Network Access Control and Cloud Security

Raj Jain
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

Audio/Video recordings of this lecture are available at:

http://www.cse.wustl.edu/~jain/cse571-14/

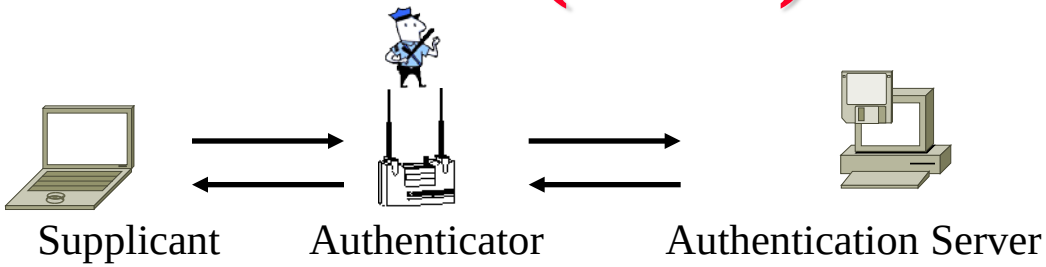
Overview

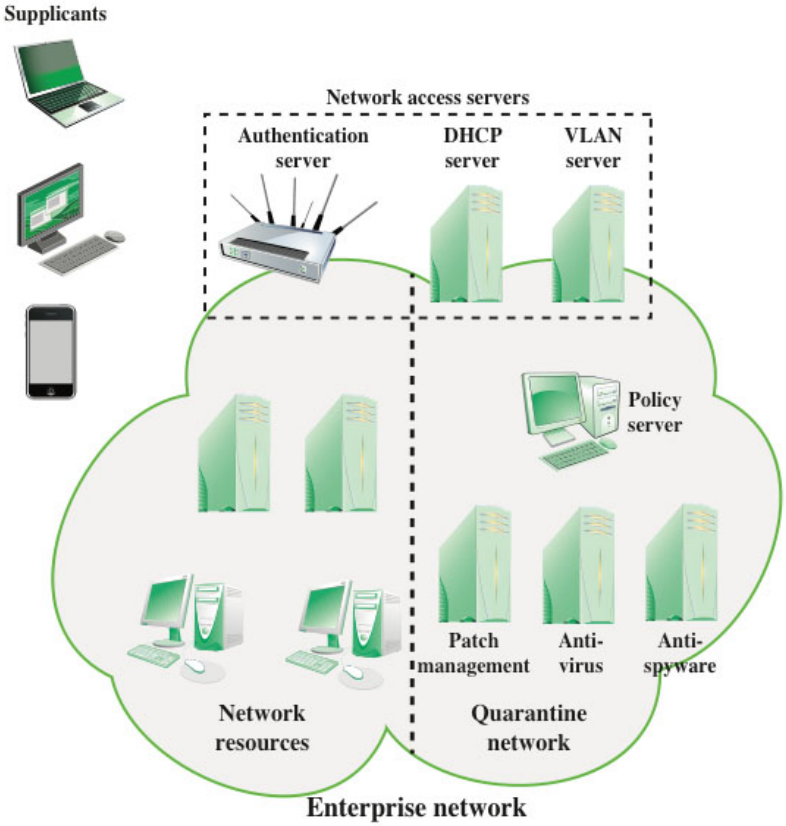
1. Network Access Control (NAC)
2. RADIUS
3. Extensible Authentication Protocol (EAP)
4. EAP over LAN (EAPOL)
5. 802.1X
6. Cloud Security

These slides are based partly on Lawrie Brown's slides supplied with William Stallings's book "Cryptography and Network Security: Principles and Practice," 6th Ed, 2013.

Network Access Control (NAC)

- **AAA**:
  - **Authentication**: Is user legit?
  - **Authorization**: What is he allowed to do?
  - **Accounting**: Keep track of usage
- Components:
  - **Supplicant**: User
  - **Authenticator**: Network edge device
  - **Authentication Server**: Remote Access Server (RAS) or Policy Server Backend policy and access control



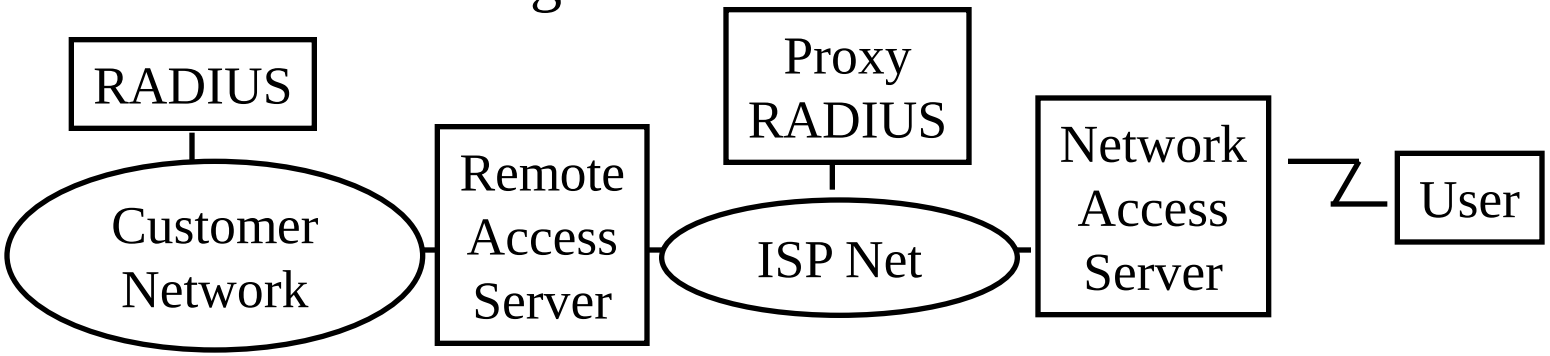


Network Access Enforcement Methods

- IEEE 802.1X used in Ethernet, WiFi
- Firewall
- DHCP Management
- VPN
- VLANs

RADIUS

- Remote Authentication Dial-In User Service
- Central point for Authorization, Accounting, and Auditing data ⇒ **AAA** server
- Network Access servers get authentication info from RADIUS servers
- Allows RADIUS Proxy Servers ⇒ ISP roaming alliances
- Uses UDP: In case of server failure, the request must be re-sent to backup ⇒ Application level retransmission required
  - TCP takes to long to indicate failure



