DENNIS GUNAWAN

IF470 COMPUTER SECURITY

10 MAN–IN–THE–MIDDLE ATTACKS

REVIEW: SECURITY IN EXTERNAL NETWORK COMMUNICATION

- Wireless or WiFi Network Communications
- Interception
- Peer-to-Peer Networks

COURSE SUB LEARNING OUTCOMES (SUB-CLO)

- Sub-CLO 10
  - Students are able to relate man-in-the-middle attacks to real case in their daily life (C3)

OUTLINE

- Threat
  - Man in the Middle
  - "In-the-Middle" Activity
- Vulnerability
  - Unwarranted Trust
  - Failed Identification and Authentication
  - Unauthorized Access
  - Inadequate Attention to Program Details
  - Protocol Weakness
- Countermeasure
  - Trust
  - Identification and Authentication
  - Cryptography
- Replay Attacks
- Session Hijack

INTRODUCTION

- So much human interaction is one-to-one
  - Voice, appearance, location, or language can confirm that the other person is who we think it is / the other party is authentic
- Computers interact with humans and other computers
  - It is more difficult to verify the authenticity of the parties or computers involved

INTRODUCTION

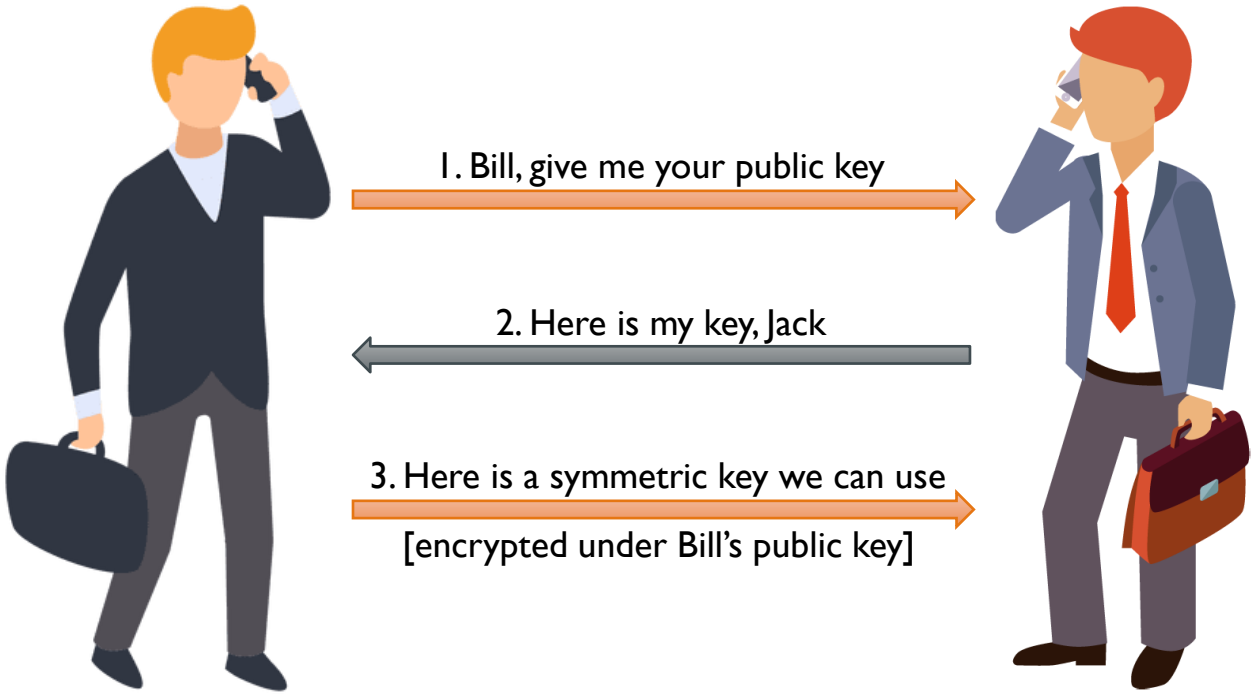
- Situations that seem to be one-to-one but are in fact three-party
- Someone or something else has interceded into what should ordinarily be a direct interaction between 2 entities
- The intervener can disrupt free interaction in a way that is difficult to detect or prevent

MAN–IN–THE–MIDDLE (MITM)

- An active wiretapping technique
- The attacker catches and replaces a communication between 2 endpoints without either endpoint knowing the transmission is modified
- One entity intrudes in an exchange between 2 parties and pretends to be the other party in interactions with each of the two sides

MAN–IN–THE–MIDDLE (MITM)

- Suppose 2 parties, Jack and Bill, want to communicate
- Asymmetric cryptography can be a way they can exchange cryptographic keys securely
- Basically, the key exchange protocol would work like this



MAN–IN–THE–MIDDLE (MITM)

In a man-in-the-middle attack, we insert the attacker, Emily, into this communication

1. Bill, give me your public key

2. No, give it to me

3. Here is my key, Jack

4. Here is the middle's key

5. Here is the symmetric key
[encrypted under the middle's public key]

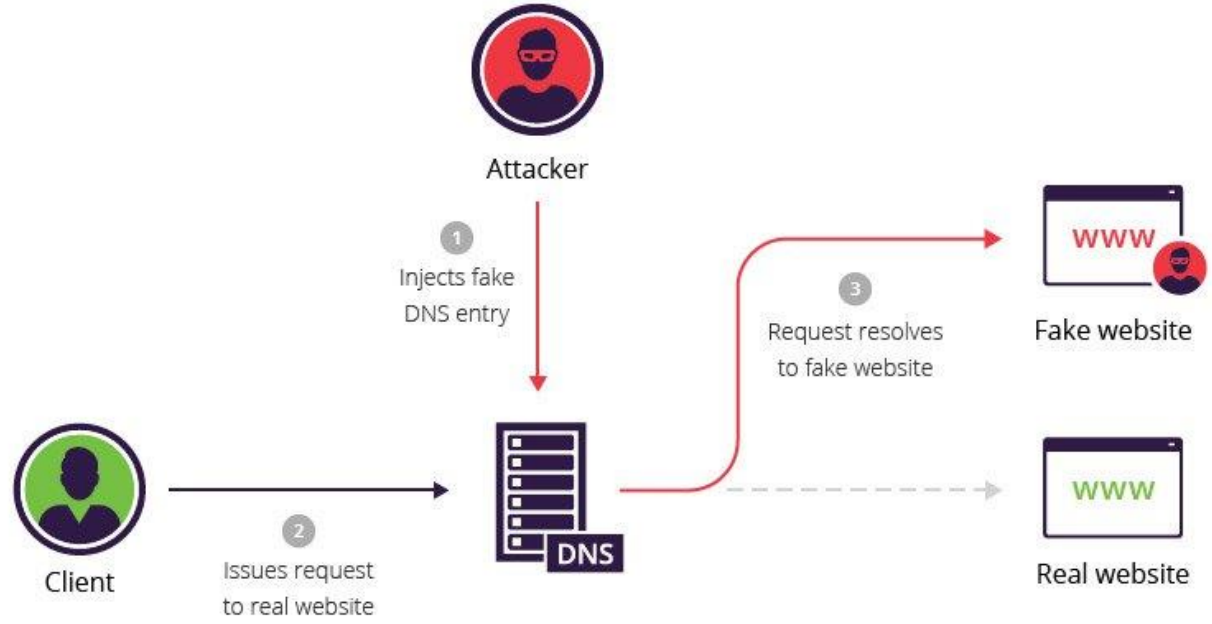
6. Here is another symmetric key
[encrypted under Bill's public key]

