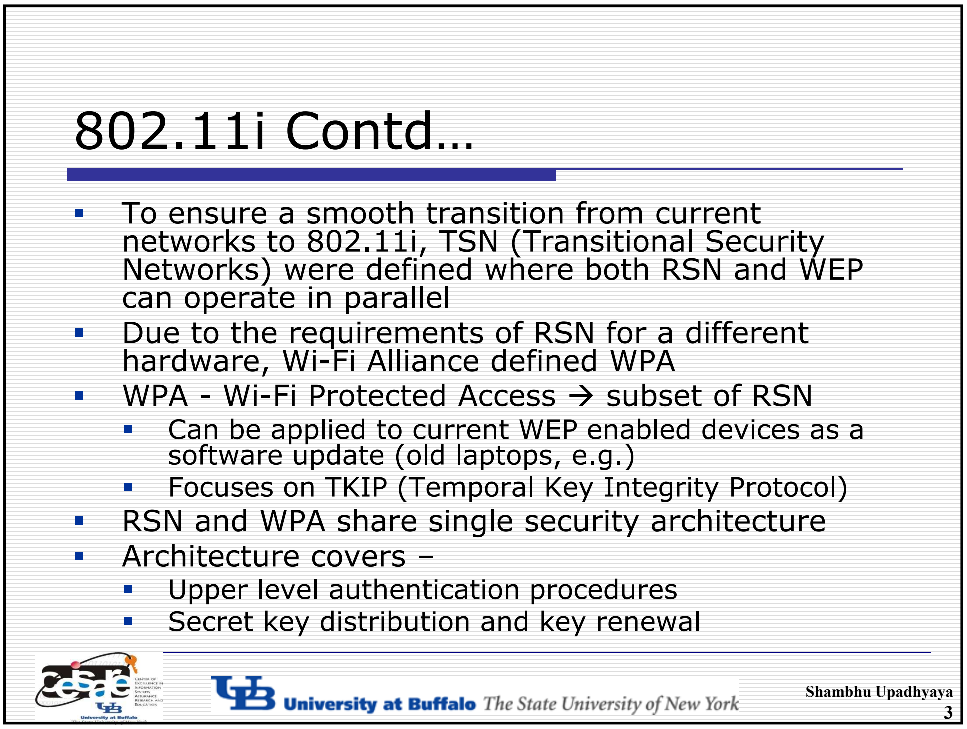
802.11 Security – 802.11i

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lectures 10, 11, 12)

802.11i Introduction

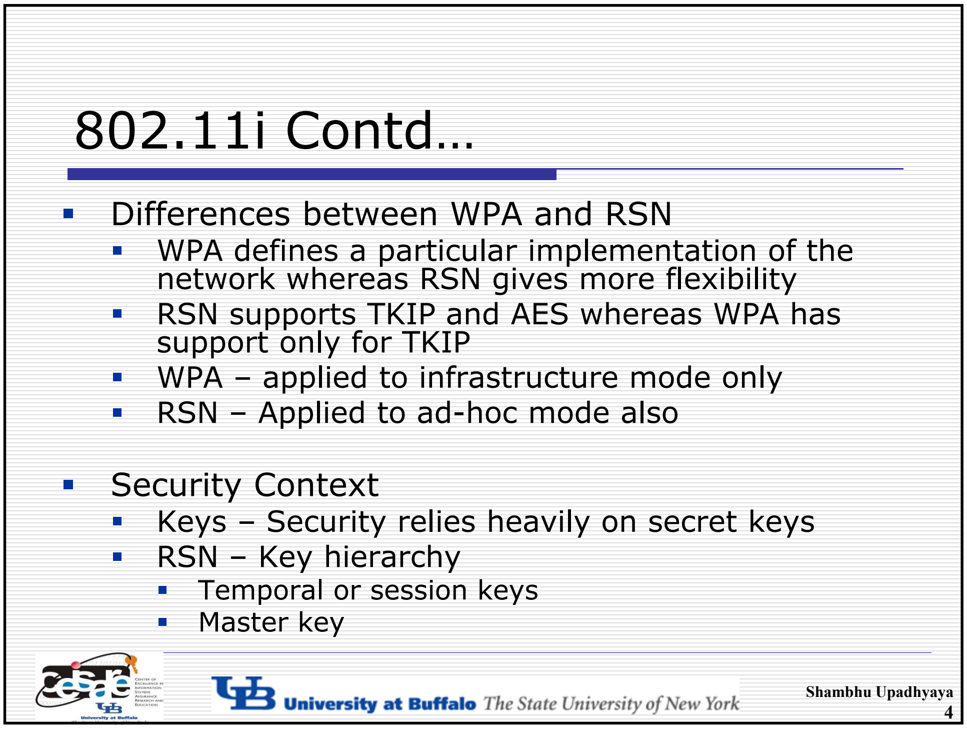
- New generation of Security Standards
- Accepted as a Standard in June, 2004
- Defines a security mechanism that operates between the Media Access Control (MAC) sublayer and the Network layer
- Introduced a new type of wireless network called RSN
- RSN - Robust Security Networks
  - Based on AES (Advanced Encryption Standard) along with 802.1X and EAP (Extensible Authentication Protocol)
  - Needs RSN compatible hardware to operate