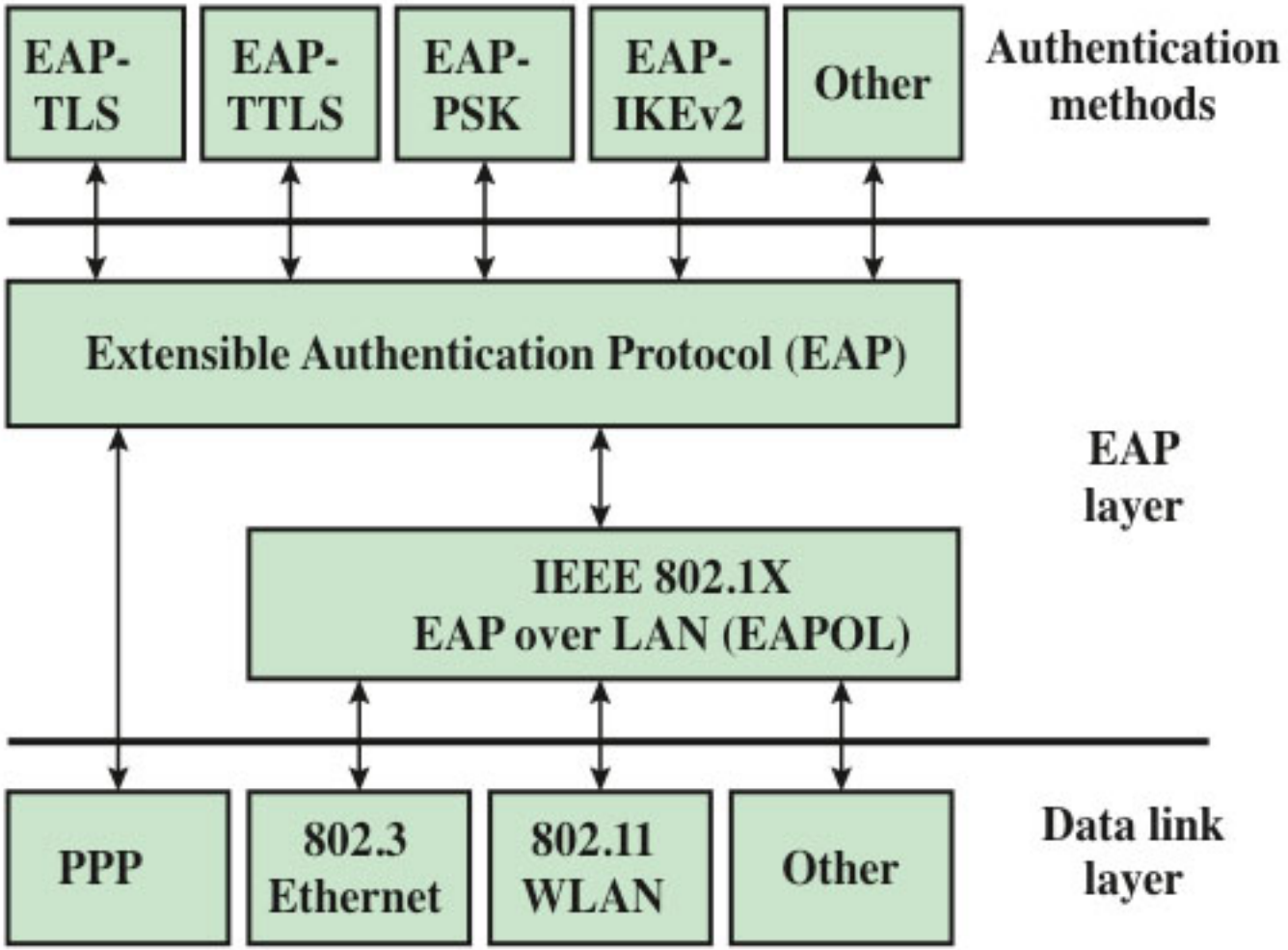
- Ref: http://en.wikipedia.org/wiki/RADIUS

Extensible Authentication Protocol (EAP)

- Old Methods: Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft CHAP (MS-CHAP
- Each authentication protocols required a new protocol ⇒ Extensible Authentication Protocol
- Allows using many different authentication methods
- Single-Step Protocol ⇒ Only one packet in flight ⇒ Duplicate Elimination and retransmission Ack/Nak ⇒ Can run over lossy link
- No fragmentation. Individual authentication methods can deal with fragmentation. One frag/round trip ⇒ Many round trips
- Allows using a backend authentication server ⇒ Authenticator does not have to know all the authentication methods
- Can run on any link layer (PPP, 802, ...). Does not require IP.
- RFC 3748, "EAP," June 2004.

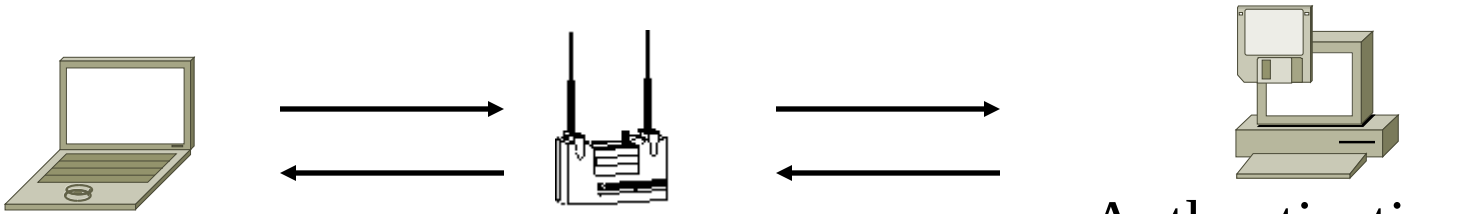
Ref: http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol

EAP (Cont)


EAP-TLS
EAP-TTLS
EAP-PSK
EAP-IKEv2
Other
Authentication methods
Extensible Authentication Protocol (EAP)
EAP layer
IEEE 802.1X
EAP over LAN (EAPOL)
PPP
802.3 Ethernet
802.11 WLAN
Other
Data link layer

EAP Terminology

- Peer: Entity to be authenticated = Supplicant
- Authenticator: Authenticating entity at network boundary
- Authentication Server: Has authentication database
- EAP server = Authenticator if there is no backend Authentication Server otherwise authentication server
- Master Session Key (MSK)= Keying material agreed by the peer and the EAP server. At least 64b. Generally given by the server to authenticator.