"IN–THE–MIDDLE" ACTIVITY

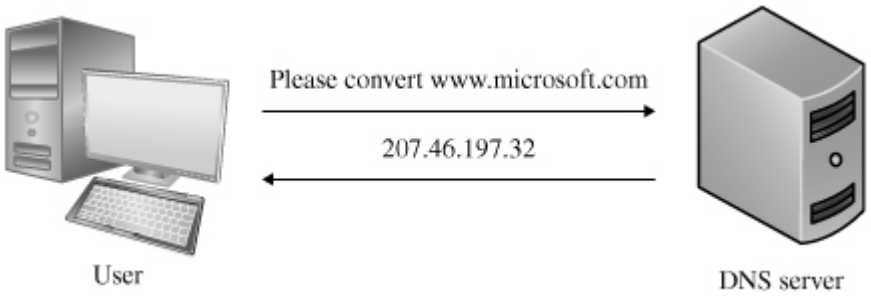
- The keystroke logger is a limited form of a man-in-the-middle attack
  - Passive, merely intercepting data without modifying it
- A classic man-in-the-middle attack involves active wiretapping
  - The intruder has to intercept all communication between the 2 legitimate parties
  - The intruder filters or rewrites traffic for his benefit

DNS POISONING

- For efficiency, a DNS server builds a cache of recently used domain names
- Attackers try to insert inaccurate entries into that cache
- Future requests are redirected to an address the attacker has chosen

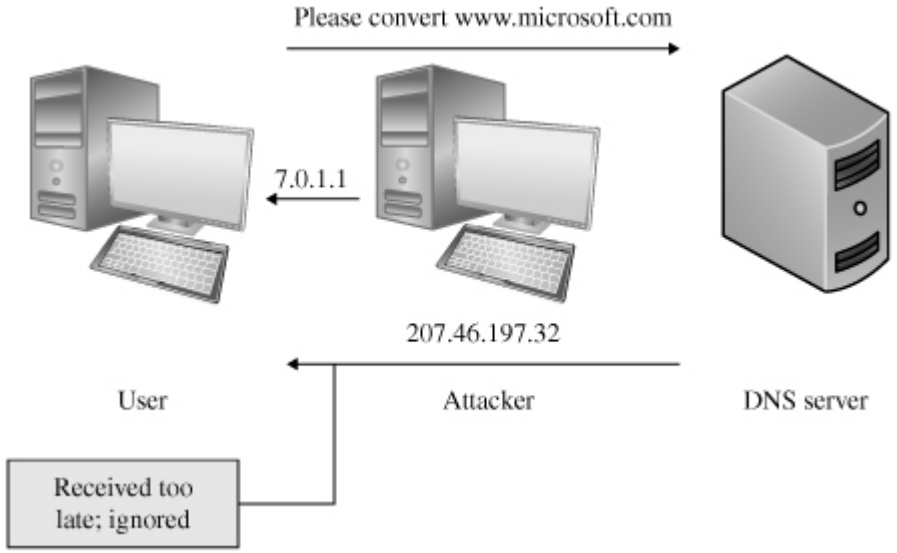


DNS SPOOFING



- A standard DNS query and response
- The user requests a translation of the URL microsoft.com
- The name server responds with the address 207.46.197.32

DNS SPOOFING



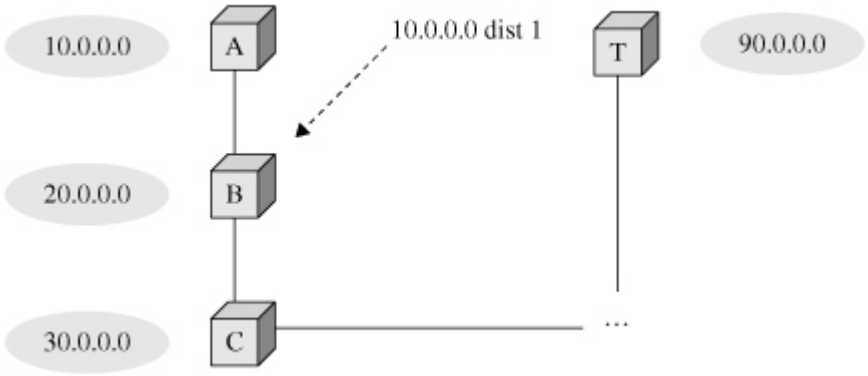
- A man-in-the-middle attack involves the attacker's intercepting and replying to a query before the real DNS server can respond
- The attacker can enter into the middle of the user's communication with www.microsoft.com

REROUTING ROUTING

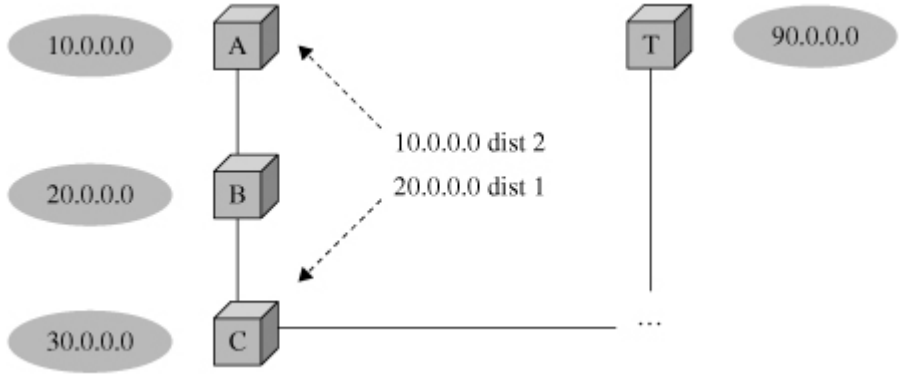
One node redirecting a network
so that all traffic flows
through the attacking node,
leading to a potential for interception

- Each router sends a message to other routers, listing addresses to which it has a path
- The other routers then add their paths and forward the extended list to the other routers as well
- In this way, all routers learn of the connection of other routers

REROUTING ROUTING

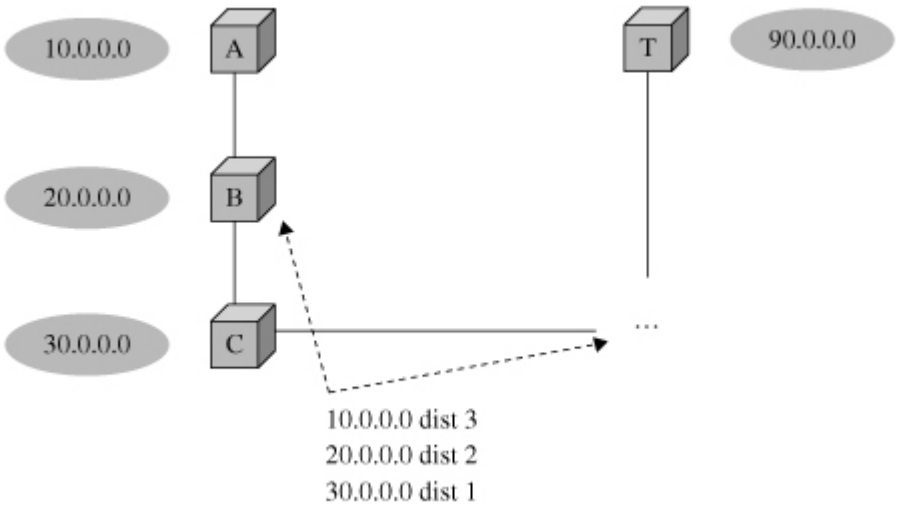


- A advertises to its neighbors that it is a distance of 1 from any machine in the 10.0.0.0 subnet