802.11i Contd…

- To ensure a smooth transition from current networks to 802.11i, TSN (Transitional Security Networks) were defined where both RSN and WEP can operate in parallel
- Due to the requirements of RSN for a different hardware, Wi-Fi Alliance defined WPA
- WPA - Wi-Fi Protected Access → subset of RSN
  - Can be applied to current WEP enabled devices as a software update (old laptops, e.g.)
  - Focuses on TKIP (Temporal Key Integrity Protocol)
- RSN and WPA share single security architecture
- Architecture covers –
  - Upper level authentication procedures
  - Secret key distribution and key renewal

University at Buffalo The State University of New York



802.11i Contd…

- Differences between WPA and RSN
  - WPA defines a particular implementation of the network whereas RSN gives more flexibility
  - RSN supports TKIP and AES whereas WPA has support only for TKIP
  - WPA – applied to infrastructure mode only
  - RSN – Applied to ad-hoc mode also

- Security Context
  - Keys – Security relies heavily on secret keys
  - RSN – Key hierarchy
    - Temporal or session keys
    - Master key

University at Buffalo The State University of New York

802.11i Contd…

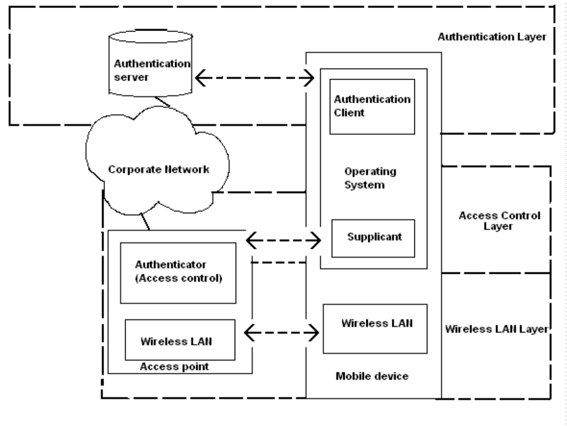
- Security Layers
  - Wireless LAN layer

    Raw communication, advertising capabilities, encryption, decryption
  - Access control layer

    Middle manager: manages the security context. Talks to the authentication layer to decide the establishment of security context and participates in generation of temporal keys
  - Authentication layer

    Layer where the policy decisions are made and proof of identity is accepted or rejected

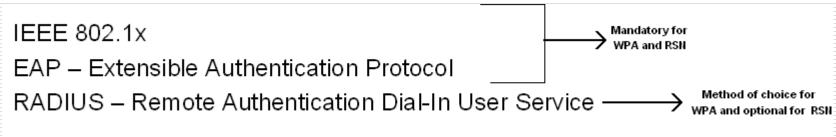
802.11i Contd…



Relationship of Layers

Access Control Methods

- Access Control Mechanism to separate authorized and unauthorized personnel
- Protocols used to implement Access Control in RSN and WPA are:
  - 802.1X
  - EAP
  - RADIUS



IEEE 802.1x

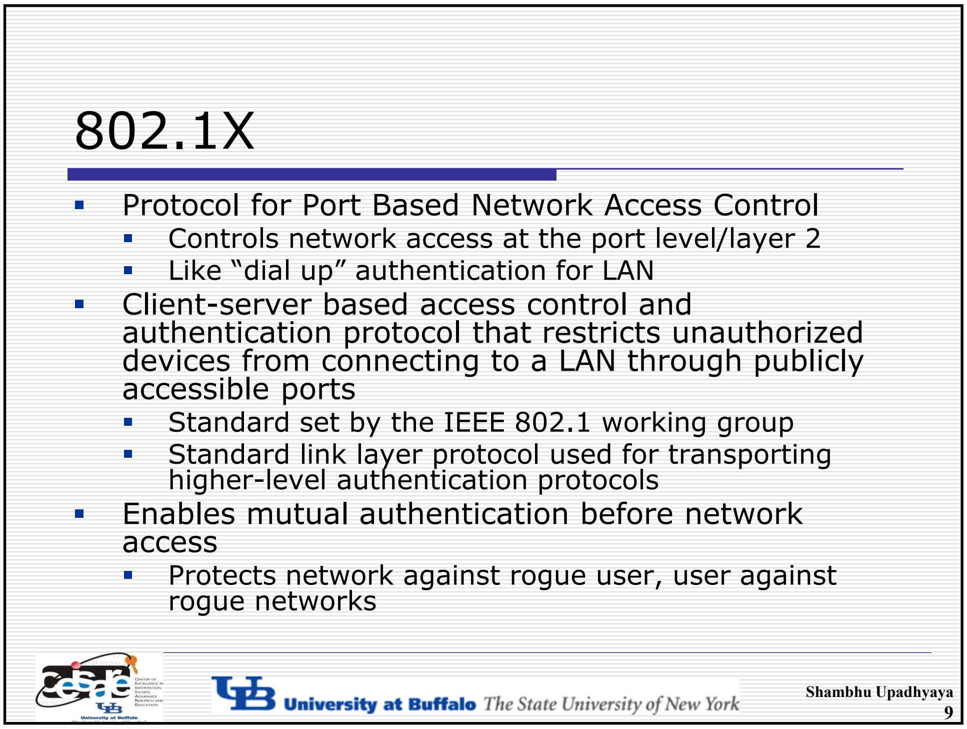
EAP – Extensible Authentication Protocol