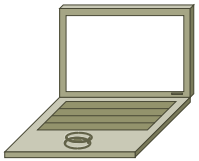


EAP Exchange

- EAP Message Format:

Code	Identifier	Length	[Type]	Data
8b	8b	16b	8b	

- Only four message codes:



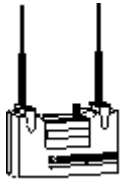
Supplicant

Request (01)

Response (02)

Success (03)

Failure (04)



Authenticator

- Identifier is incremented for each message.
  Identifier in response is set equal to that in request.
- Type field in the request/response indicates the authentication.
  Assigned by Internet Assigned Number Authority (IANA)

EAP Types

1 = Identity

2 = Notification (messages to be displayed to user)

3 = Nak

4 = MD5 Challenge (CHAP)

5 = One time password

6 = Generic Token card (GTC)

254 = Expanded types (allows vendor specific options)

255 = Experimental

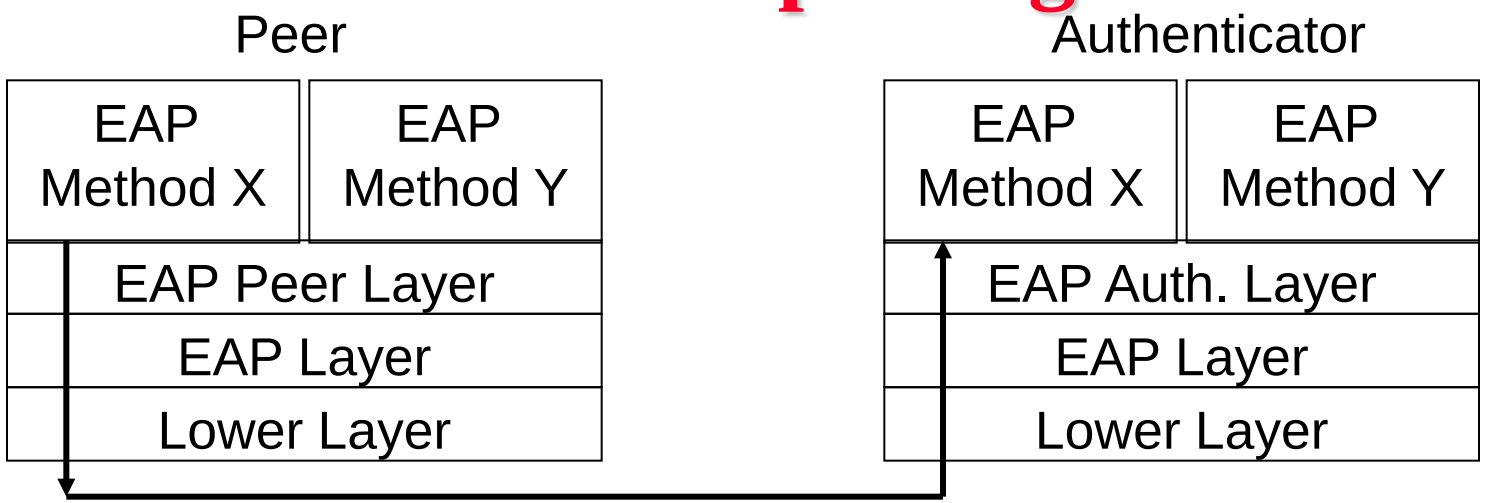
Notification requests are responded by notification responses.

Nak type is valid only for responses.

Expanded types include a 3B vendor ID and 4B vendor msg type.

Expanded Nak is used in response to requests of type 254 and may include alternative suggestions for methods.