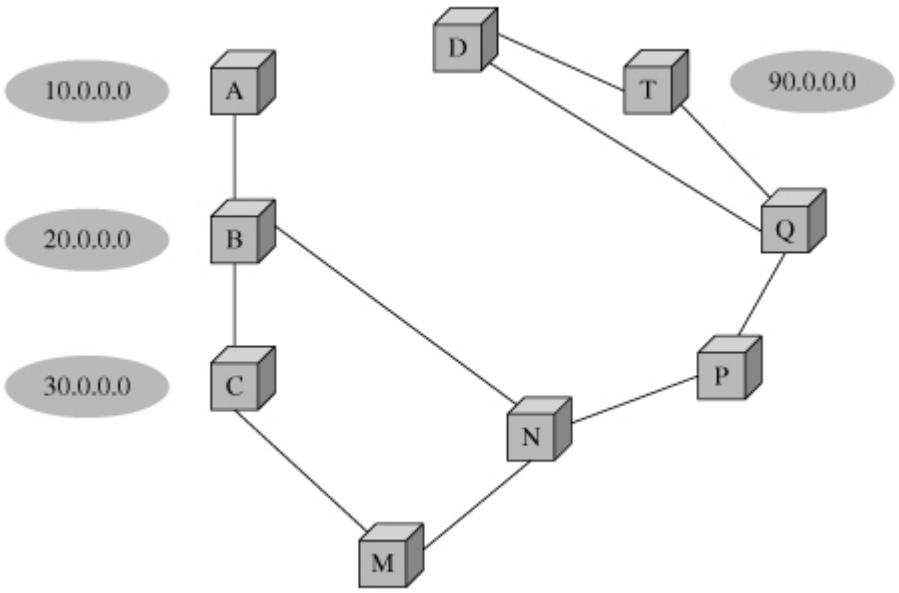
- B has just learned that router A is only distance 1 from the 10.0.0.0 subnet
  - B advertises to its neighbors A and C that it is distance 1 from its own subnet and distance 2 from the 10.0.0.0 subnet

REROUTING ROUTING



- C takes what it has just learned from B and broadcasts it to other routers adjacent to it
- Each router maintains a table of destination and next steps
  - If C had something for the 10.0.0.0 subnetwork, its table would indicate it should forward that data stream to B
- These routers will all advertise their connectivity, from which they can determine the shortest path between any pair of points

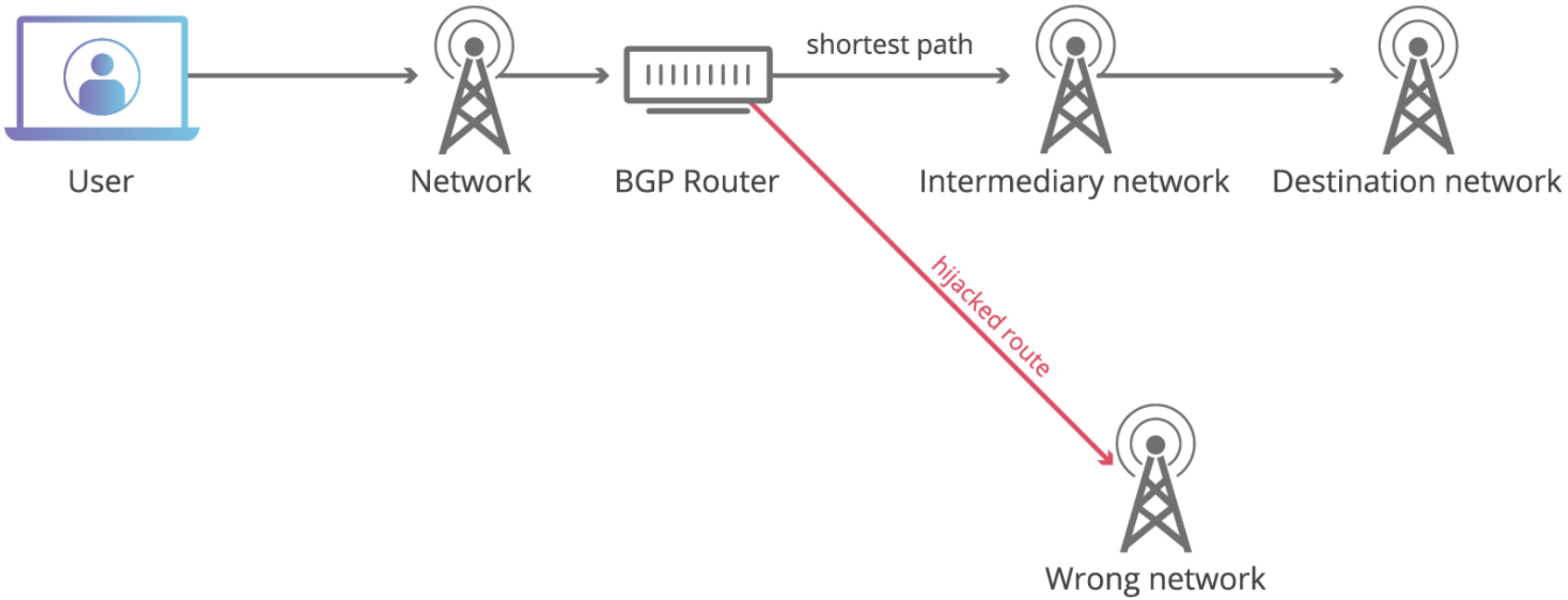
REROUTING ROUTING



- Routing tables can become corrupted from nonmalicious (and malicious) causes
  - Routers sometimes malfunction
  - Their administrators enter inaccurate data
- If router A advertised it was distance 1 from the 90.0.0.0 subnetwork, most traffic to that subnetwork would be routed to A
  - It could easily intercept and modify any traffic to that network