RADIUS – Remote Authentication Dial-In User Service

Mandatory for WPA and RSN
Method of choice for WPA and optional for RSN

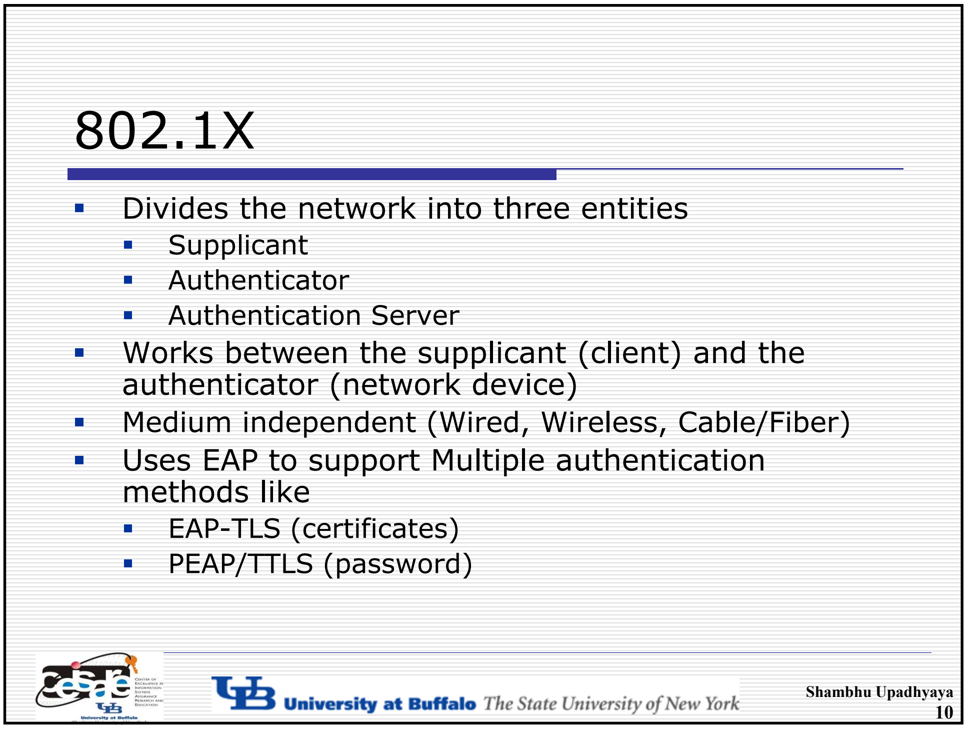
Access Control Methods

- Elements of Access Control
  - Supplicant
  - Authenticator
  - Authorizer
- Steps in Access Control
  - Authenticator is alerted by the supplicant
  - Supplicant identifies himself
  - Authenticator requests authorization from authorizer
  - Authorizer indicates Yes or No
  - Authenticator allows or blocks device