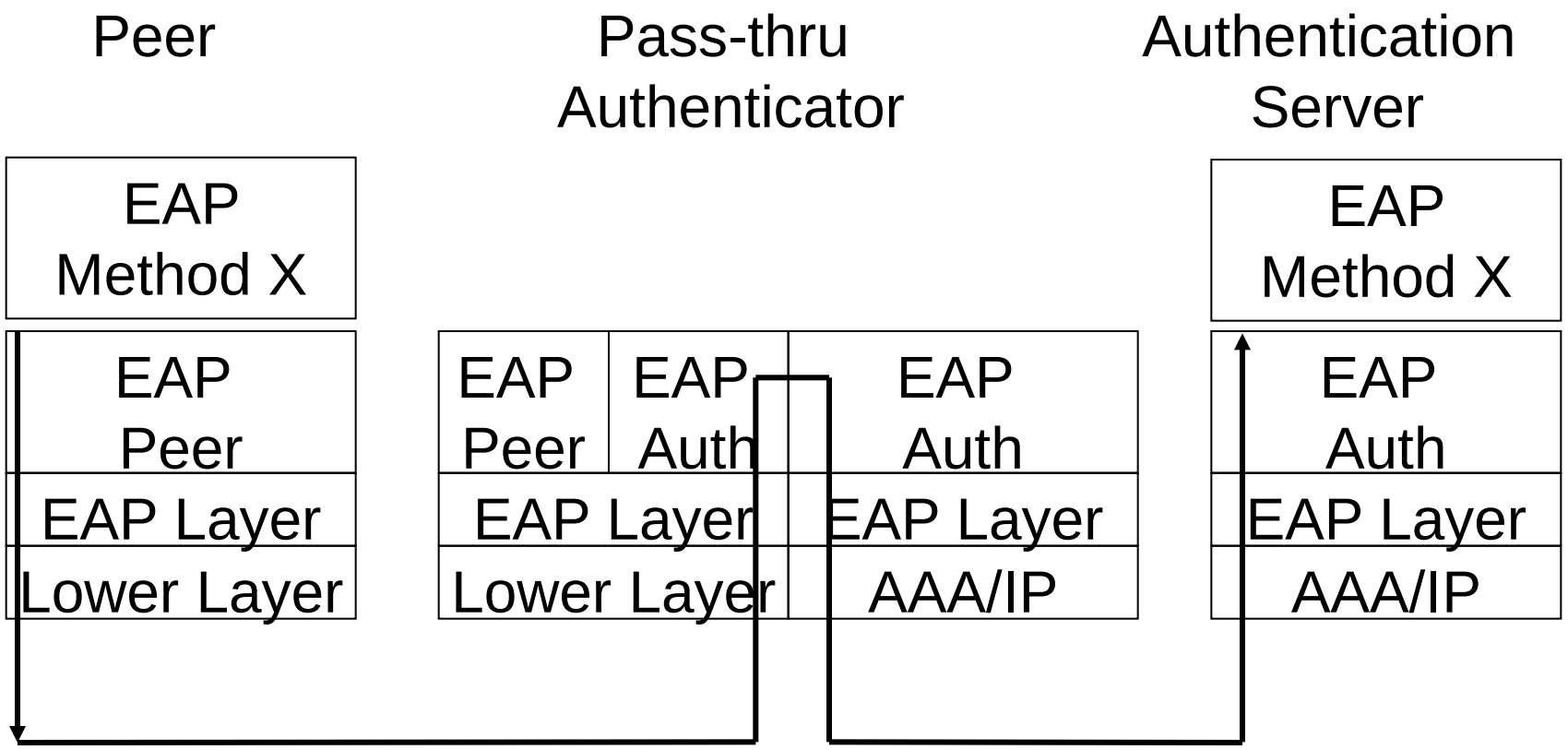
EAP Multiplexing Model



- EAP Layer demultiplexes using code. Code 1 (request), 3 (success), and 4 (failure) are delivered to the peer layer
- Code 2 (response) is delivered to the EAP authenticator layer.
- Both ends may need to implement peer layer and authenticator layer for mutual authentication
- Lower layer may be unreliable but it must provide error detection (CRC)
- Lower layer should provide MTU of 1020B or greater

Ref: RFC 3748

EAP Pass through Authenticator



- EAP Peer/Auth layers demultiplex using "type" field.

EAP Upper Layer Protocols

- Lightweight EAP (LEAP): Uses MS-CHAP. Not secure.
- EAP-TLS: Transport Level Security. Both sides need certificates
- EAP-TTLS: Tunneled TLS. Only server certificates. Secure tunnel for peer.
- EAP-FAST: Flexible Authentication via Secure Tunneling. Certificates optional. Protected tunnels.
- Protected EAP (PEAP): Server Certificates. Client password.
- PEAPv1 or EAP-GTC: Generic Token Cards. Client uses secure tokens.
- EAP-SIM: Subscriber Identity Module used in GSM. 64b keys.
- EAP-AKA: Authentication and Key Agreement. Used in 3G. 128b keys.
- EAP-PSK: Pre-shared key+AES-128 to generate keys
- EAP-IKEv2: Internet Key Exchange. Mutual authentication. Certificate, Password, or Shared secret

Ref: http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol

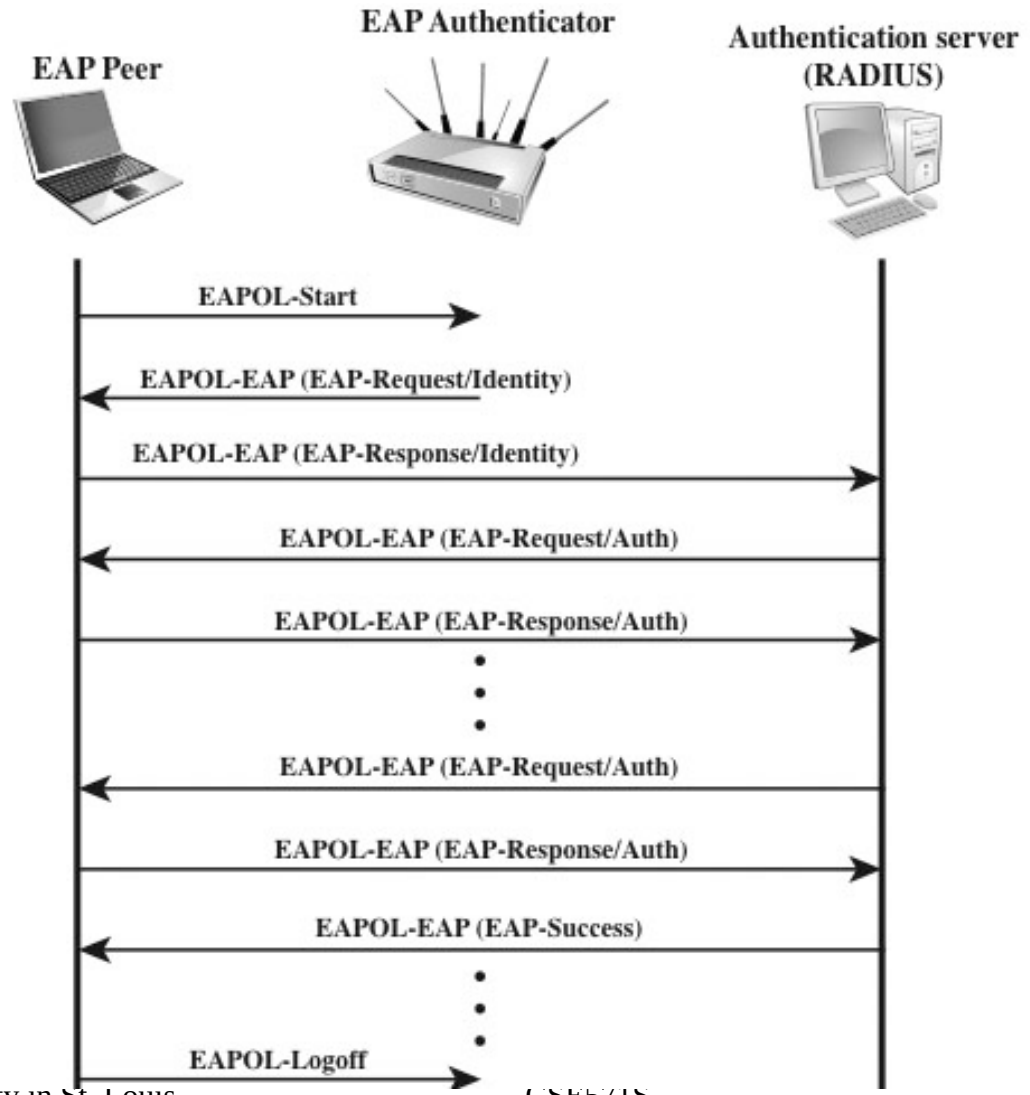
EAP over LAN (EAPOL)