ROUTER TAKES OVER A NETWORK

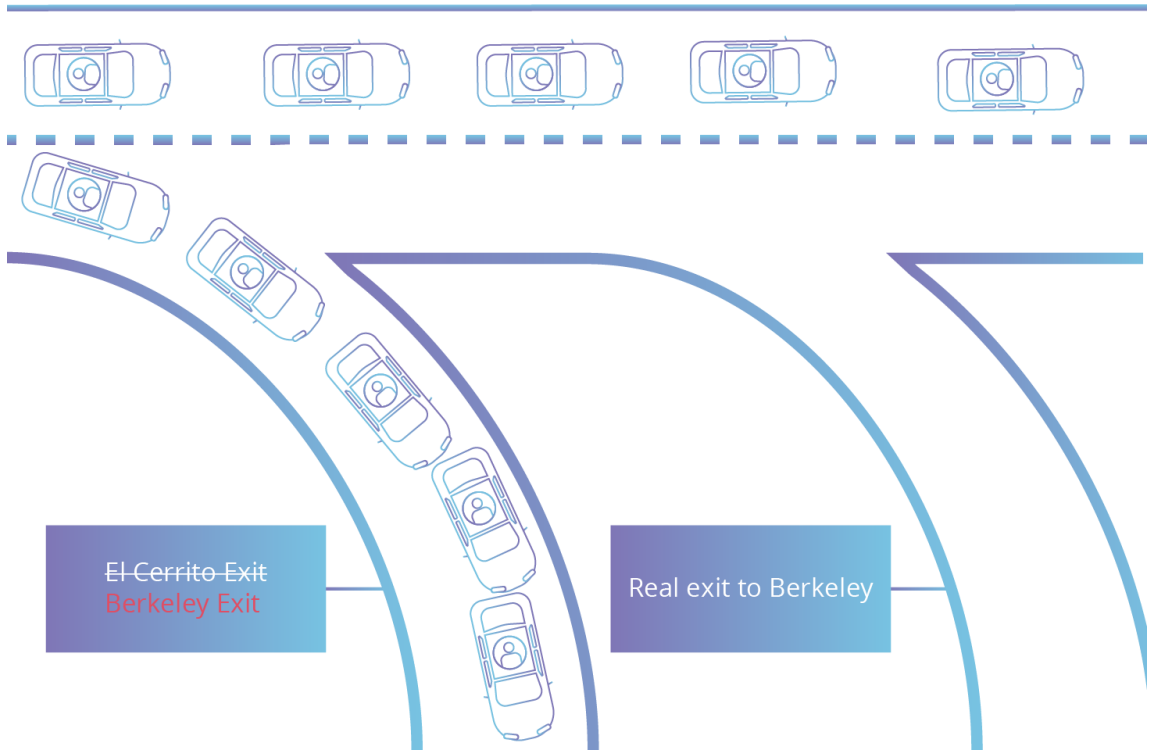
At the 2008 Defcon conference, most attendees were unaware that 2 researchers had rerouted the conference's wireless network through their equipment. The researchers described and demonstrated their attack.



BGP HIJACKING

A malicious rerouting of Internet traffic that exploits the trusting nature of BGP, the routing protocol of the Internet

- Internet traffic can go the wrong way, be monitored or intercepted, be 'black holed', or be directed to fake websites as part of a man-in-the-middle attack



SOURCE ROUTING

A sender can specify

some or all of the intermediate points

by which a data unit is transferred

Strict source routing

The complete path from source to destination is specified

Loose source routing

Certain (some or all) required intermediate points are specified

SOURCE ROUTING

To test or troubleshoot routers by forcing traffic

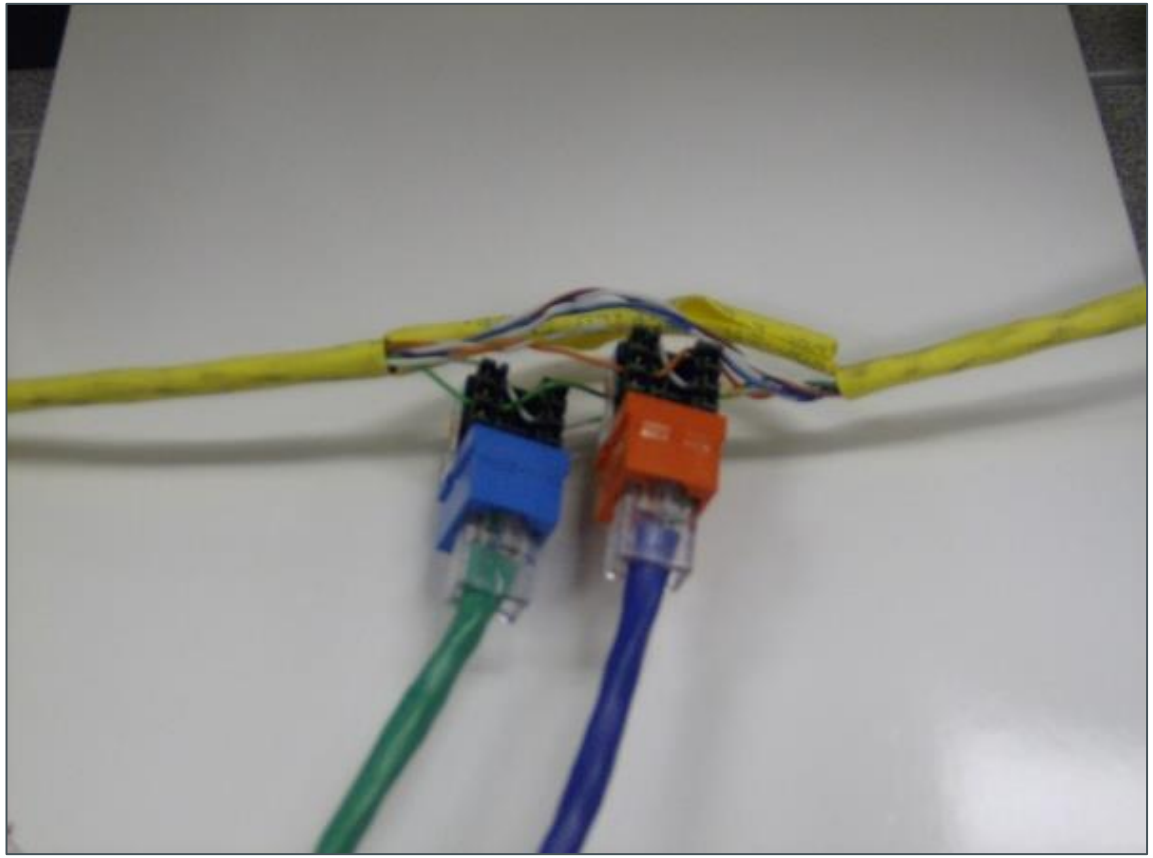
to follow a specific path that an engineer can then trace

To force data

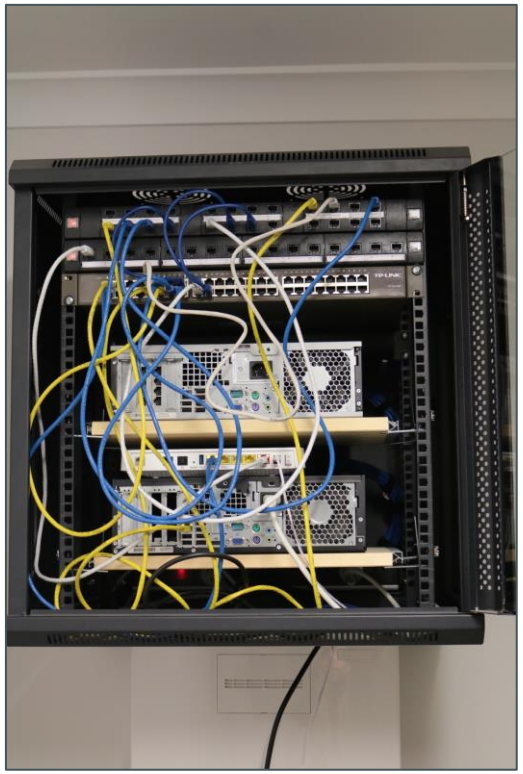
to flow through a malicious router or network link

PHYSICAL MAN IN THE MIDDLE

- Someone with wire cutters who physically had to cut a cable and splice in a second connection



