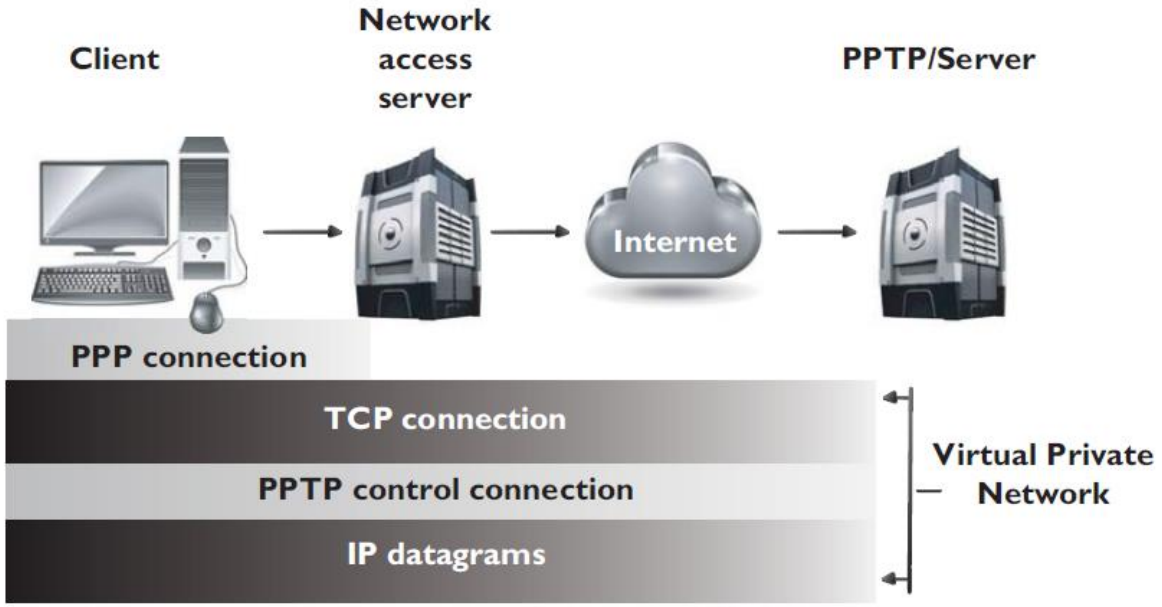
SENG 460

Practice of Information Security and Privacy

Telecommunications and Network Security (II)

Remote Connection Security
- VPN Solutions – Network Layer

1) Point-To-Point Tunneling Protocol (PPTP) + IPSec: PPTP encapsulate **PPP** packets and extend a **PPP** connection through an IP network.
2) Layer 2 Tunneling Protocol (L2TP) + IPSec: L2TP tunnels PPP traffic over various network types (IP, ATM, X.25, etc.); thus, it is not just restricted to IP networks



Remote Connection Security
- PPTP vs. L2TP

1. If the Internet is an IP-based network, why do we even need PPP?
Answer: *The point-to-point telecommunication line devices that connect individual systems to the Internet do not understand IP, so the traffic that travels over these links has to be encapsulated in PPP.*