- EAP was designed for Point-to-point line
- IEEE extended it for LANs ⇒ Defines EAPOL
- Added a few more messages and fields
- Five types of EAPOL messages:
  - EAPOL Start: Sent to a multicast address
  - EAPOL Key: Contains encryption and other keys sent by the authenticator to supplicant
  - EAPOL packet: Contains EAP message (Request, Response, Success, Failure)
  - EAPOL Logoff: Disconnect
  - EAPOL Encapsulated-ASF-Alert: Management alert
- Message Format: Version=1, Type=start, key, …,

Ethernet Header	Version	Type	Packet Body Len	Packet Body

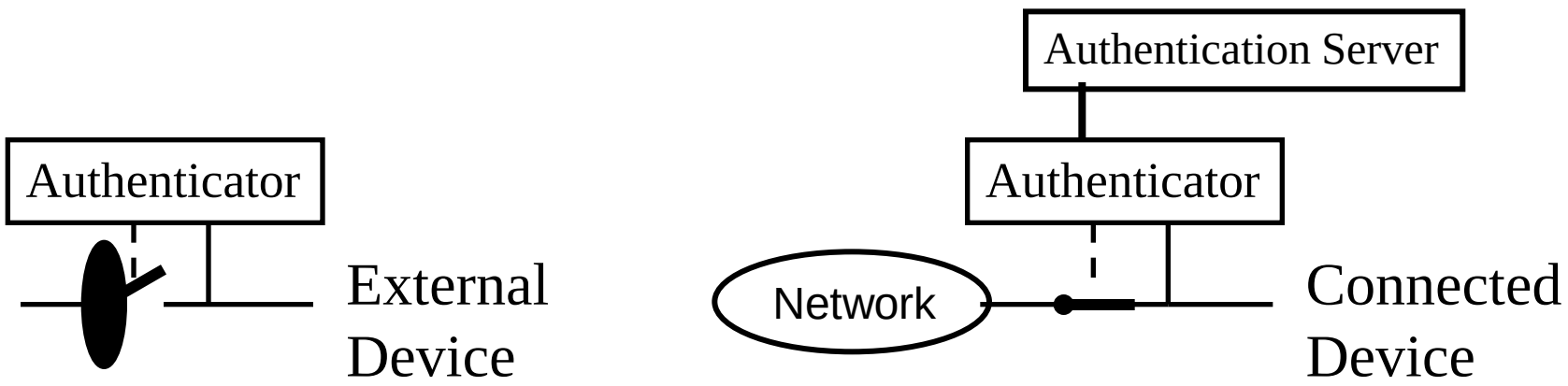
Ref: http://en.wikipedia.org/wiki/Eapol

EAPOL (Cont)


EAP Peer
EAP Authenticator
Authentication server
(RADIUS)
EAPOL-Start
EAPOL-EAP (EAP-Request/Identity)
EAPOL-EAP (EAP-Response/Identity)
EAPOL-EAP (EAP-Request/Auth)
EAPOL-EAP (EAP-Response/Auth)
EAPOL-EAP (EAP-Request/Auth)
EAPOL-EAP (EAP-Response/Auth)
EAPOL-EAP (EAP-Success)
EAPOL-Logoff

802.1X

- Authentication *framework* for IEEE802 networks
- Supplicant (Client), Authenticator (Access point), Authentication server
- No per packet overhead ⇒ Can run at any speed
- Need to upgrade only driver on NIC and firmware on switches
- User is not allowed to send any data until authenticated