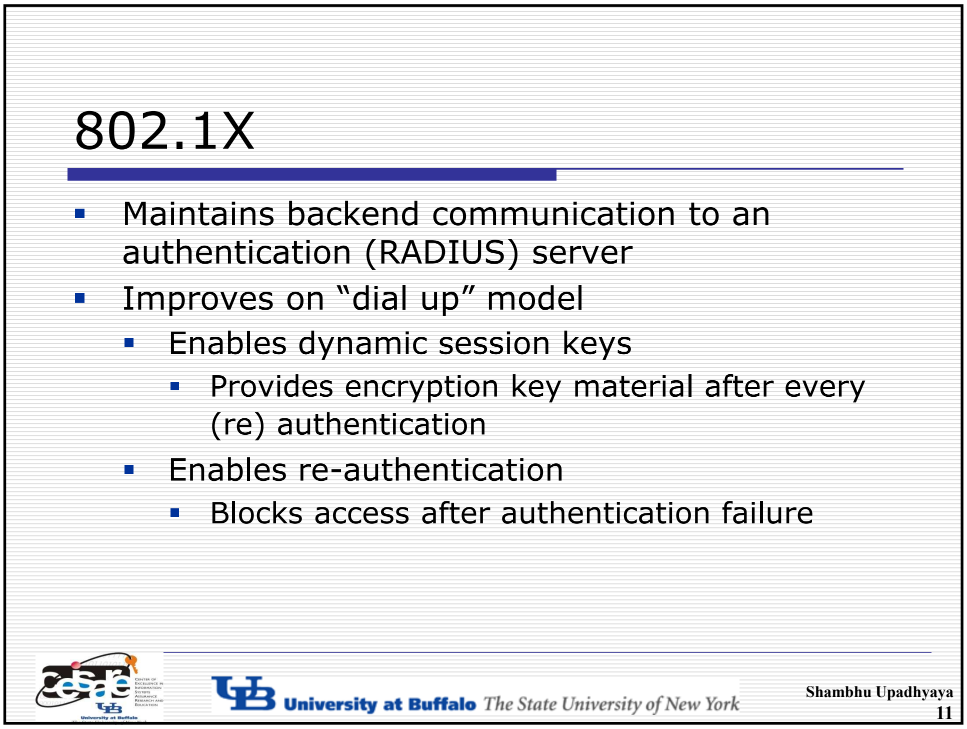
802.1X

- Protocol for Port Based Network Access Control
  - Controls network access at the port level/layer 2
  - Like “dial up” authentication for LAN
- Client-server based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports
  - Standard set by the IEEE 802.1 working group
  - Standard link layer protocol used for transporting higher-level authentication protocols
- Enables mutual authentication before network access
  - Protects network against rogue user, user against rogue networks



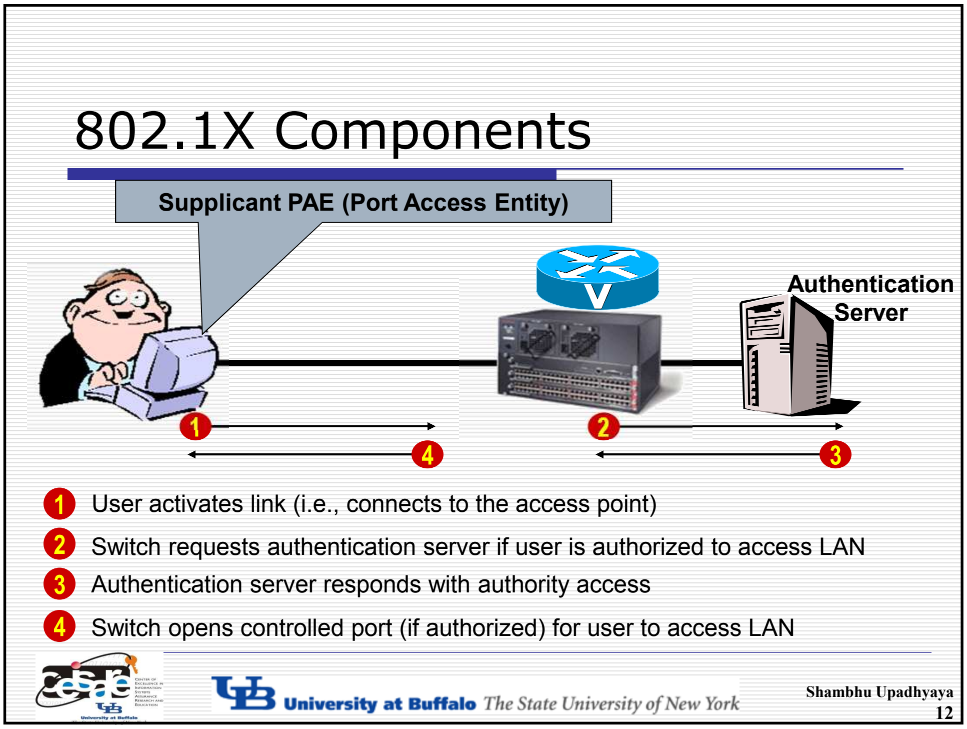
802.1X

- Divides the network into three entities
  - Supplicant
  - Authenticator
  - Authentication Server
- Works between the supplicant (client) and the authenticator (network device)
- Medium independent (Wired, Wireless, Cable/Fiber)
- Uses EAP to support Multiple authentication methods like
  - EAP-TLS (certificates)
  - PEAP/TTLS (password)



802.1X

- Maintains backend communication to an authentication (RADIUS) server
- Improves on “dial up” model
  - Enables dynamic session keys
    - Provides encryption key material after every (re) authentication
  - Enables re-authentication
    - Blocks access after authentication failure