NETWORK INTRUSION

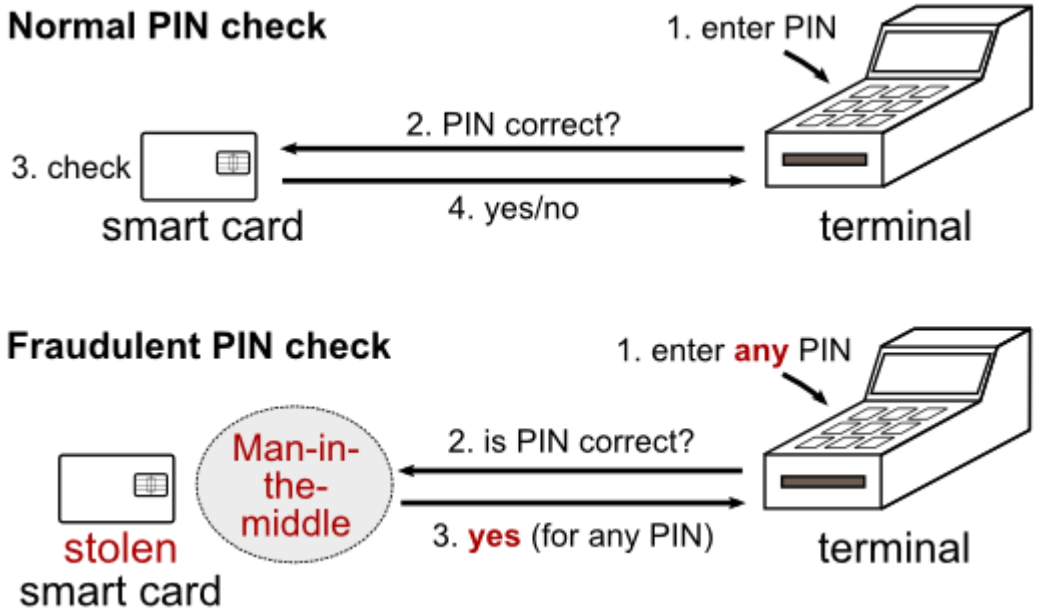


- Unmonitored, stand-alone collections of hardware
- An attacker can easily unplug the local network and add a second router between the network and the Internet router
- The attacker can connect other devices to the new router, and can then perform man-in-the-middle operations on all traffic to and from the original local network

MAN IN THE CREDIT CARD

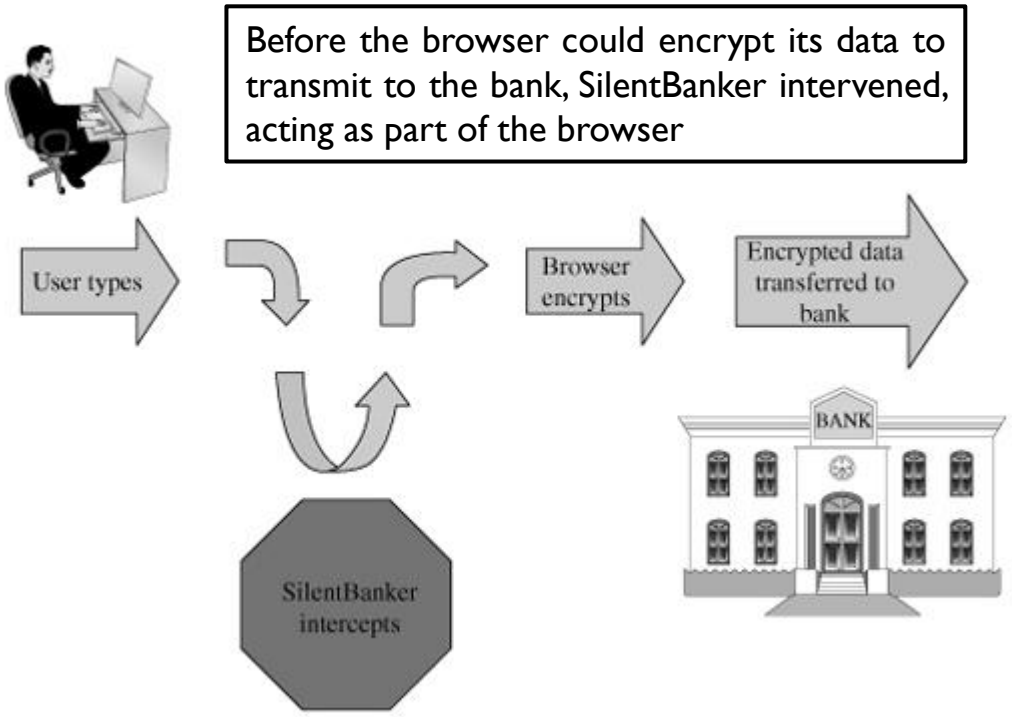
- Verification of the PIN
  - Locally by the card and terminal
  - Remotely (over an active network connection) by the bank that issued the card

- The middle agent intercepts the PIN, informs the card that verification is being done remotely, and informs the reader that the smartcard accepted the PIN

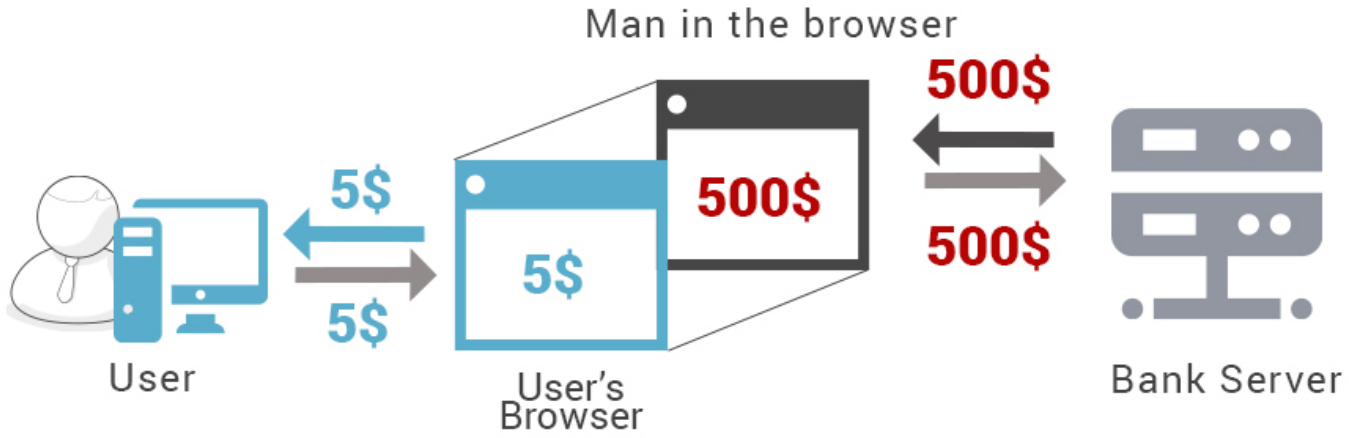


MAN-IN-THE-BROWSER ATTACK

- Malicious code that has infected a browser
- Code inserted into the browser can read, copy, and redistribute anything the user enters in a browser
- The attacker will intercept and reuse credentials to access financial accounts and other sensitive things



MAN-IN-THE-BROWSER ATTACK



- SilentBanker converted the request to make the transfer go to its own account
- When the bank returned its confirmation, SilentBanker changed the details before displaying them on the screen

MAN-IN-THE-PHONE ATTACK

PeskySpy

Intercepts digital audio traffic between the analog-to-digital decoder and Skype processing, before Skype can perform its encryption