Ref: http://en.wikipedia.org/wiki/802.1x

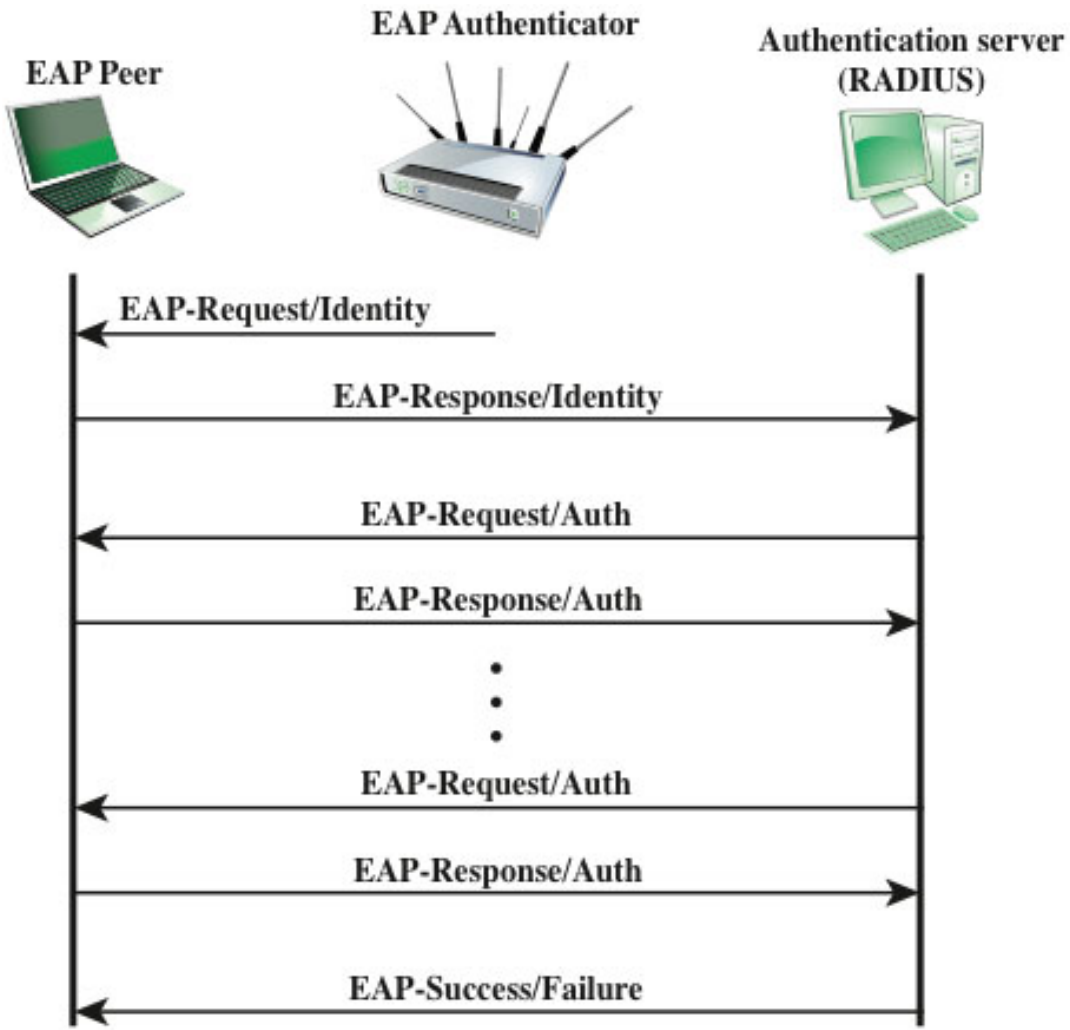
802.1X Authentication

Station | **Access Point** | **Authentication Server**

Can I connect please?	Associate ⇢	
What's your user name?	EAP Identity Request ⇠	
My user name is john	EAP Identity Response ⇢	EAP Identity Response ⇢
What's your password?	EAP Auth Request ⇠	EAP Auth Request ⇠
My password is mary?	EAP Auth Response ⇢	EAP Auth Response ⇢
You can connect!	EAP-Success ⇠	EAP-Success ⇠

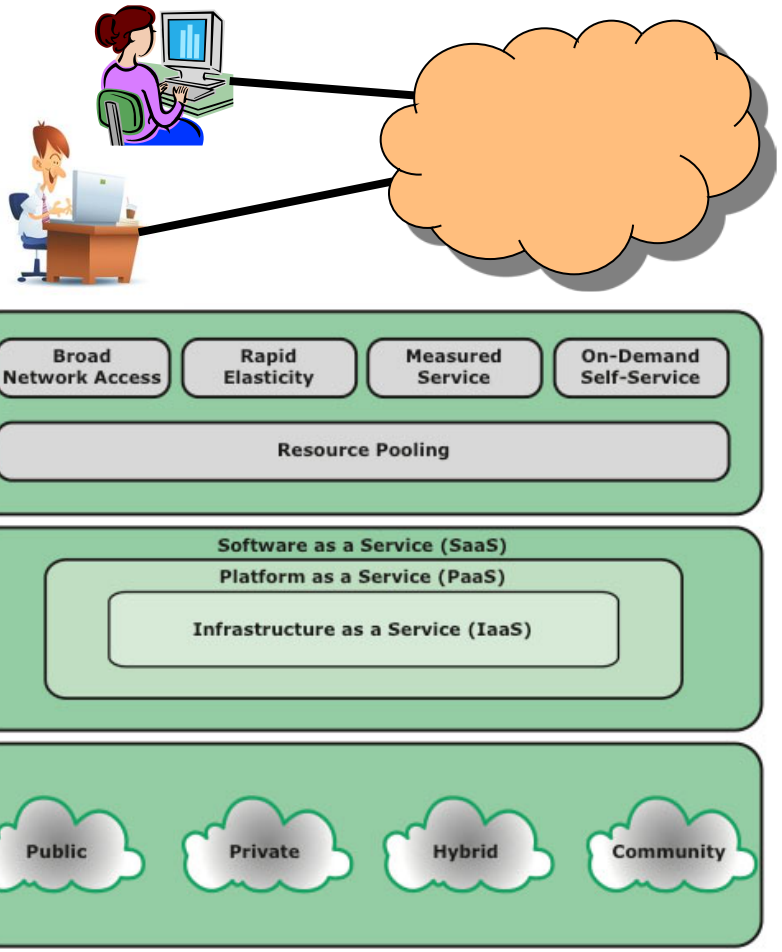
- Authentication method can be changed without upgrading switches and access points
- Only the client and authentication server need to implement the authentication method

EAP with RADIUS



Cloud Computing

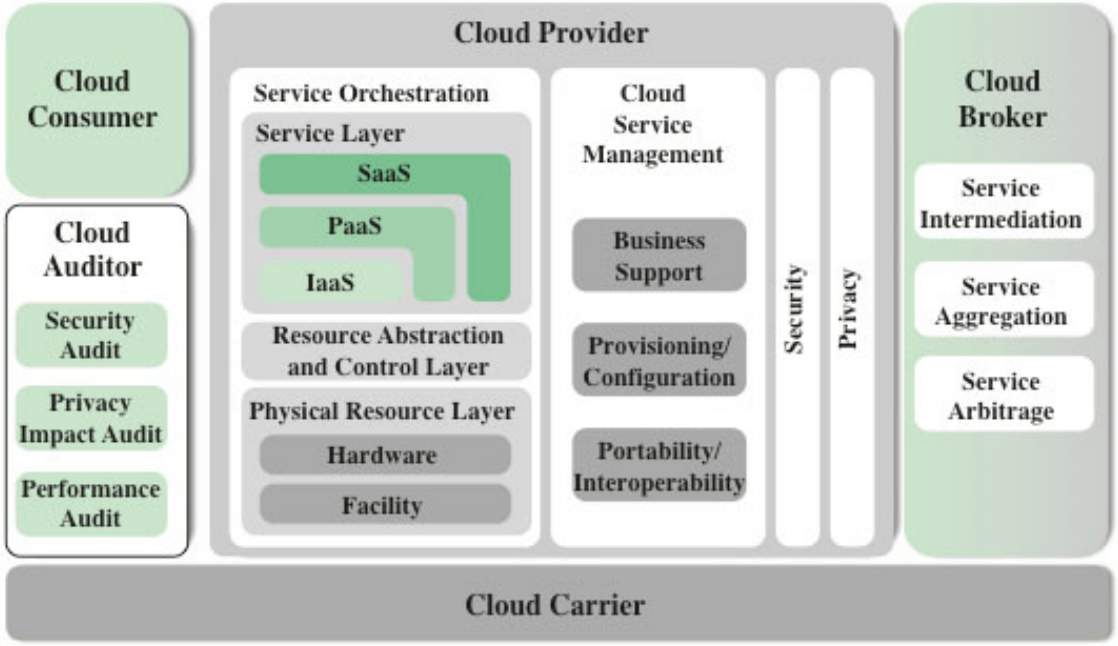
- Using remote resources (Processor, Storage, Network, software, services)
- Five **Characteristics**
  1. Shared: Resource Pooling
  2. Ubiquitous: Broad network access
  3. Rapidly Provisioned: Rapid Elasticity
  4. Configurable: Measured Service
  5. On-demand Self-Service
- Three **Service Models**
  1. Infrastructure as a Service (IaaS):CPU
  2. Platform as a Service (PaaS):CPU+OS
  3. Software as a Service (SaaS): Application
- Four **Deployment models**
  1. Public
  2. Private
  3. Hybrid
  4. Community