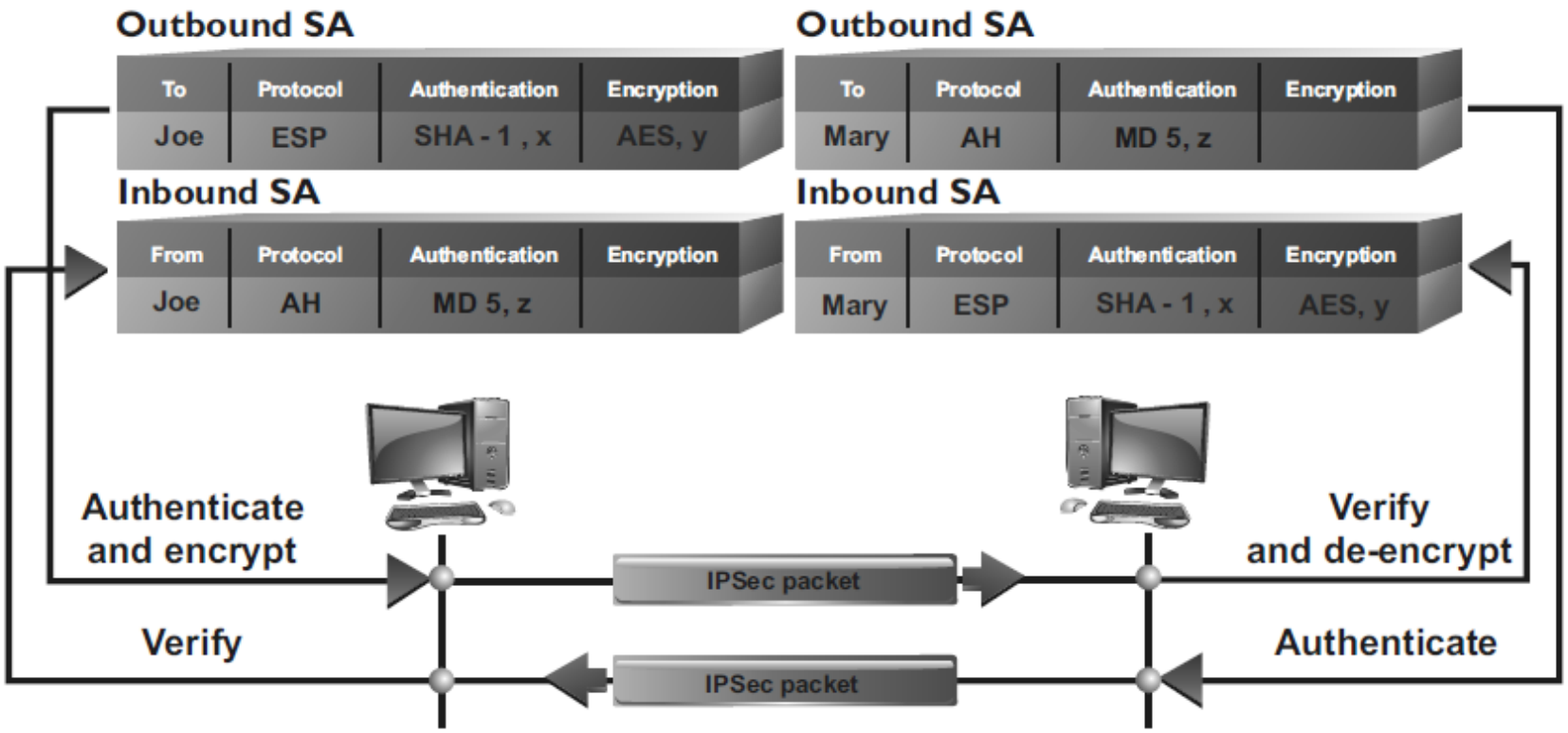
2. If PPTP and L2TP do not actually secure data themselves, then why do they exist?
Answer: *They extend PPP connections by providing a tunnel through networks that do not understand PPP.*

3. If PPTP and L2TP basically do the same thing, why choose L2TP over PPTP?
Answer: *PPTP only works over IP-based networks. L2TP works over IP-based and WAN-based (ATM, frame relay) connections. If a PPP connection needs to be extended over a WAN-based connection, L2TP must be used.*

4. If a connection is using IP, PPP, and L2TP, where does IPSec come into play?
Answer: *IPSec provides the encryption, data integrity, and system-based authentication.*

Remote Connection Security
- IPSec

IPSec is a suite of protocols that was developed to specifically protect IP traffic. IPv4 does not have any integrated security, so IPSec was developed to “bolt onto” IP and secure the data the protocol transmits. Where PPTP and L2TP work at the data link layer, IPSec works at the network layer of the OSI model.



Remote Connection Security
- VPN Solutions – Application Layer

3) Secure Sockets Layer (SSL): SSL works at the transport and session layers of the network stack and is used mainly to protect HTTP traffic.