Not specific to Skype

Because the interception occurs at the level of the audio driver, it will work against any voice-over-Internet program

PAGE-IN-THE-MIDDLE ATTACK

The attacker redirects the user,

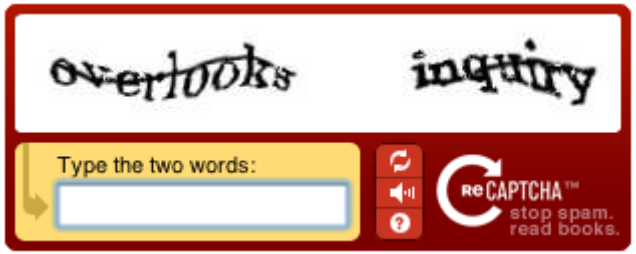
presenting fictitious web pages for the user to see

–

The attacker can capture the user's credentials

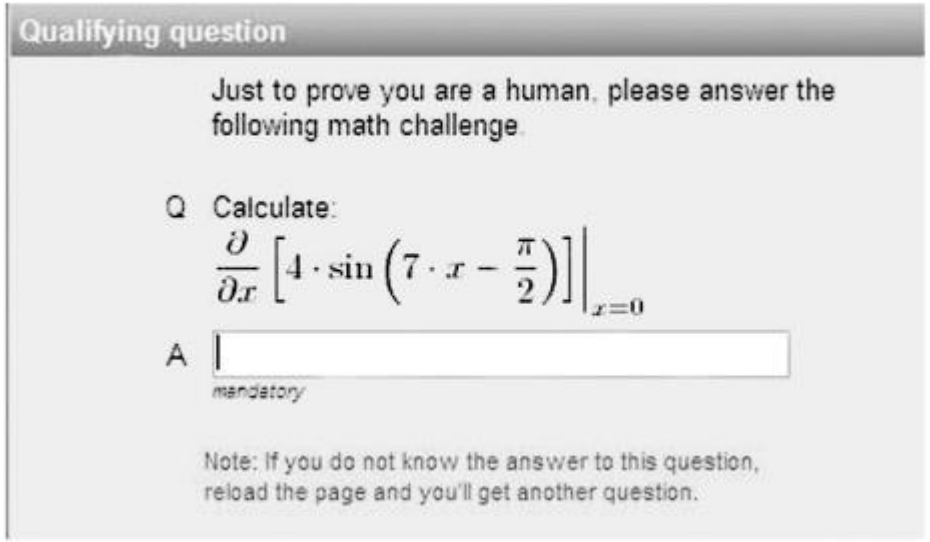
CAPTURING CAPTCHAS

- Completely Automated Public Turing test to tell Computers and Humans Apart
  - A puzzle that supposedly only a human can solve



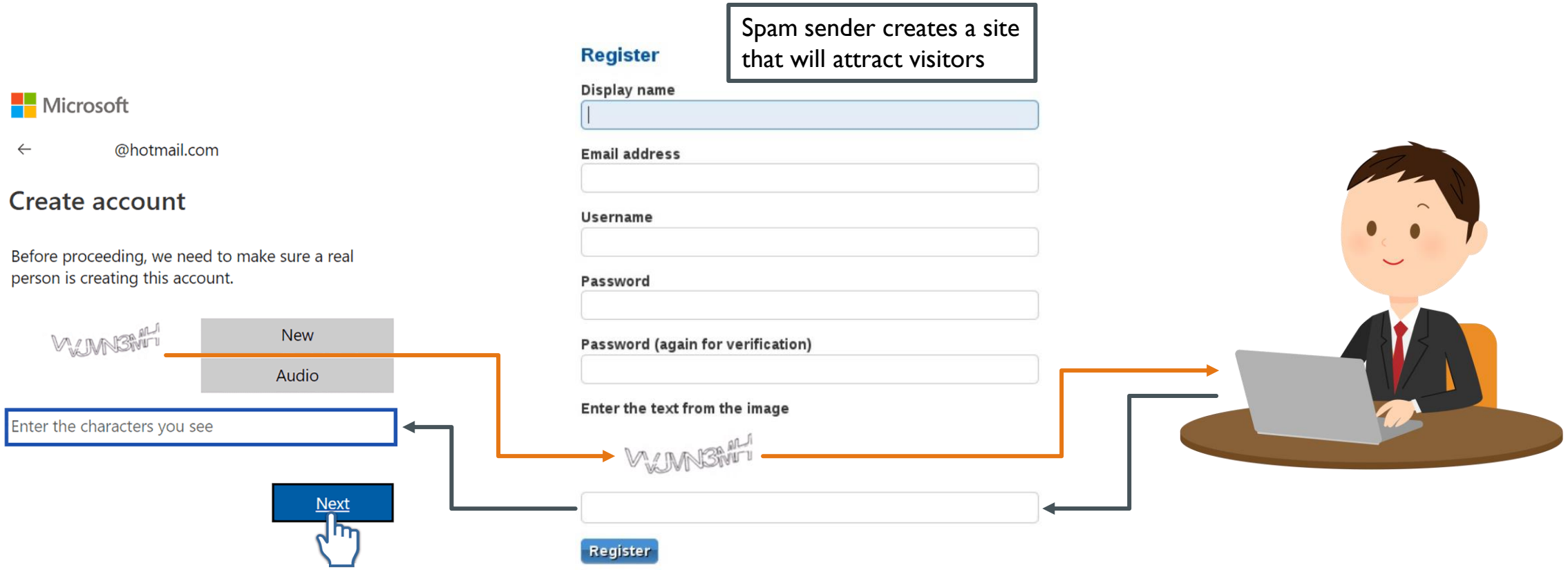
- Distortions are intended to defeat optical character recognition software that might be able to extract the characters

CAPTURING CAPTCHAS



- There is a fine line between what a human can still interpret and what is too distorted for pattern recognizers to handle

CAPTURING CAPTCHAS



UNWARRANTED TRUST

- The DNS attack and the BGP routing attacks both rely on failed trust
- Trust in the authenticity and correctness of a router's communications was implicit in the protocol's design

- The designers of the protocols knew 2 things
  - Pretending to be a router is difficult, so a message coming from a router is likely to really be from a router
  - For each router to map all paths independently through the Internet would be prohibitively time consuming

FAILED IDENTIFICATION AND AUTHENTICATION

- Usability and accuracy can conflict for identification and authentication
  - A more usable system may be less accurate

- In computer-to-computer interaction there are limited bases for authentication
  - Computer authentication is mainly based on what the computer knows (stored or computable data)
  - Stored data can be located by unauthorized processes, and what one computer can compute so can another

FAILED IDENTIFICATION AND AUTHENTICATION

- Malicious software can undermine authentication by eavesdropping on the authentication data and allowing it to be reused later
  - Well-placed attack code can also wait until a user has completed authentication and then interfere with the content of the authenticated session
- Each side of a computer interchange needs assurance of the authentic identity of the opposing side

UNAUTHORIZED ACCESS

The middle-man achieves access to data between 2 legitimate parties

–

The access is covert, not approved by the system,

but still the attacker has access

INADEQUATE ATTENTION TO PROGRAM DETAILS

- Programming requires great precision
  - Ignoring a small point may undermine the logic of an entire program, thus leading to program vulnerabilities
- Security requirements were dropped when not all requirements could be satisfied