802.1X Components

1 User activates link (i.e., connects to the access point)

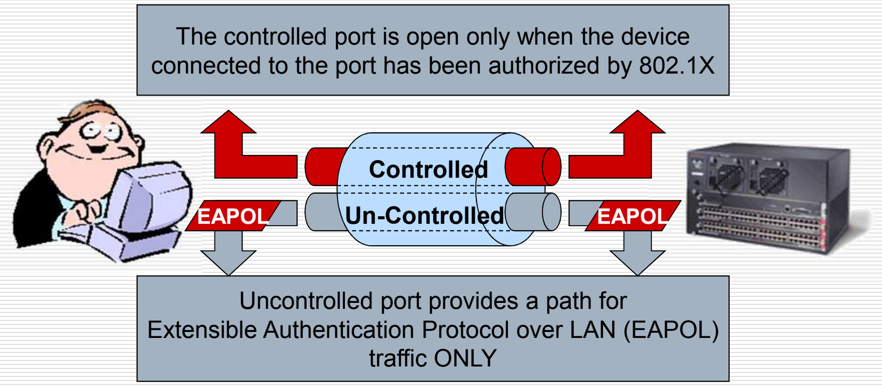
2 Switch requests authentication server if user is authorized to access LAN

3 Authentication server responds with authority access

4 Switch opens controlled port (if authorized) for user to access LAN

802.1X Components

- For each 802.1X switch port, the switch creates TWO virtual access points at each port

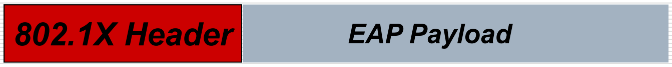


The controlled port is open only when the device connected to the port has been authorized by 802.1X

Uncontrolled port provides a path for Extensible Authentication Protocol over LAN (EAPOL) traffic ONLY

What Does 802.1X Do?

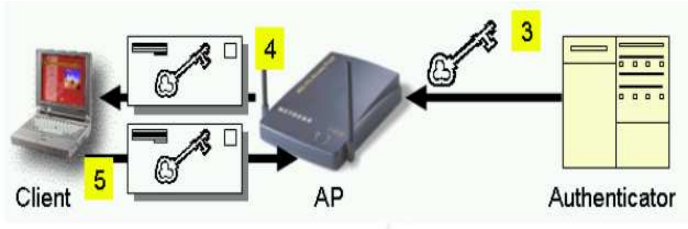
- Transport authentication information in the form of Extensible Authentication Protocol (EAP) payloads
- Authenticator (switch or router) becomes the middleman for relaying EAP received in 802.1X packets to an authentication server by using RADIUS to carry the EAP information
- Three forms of EAP are specified in the standard
  - EAP-MD5 – MD5 Hashed Username/Password
  - EAP-OTP – One-Time Passwords
  - EAP-TLS – Strong PKI Authenticated Transport Layer Security (SSL)



802.1X Authentication

- Following are the steps in 802.1X authentication
  - The client sends an EAP-start message
  - The access point replies with an EAP-request identity message
  - The client sends an EAP-response packet containing the identity to the authentication server (through AP)
  - The authentication server uses a specific authentication algorithm to verify the client's identity
  - The authentication server will either send an *accept* or *reject* message to the access point
  - The access point sends an EAP-success packet (or reject packet) to the client
  - If the authentication server accepts the client, then the access point will transition the client's port to an authorized state and forward additional traffic

802.1X and Dynamic Key Management



Server

Courtesy: SANS Institute Reading Room 2002

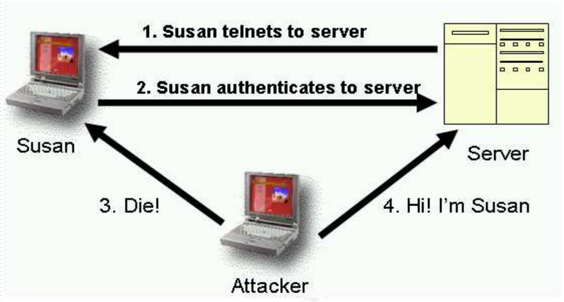
- Initial Authentication done using a Master Key
- Authentication server returns both the results of authentication plus a session key
- AP uses the session keys from the authentication server to sign and encrypt a message that is forwarded to the client
- The client can then use contents of the key message to define appropriate encryption keys

802.1X and Dynamic Key Management

- Advantages of Dynamic key management
  - Provides a more secure mechanism than the manual maintenance of keys
  - Allows to automatically change encryption keys as often as necessary to minimize the possibility of a passive attack

802.1X Susceptibility

- 802.1X is susceptible to session hijacking as well as man-in-the-middle attacks