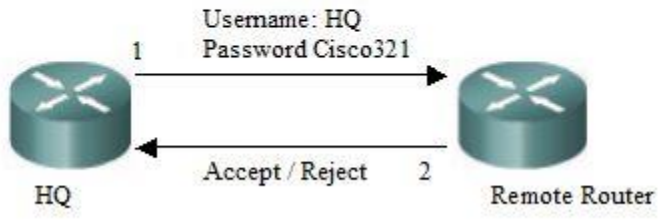
SSL Portal VPNs: An individual uses a single standard SSL connection to a web site to securely access multiple network services. The web site accessed is typically called a portal because it is a single location that provides access to other resources. The remote user accesses the SSL VPN gateway using a web browser, is authenticated, and is then presented with a web page that acts as the portal to the other services.

SSL Tunnel VPNs: An individual uses a web browser to securely access multiple network services, including applications and protocols that are not web-based, through an SSL tunnel. This commonly requires custom programming to allow the services to be accessible through a web-based connection.

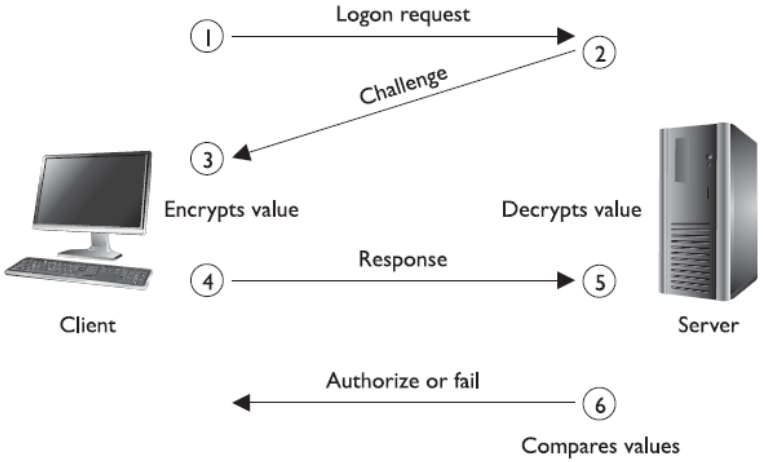
Remote Connection Security
- Remote Authentication Protocols

Password Authentication Protocol (PAP)

PAP 2-way handshake



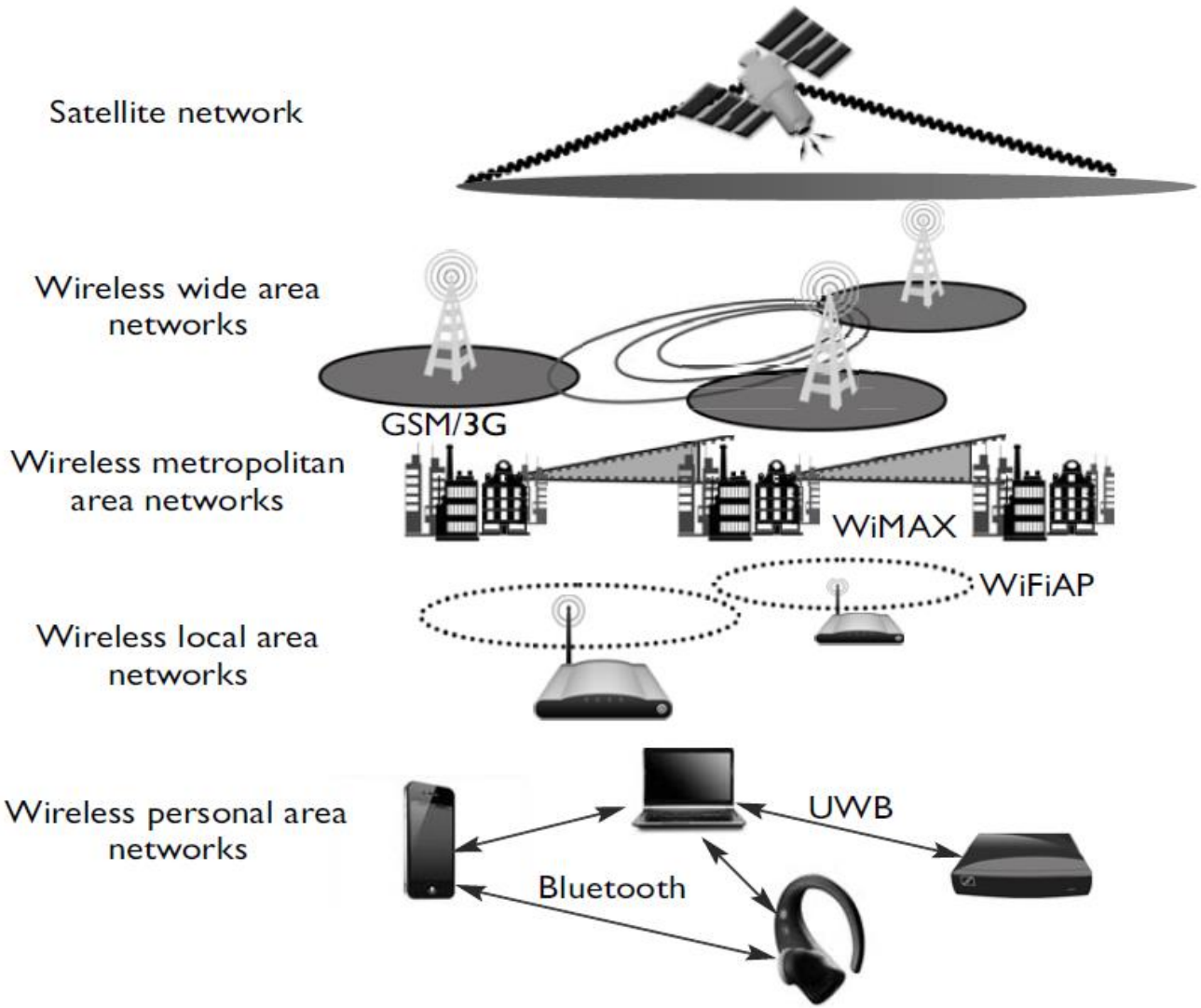
Challenge Handshake Authentication Protocol (CHAP)