PROTOCOL WEAKNESS

Failure to recognize a requirement in protocol design

(or similar requirements in system development)

also points to failing to think critically (failing to consider details)

TRUST

Monitoring

Detecting anomalies

Skepticism

Developed to limit trust

IDENTIFICATION AND AUTHENTICATION

Shared Secret

Something only the 2 entities on the end should know

- Mother's maiden name
- A secret verification number imprinted on a credit card
- Questions presumably only the right person will know

IDENTIFICATION AND AUTHENTICATION

One Time Password

The two end parties need to have a shared secret list of passwords

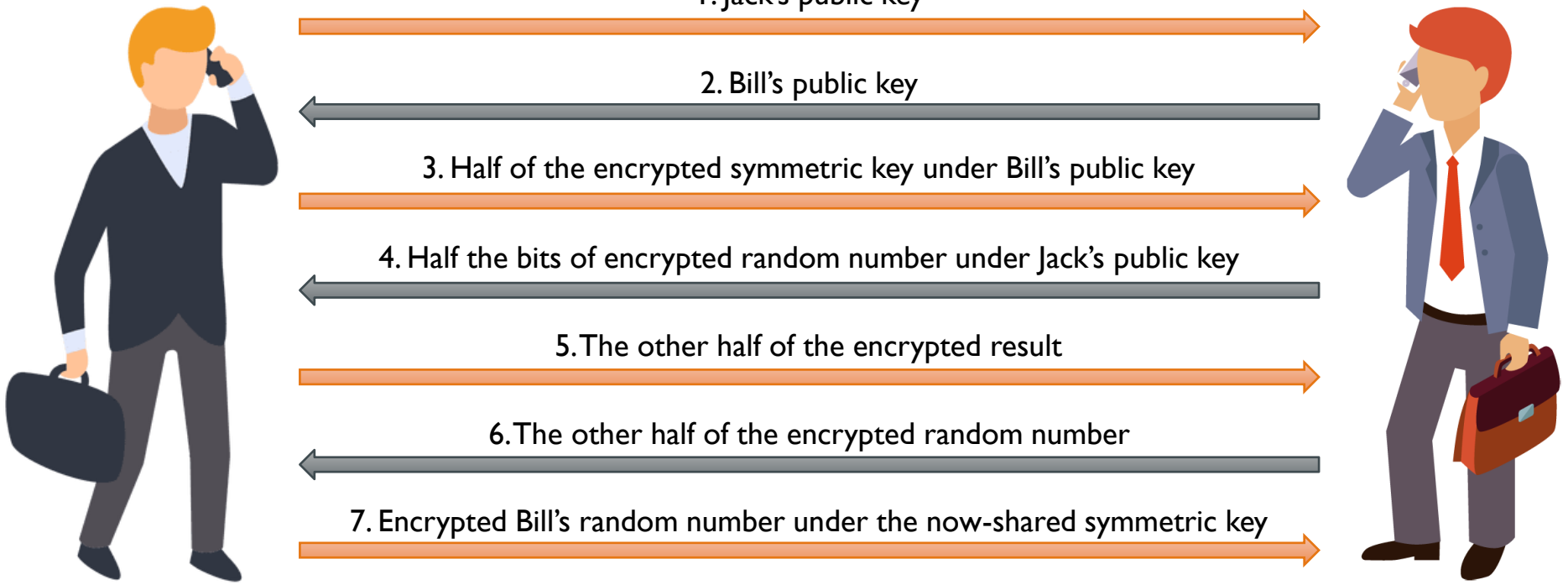
IDENTIFICATION AND AUTHENTICATION

Out-of-Band Communication

Transferring one fact along a communication path separate from that of another fact

- Bank card PINs are always mailed separately from the bank card
- If a customer calls a bank about having forgotten a PIN, the bank does not simply provide a new PIN in that conversation over the phone
  - The bank mails a separate letter containing a new PIN

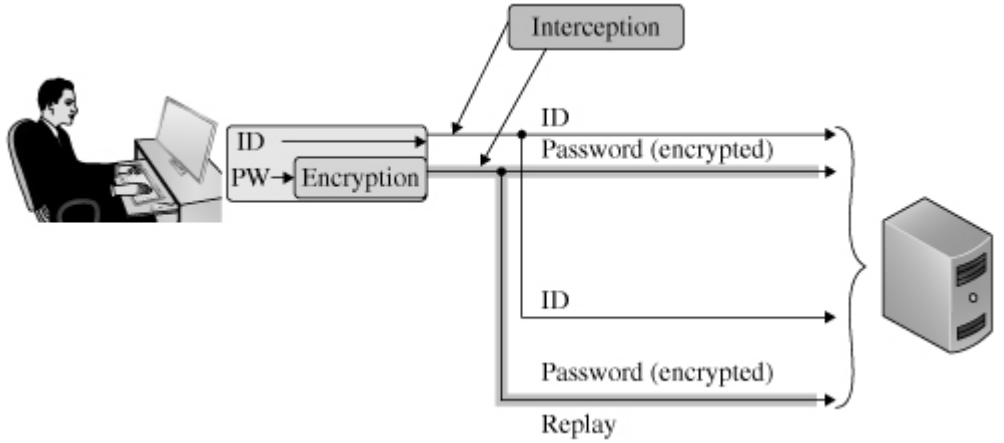
CRYPTOGRAPHY:
REVISED KEY EXCHANGE PROTOCOL – RIVEST & SHAMIR



Bill decrypts Jack's transmission with the symmetric key
and compares it to the random number he selected.
A match confirms the validity of the exchange.

REPLAY ATTACKS

Legitimate data are intercepted and reused, generally without modification



Even without knowing the password, if the attacker can interject the encrypted password into the communications line, the attacker can impersonate a valid user

REUSE OF SESSION DATA

The weakness exploited in replay attacks is inability to detect old, repeated, or used data

UNREPEATABLE PROTOCOL

Liveness

- A live, or one-time, password

Liveness Beacon: a signal that demonstrates that a data stream comes from an active source

- A blinking light in the video camera's field of view
- Time and date on security cameras' images

Sequence Number

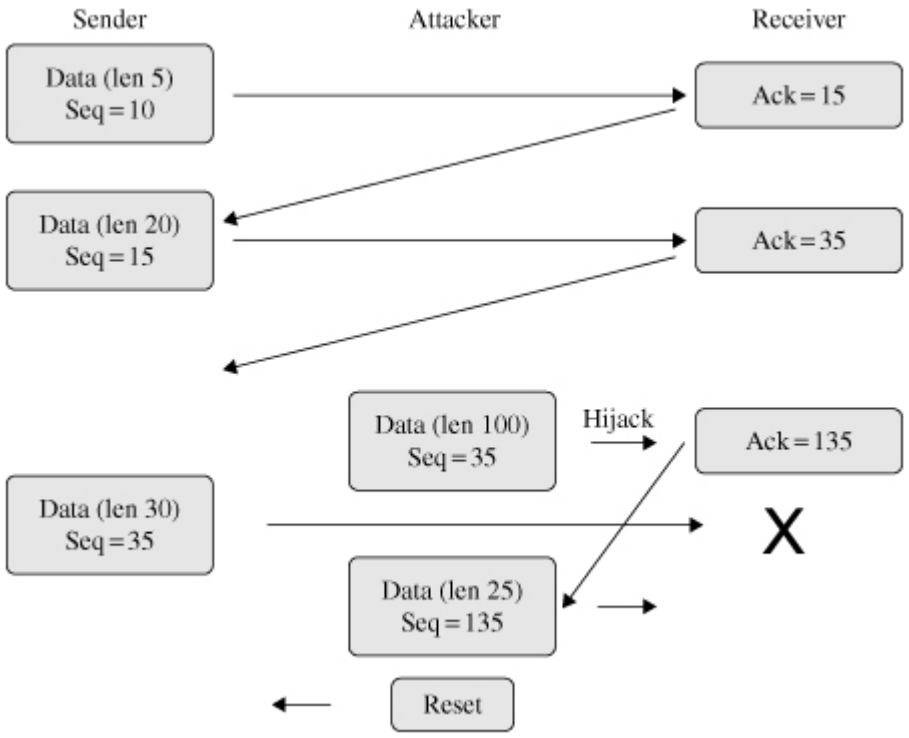
- TCP protocols use sequence numbers to ensure liveness in a communication session