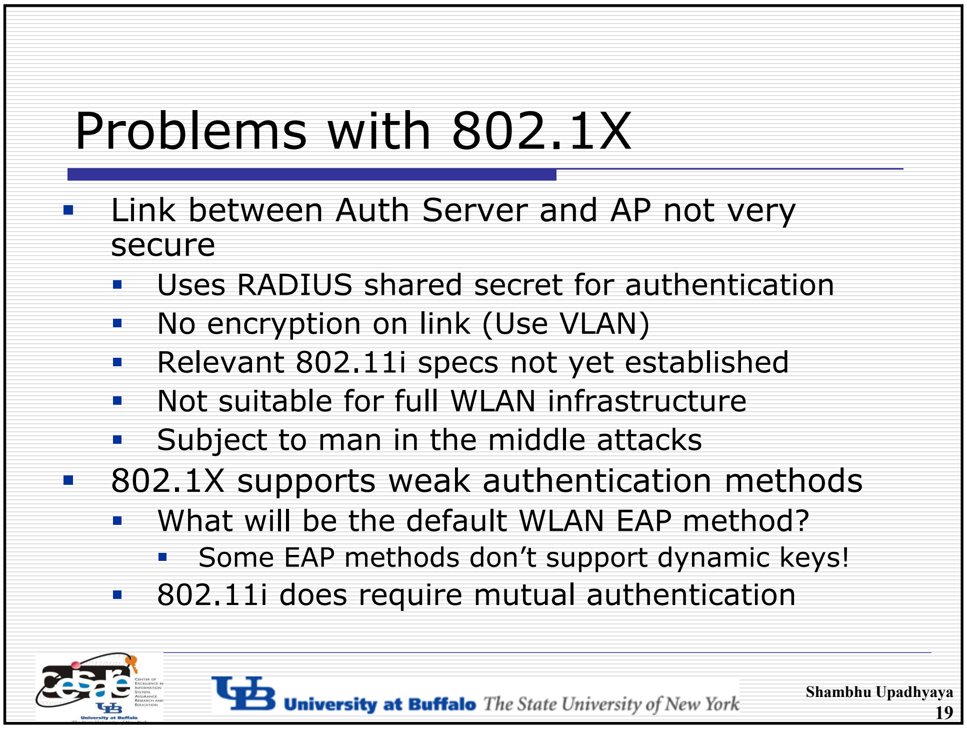
1. Susan telnets to server

2. Susan authenticates to server

3. Die!

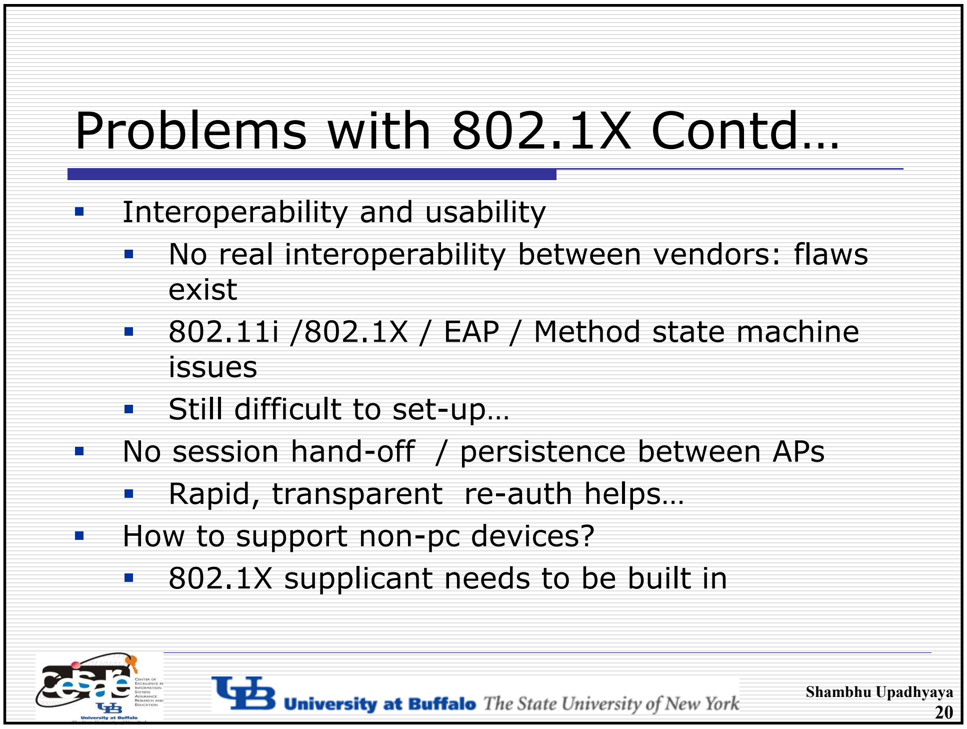
4. Hi! I'm Susan

Courtesy: SANS Institute Reading Room 2002



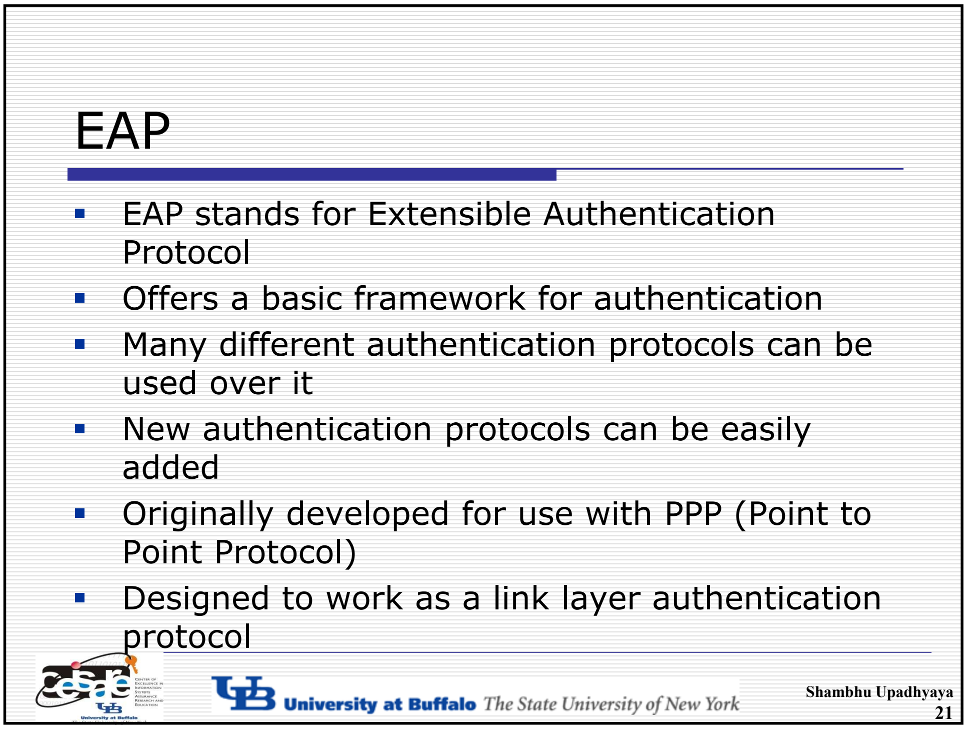
Problems with 802.1X

- Link between Auth Server and AP not very secure
  - Uses RADIUS shared secret for authentication
  - No encryption on link (Use VLAN)
  - Relevant 802.11i specs not yet established
  - Not suitable for full WLAN infrastructure
  - Subject to man in the middle attacks
- 802.1X supports weak authentication methods