Extensible Authentication Protocol (EAP)

Protocol	Description
Lightweight EAP (LEAP)	Wireless LAN authentication method developed by Cisco Systems
EAP-TLS	Digital certificate-based authentication
EAP-MD5	Weak system authentication based upon hash values
EAP-PSK	Provides mutual authentication and session key derivation using a preshared key
EAP-TTLS	Extends TLS functionality
EAP-IKE2	Provides mutual authentication and session key establishment using asymmetric or symmetric keys or passwords
PEAPv0/EAP-MSCHAPv2	Similar in design to EAP-TTLS; however, it only requires a server-side digital certificate
PEAPv1/EAP-GTC	Cisco variant-based on Generic Token Card (GTC) authentication
EAP-FAST	Cisco-proprietary replacement for LEAP based on Flexible Authentication via Secure Tunneling (FAST)
EAP-SIM	For Global System for Mobile Communications (GSM), based on Subscriber Identity Module (SIM), a variant of PEAP for GSM
EAP-AKA	For Universal Mobile Telecommunication System (UMTS) Subscriber Identity Module (USIM) and provides Authentication and Key Agreement (AKA)
EAP-GSS	Based on Generic Security Service (GSS), it uses Kerberos

Wireless Security
- Wireless Transmission Types



Wireless Security
- WLAN Elements

- **Access Point (AP):** a transceiver which connects to an wired network.
- ***Service Set ID (SSID)***: AP's identification information.
- **Wireless Devices:** devices that communicates with AP.
- **Channel:** a certain frequency within a given frequency band. The AP is configured to transmit over a specific channel, and the wireless device will "tune" itself to be able to communicate over this same frequency.

Wireless Security
- WLAN Security

- **Wired Equivalent Privacy (WEP):**
  - CHAP for authentication
  - RC4 Cipher with pre-shared key + IV for encryption
  - No data integrity protection

- **Wi-Fi Protected Access (WPA):**
  - EPA for authentication
  - Temporal Key Integrity Protocol (TKIP) for encryption (rotate encryption keys for each data frame)
  - Use message authentication code (MAC) for data integrity

- **Wi-Fi Protected Access II (WPA2):**
  - EPA for authentication
  - CCMP for encryption (an AES-based encryption mode)
  - CCMP for data integrity

Wireless Security
- Bluetooth Security

Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth.