Ref: M. Schultz, ""A Survey of Cloud Security Issues and Offerings, " http://www.cse.wustl.edu/~jain/cse571-11/cloud.htm

Roles

- Cloud Consumer
- Cloud Service Provider (CSP)
- Cloud Broker
- Cloud Auditor
- Cloud Carrier: Internet service Provider (ISP)



Cloud Security Risks and Countermeasures

- 7 Risks and Countermeasures

1. **Abuse and Criminal Use**:
   - Strict user authentication
   - Intrusion detection
   - Monitoring public blacklists for own network blocks
2. **Malicious Insiders**:
   - Comprehensive assessment of CSP
   - Human resource requirement as a part of the legal contract
   - Transparency into overall security management
   - Security breach notification process

Risks and Countermeasures (Cont)

3. Insecure Interfaces and API's:

- Analyze security models of CSP interface
- Ensure strong authentication and encryption

4. Shared Technology Issues:

- Monitor environment for unauthorized changes
- Strong authentication and access control for adminstrators
- SLAs for patching vulnerability remediation
- Conduct vulnerability scanning and configuration audits

Risks and Countermeasures (Cont)

5. Data Loss or Leakage:

- Strong API access control
- Encrypt data in transit
- Analyze data protection at design and runtime
- Strong key generation, storage, management, and destruction

6. Account or Service Hijacking:

- No sharing of credentials between users and services
- Strong two-factor authentication
- Intrusion detection
- Understand CSP security policies and SLAs

Risks and Countermeasures (Cont)

7. Unknown Risk Profile:

- Disclosure of applicable logs and data
- Partial/full disclosure of infrastructure details
- Monitoring and alerting on necessary information

NIST Guidelines on Cloud Security

- 9 Guidelines

1. Governance:

- Extend organizational policies and procedures to cloud
- Audit mechanisms to ensure that policies are followed

2. Compliance:

- Understand legal and regulatory obligations
- Ensure that the contract meets these obligations
- Ensure that CSP's discovery capabilities do not compromise security and privacy of data

NIST Guidelines (Cont)

3. Trust:

- Visibility into the security and privacy controls of CSP
- Clear exclusive ownership of data
- Institute a risk management system
- Continuously monitor the system

4. Architecture:

- Understand CSP's provisioning methods and their impact on the security over the entire life cycle

5. Identity and Access Management:

- Ensure strong authentication, authorization, and identity management

NIST Guidelines (Cont)

6. Software Isolation:

- Understand the virtualization techniques and their risks

7. Data Protection:

- Evaluate CSP's ability to control access to data at rest, in transit, and in use and to sanitize data
- Access risk of collating data with other organizations with high threat value
- Understand CSP's cryptographic key management

NIST Guidelines (Cont)

8. Availability:

- Assess procedures for data backup, recovery, and disaster recovery
- Ensure critical operations can be resumed immediately after a disaster and other operations can be eventually resumed

9. Incident Response:

- Ensure contract provisions for incident response meet your requirements
- Ensure that CSP has a transparent process to share information during and after an incident
- Ensure that you can respond to incident in coordination with CSP

Data Protection Risks

Two database service models:

1. Multi-instance model:

- Each subscriber gets a unique DBMS on a VM
- Subscriber has complete control over role definition, user authorization, and other administrative tasks related to security

2. Multi-tenant model:

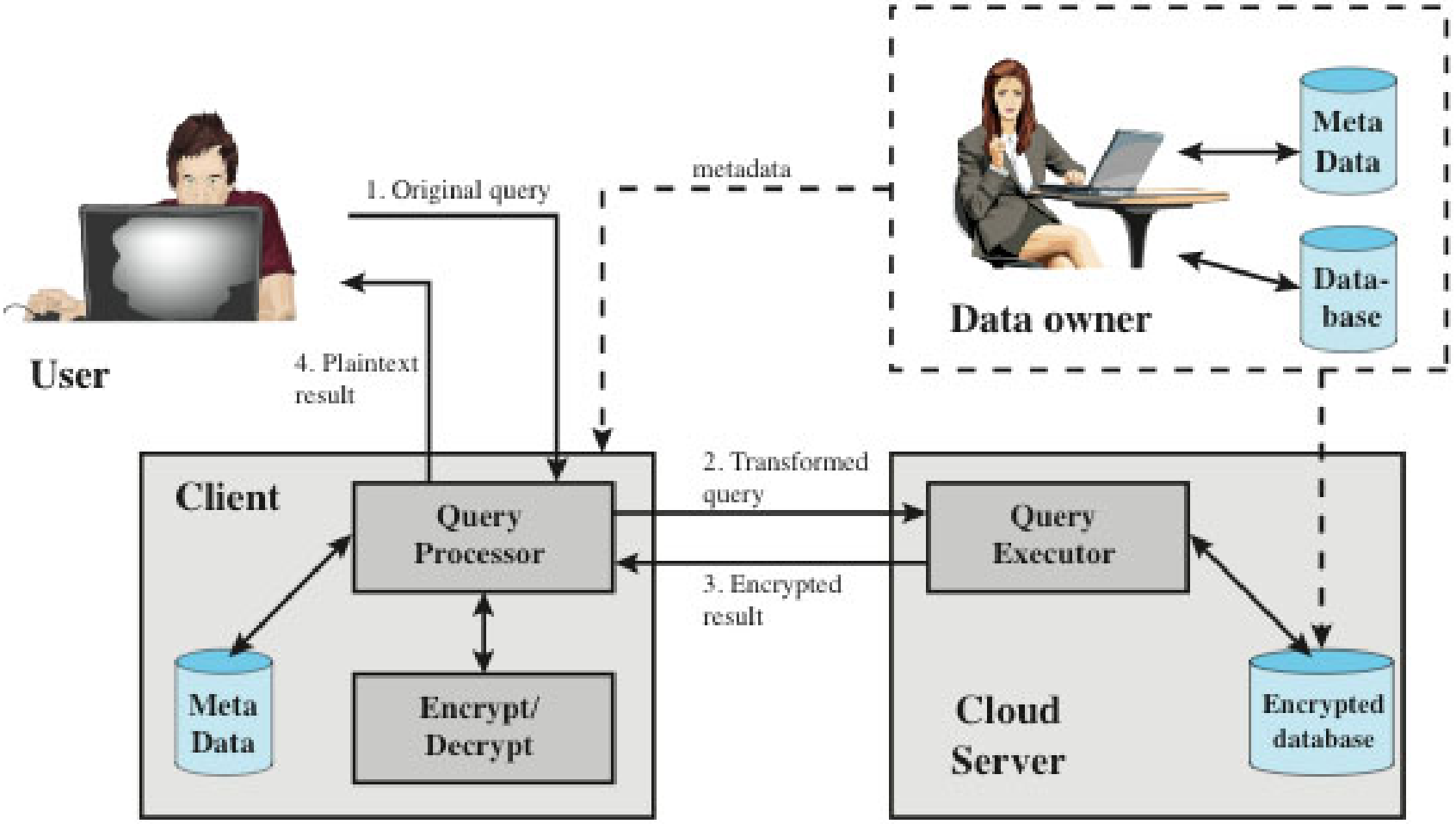
- Subscriber shares a predefined environment with other tenants, typically by tagging data with a subscriber identifier
- CSP needs to establish and maintain a sound secure database environment