  - What will be the default WLAN EAP method?
    - Some EAP methods don’t support dynamic keys!
  - 802.11i does require mutual authentication



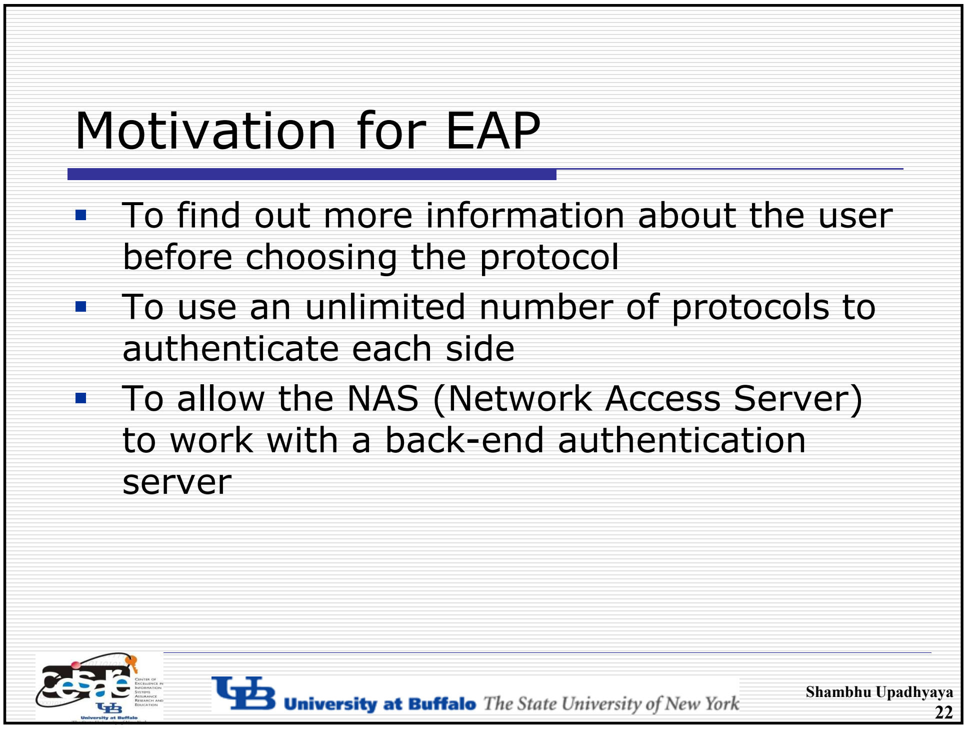
Problems with 802.1X Contd…

- Interoperability and usability
  - No real interoperability between vendors: flaws exist
  - 802.11i /802.1X / EAP / Method state machine issues
  - Still difficult to set-up…
- No session hand-off / persistence between APs
  - Rapid, transparent re-auth helps…
- How to support non-pc devices?
  - 802.1X supplicant needs to be built in