User Recommendations

- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

Developer Recommendations

- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Use configuration and link activity indicators like LEDs or desktop icons.
- Use non-descriptive Bluetooth device names on each device and identify all paired and connected Bluetooth devices by hardware (MAC) address.
- Require user authorization for all incoming connection requests, and don't accept connections, files, or other objects from unknown, untrusted sources.

Wireless Security
- Bluetooth Security

Both users and Bluetooth application developers have responsibilities and opportunities to minimize the risk of compromise via Bluetooth.

Recommendations to Users

- Make devices discoverable (visible to other Bluetooth devices) only if/when absolutely necessary.
- Make devices connectable (capable of accepting and completing incoming connection requests) only if/when absolutely necessary and only until the required connection is established.
- Pair Bluetooth devices in a secure area using long, randomly generated passkeys. Never enter passkeys when unexpectedly prompted for them.
- Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

Recommendations to Developers

- Passkeys should be at least eight digits long. Passkeys must not be valid indefinitely.
- Use configuration and link activity indicators like LEDs or desktop icons.
- Use non-descriptive Bluetooth device names on each device and identify all paired and connected Bluetooth devices by hardware (MAC) address.
- Require user authorization for all incoming connection requests, and don't accept connections, files, or other objects from unknown, untrusted sources.

Wireless Security
- Mobile Device Security

Mobile devices, if not properly managed, can compromise security in enterprise environment. The following is a short list of items that should be put into place for enterprise mobile device security:

- Only devices that can be centrally managed should be allowed access to corporate resources.
- Remote policies should be pushed to each device, and user profiles should be encrypted with no local options for modification.
- Data encryption, idle timeout locks, screen-saver lockouts, authentication, and remote wipe should be enabled.
- Bluetooth capabilities should be locked down, only allowed applications can be installed, camera policies should be enforced, and restrictions for social media sites (Facebook, Twitter, etc.) should be enabled.
- Endpoint security should expand to mobile endpoints.
- Implement 802.1X on wireless VoIP clients on mobile devices.

Network Threats & Countermeasures
- ICMP Attacks

- **Ping of Death:** a type of DoS attack in which oversized ICMP packets are sent to the victim, which may freeze or reboot the vulnerable machines.
- **Smurf:** the attacker sends an ICMP ECHO REQUEST packet with a spoofed source address to a victim's network broadcast address. This means that each system on the victim's subnet receives an ICMP ECHO REQUEST packet. Each system then replies to that request with an ICMP ECHO REPLY packet to the spoof address provided in the packets—which is the victim's address.
- **Port Scanning:** ICMP can be used to scan the network for open ports

The countermeasures to these types of attacks are to use firewall rules that only allow the necessary ICMP packets into the network and the use of IDS or IPS to watch for suspicious activities. Host-based protection (host firewalls and host IDS) can also be installed and configured to identify this type of suspicious behavior.

Network Threats & Countermeasures
- Email Related Attacks

- **E-mail Spoofing:** sending an email that appears to come from one source when it really comes from another.
- **Spear Phishing:** A phishing attack but targets on a specific person rather than a random set of people.
- **Spam:** Sending massive emails for profit.

The countermeasures to these types of attacks includes enabling SMTP authentication on the sending server, Implementing Sender Policy Framework (which validates emails data against pre-defined policy before delivering the email), enabling anti-spam services, and regulating with laws, etc.

Network Threats & Countermeasures
- Other Attacks

- **Eavesdropping:** sniffing data as it passes over a network. (***passive attacks)***
  - Encryption
- **Distributed Denial-of-service (DDoS) attack** An attacker is able to trigger large amounts of service requests to the victim's computer from a set of zombie machines.
  - Smart firewalls
- **Wardialing:** a brute force attack in which an attacker has a program that systematically dials a large bank of phone numbers with the goal of finding ones that belong to modems instead of telephones. These modems can provide easy access into an environment.
  - The countermeasures are to not publicize these telephone numbers and to implement tight access control for modems and modem pools.

Network Threats & Countermeasures
- Other Attacks

- **DNS Cache Poisoning:** provide a DNS server with incorrect information, which would point the victim to a malicious web site.
  - Limit the updates on DNS entries
- **URL Hiding:** Divert traffic to a fake website using embedded URLs.
  - Be cautious!
- **Session Hijacking:** Hijack a connection session to impersonate victims.
  - Protect session token!