UNREPEATABLE PROTOCOL

Nonce: an arbitrary random number

- One party chooses the nonce and sends it encrypted to the other
- The other decrypts it, performs a predefined operation on it (for example, adding 1 to it), and returns the reencrypted result to the originator
- A predefined operation performed on the nonce shows the recipient that the other party is actively involved in the interchange

SESSION HIJACK



- The attacker inserts a packet that maintains synchronization with the receiver but destroys synchronization with the real sender
- The attacker and the recipient are now resynchronized and continue the exchange begun by the original sender
- The attacker has surreptitiously slid into the session, taking the place of the original sender
- The attacker sends an RST command to the original sender, convincing the sender that the receiver has closed the original connection

SESSION HIJACK: VULNERABILITY

Electronic Impersonation

- Impersonation between 2 computing systems
- In many systems, identification and authentication are performed once, at the beginning of a transaction

Nonsecret Token

- Large tokens are difficult – but not impossible – to predict, guess, or intercept

SSH ENCRYPTION

- SSH (secure shell) provides an authenticated and encrypted path to the shell or operating system command interpreter

- Protects against spoofing attacks and modification of data in communication

SSL AND TLS ENCRYPTION

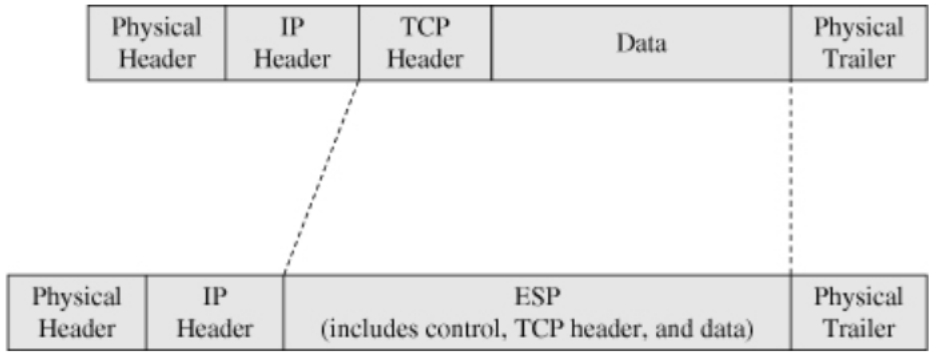
- SSL (Secure Sockets Layer) protects communication between a web browser and server
- SSL 3.0 was upgraded and named TLS (Transport Layer Security)
- Implemented at level 4 in the OSI network model
- Operates between applications (such as browsers) and the TCP/IP protocols to provide server authentication, optional client authentication, and an encrypted communication channel between client and server
- Because SSL is commonly used with web pages, it is often represented as HTTPS (HTTP Secure)

IPSEC

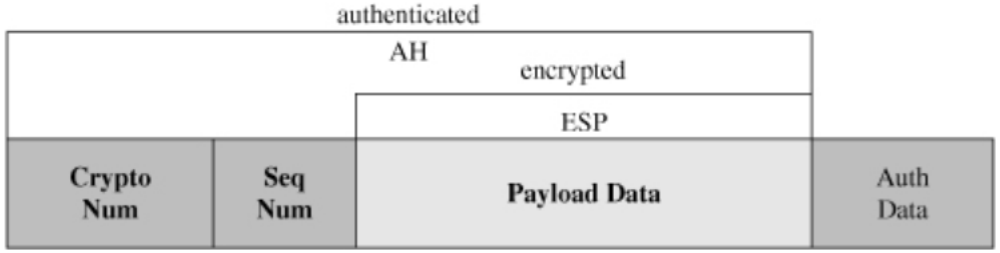
- Designed to address fundamental shortcomings such as being subject to spoofing, eavesdropping, and session hijacking
- Defines a standard means for handling encrypted data
- Implemented at the IP layer (3), it protects data produced in all layers above it, in particular, TCP and UDP control information, as well as the application data
- Fundamental data structures: authentication header (AH) and encapsulated security payload (ESP)

IPSEC

- The ESP (encapsulated security payload) replaces / includes the conventional TCP header and data portion of a packet

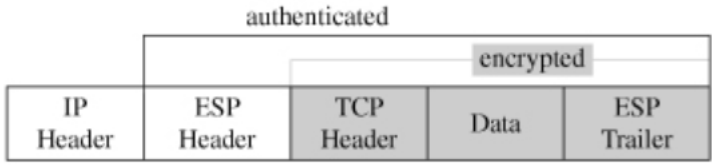


- The ESP contains both an authenticated portion and an encrypted portion



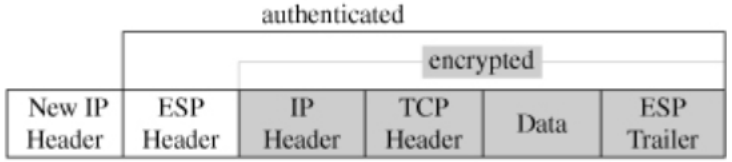
IPSEC: MODES OF OPERATION

Transport Mode



- The IP address header is unencrypted

Tunnel Mode



- The recipient's address is concealed by encryption
- IPsec substitutes the address of a remote device, such as a firewall, that will receive the transmission and remove the IPsec encryption

REFERENCES

- Pfleeger, Charles P. and Shari Lawrence Pfleeger (2012), *Analyzing Computer Security*, 1st Edition, Prentice Hall.

NEXT WEEK: DENIAL-OF-SERVICE ATTACKS

- Threat
  - Denial of Service
  - Flooding
  - Blocked Access
  - Access Failure
- Vulnerability
  - Insufficient Resources
  - Addressee Cannot Be Found
  - Exploitation of Known Vulnerability
  - Physical Disconnection
- Countermeasure
  - Network Monitoring and Administration
  - Intrusion Detection and Prevention Systems
  - Management
- Distributed Denial of Service

AS THE WORLD IS INCREASINGLY INTERCONNECTED, EVERYONE SHARES THE RESPONSIBILITY OF SECURING CYBERSPACE

Vision

To become an **outstanding** undergraduate Computer Science program that produces **international-minded** graduates who are **competent** in software engineering and have **entrepreneurial spirit** and **noble character**.

INFORMATIKA
UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA

Mission

1. To conduct studies with the best technology and curriculum, supported by professional lecturer
2. To conduct research in Informatics to promote science and technology
3. To deliver science-and-technology-based society services to implement science and technology