Data Protection in the Cloud

- Data must be secured while at rest, in transit, and in use, and access to the data must be controlled
- Use encryption to protect data in transit
  ⇒ key management responsibilities for the CSP
- Store only encrypted data in the cloud
  ⇒ CSP has no access to the encryption key
  - Encrypt the entire database and not provide the encryption/decryption keys to CSP
  - Can't access individual data items based on searches or indexing on key parameters
  - Need to download entire tables from the database, decrypt the tables, and work with the results

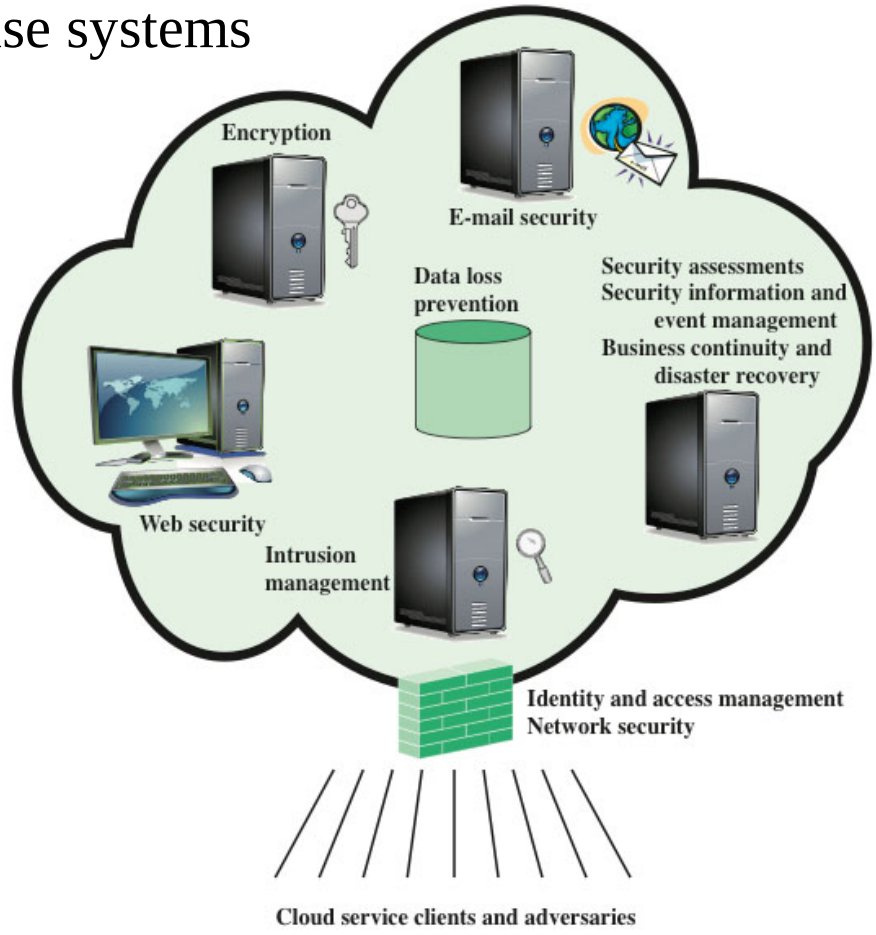
  ⇒ To provide more flexibility it must be possible to work with the database in its encrypted form

Data Protection (Cont)

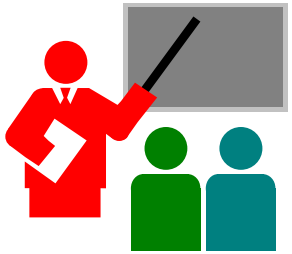


Cloud Security as a Service (SecaaS)

- **SecaaS**: Provisioning of security applications and services via the cloud either to cloud-based infrastructure and software or from the cloud to the customers' on-premise systems
- **SecaaS Categories of Service**:
  1. Identity and access management
  2. Data loss prevention
  3. Web security
  4. E-mail security
  5. Security assessments
  6. Intrusion management
  7. Security information and event management
  8. Encryption
  9. Business continuity and disaster recovery
  10. Network security



Summary



1. RADIUS allows centralized authentication server and allows roaming
2. EAP allows many different authentication methods to use a common framework ⇒ Authenticators do not need to know about authentication methods
3. Many variations of EAP authentication methods depending upon certificates, shared secrets, passwords
4. 802.1X adds authentication to LAN and uses EAPOL
5. Cloud computing uses a shared pool of resources. Numerous security issues and counter measures.

Homework 16

- Read RFC 3748 on EAP. Is clear text password one of the EAP authentication method? If yes, what is the code for this. If not, why not?