists of:**
  - A simple authentication request containing the station ID
  - An authentication response containing success or failure data

Shared Key Authentication

Shared Key Authentication is a standard challenge and response mechanism that makes use of WEP and a shared secret key to provide authentication

Ad Hoc Mode

- One of the networking topologies provided in the 802.11 standard
- Consists of at least two wireless endpoints where there is no access point involved in their communication

Infrastructure Mode

- A networking topography in the 802.11 standard
- Consists of a number of wireless stations and access points
- The access points usually connect to a larger wired network

Wired Equivalent Privacy Protocol (WEP)

- Basic security feature in the IEEE 802.11 standard
- Provides confidentiality over a wireless network by encrypting information sent over the network

Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access 2 (WPA2)

Provides users a higher level of assurance that their data will remain protected by using the Temporal Key Integrity Protocol (TKIP) for data encryption

A "Parking Lot" Attack

- Attackers actually sit in the organization's parking lot and try to access internal hosts via the wireless network
- If a network is compromised, the attacker has achieved a high level of penetration into the network

Shared Key Authentication Flaw

Shared key authentication can easily be exploited through a passive attack by eavesdropping on both the challenge and the response between the access point and the authenticating client

Service Set Identifier (SSID) Flaw

If the default SSID is not changed, it is very likely that an attacker will be able to successfully attack the device due to the use of the default configuration

The Vulnerability of Wired Equivalent Privacy Protocol (WEP)

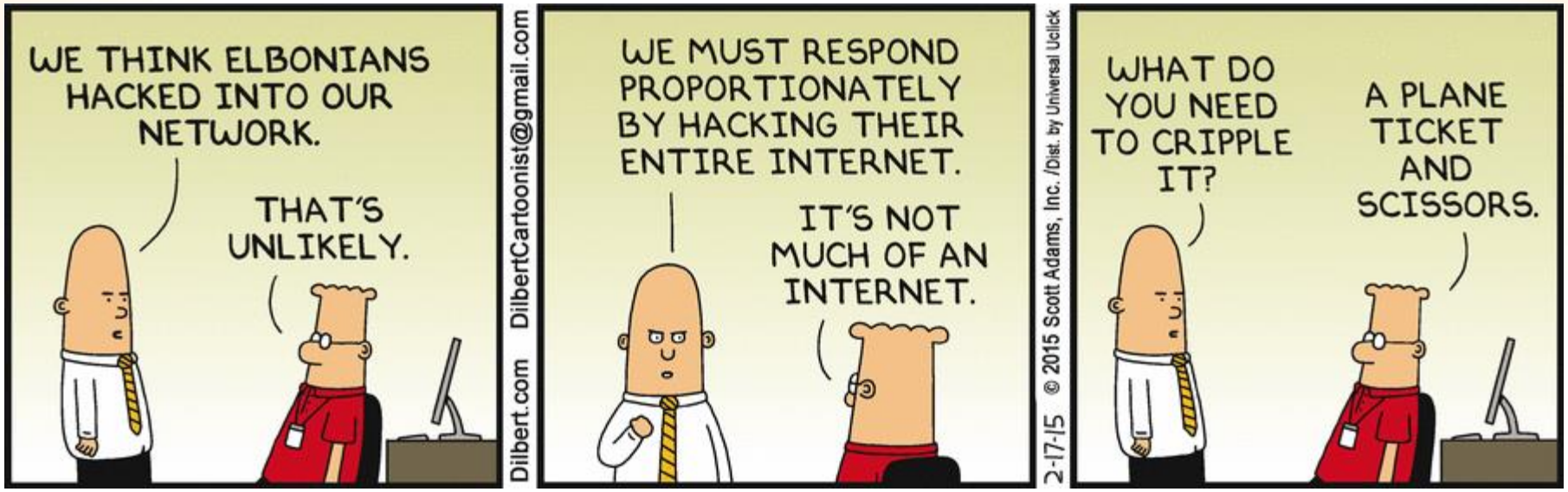
Data passing through a wireless LAN with WEP enabled is susceptible to eavesdropping and data modification attacks

Attack on Temporal Key Integrity Protocol (TKIP)

TKIP attack tries to decode data one byte at a time using multiple replays and observing the response over the air

An attacker can decode small packets such as ARP frames in about 15 minutes

If QoS is enabled, the attacker can further inject up to 15 arbitrary frames for every decrypted packet


WE THINK ELBONIANS HACKED INTO OUR NETWORK.
THAT'S UNLIKELY.
Dilbert.com DilbertCartoonist@gmail.com
WE MUST RESPOND PROPORTIONATELY BY HACKING THEIR ENTIRE INTERNET.
IT'S NOT MUCH OF AN INTERNET.
2-17-15 © 2015 Scott Adams, Inc. /Dist. by Universal Uclick
WHAT DO YOU NEED TO CRIPPLE IT?
A PLANE TICKET AND SCISSORS.