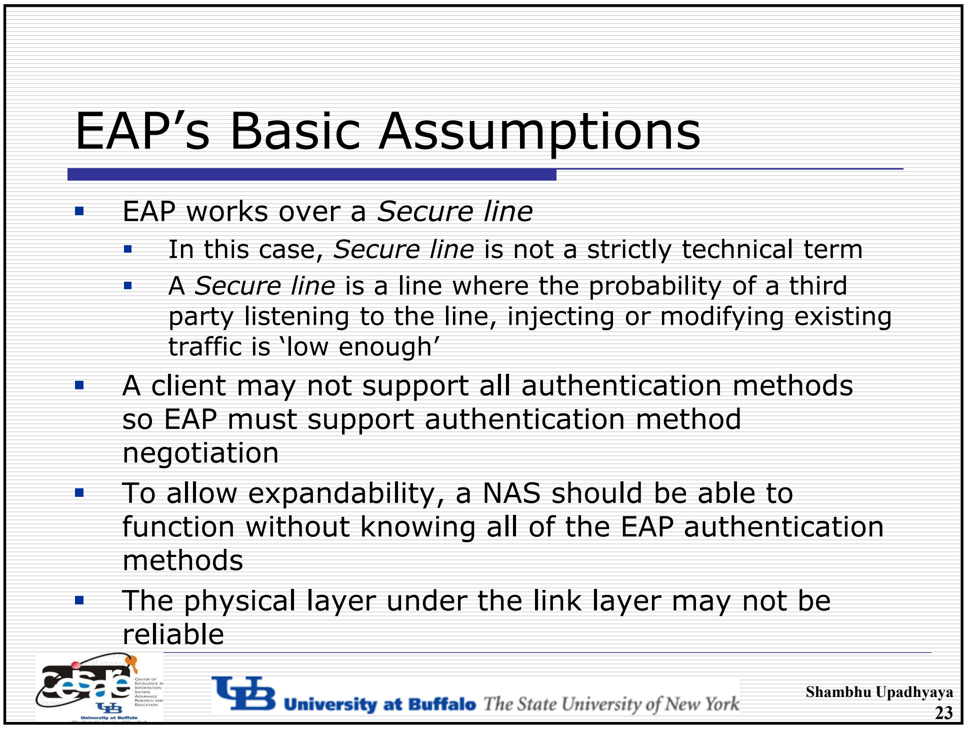
EAP

- EAP stands for Extensible Authentication Protocol
- Offers a basic framework for authentication
- Many different authentication protocols can be used over it
- New authentication protocols can be easily added
- Originally developed for use with PPP (Point to Point Protocol)
- Designed to work as a link layer authentication protocol



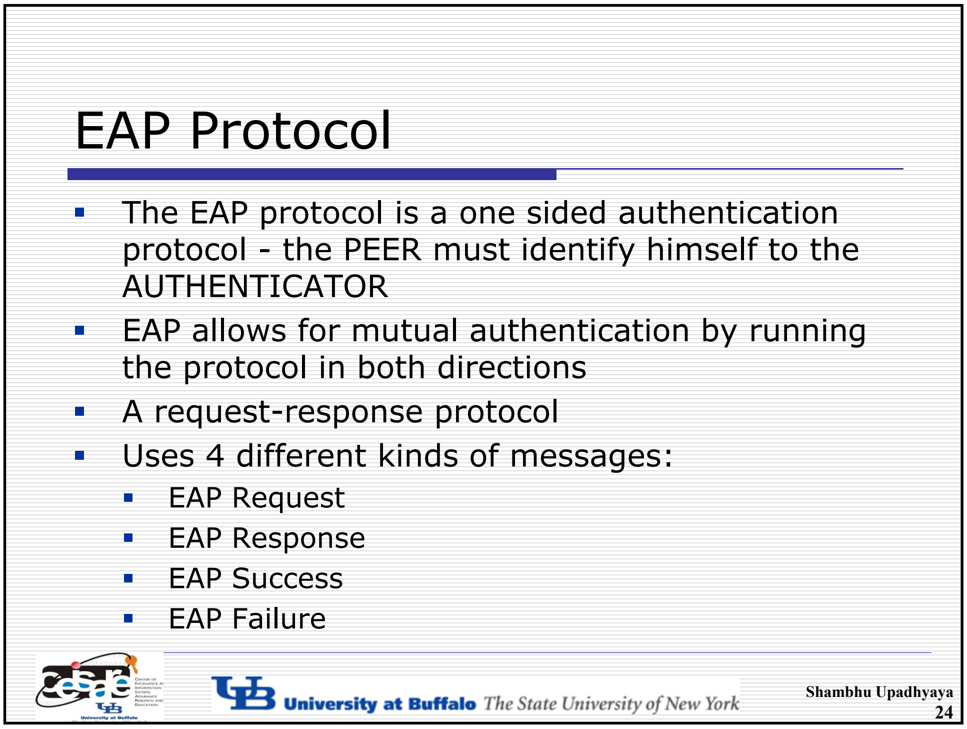
Motivation for EAP

- To find out more information about the user before choosing the protocol
- To use an unlimited number of protocols to authenticate each side
- To allow the NAS (Network Access Server) to work with a back-end authentication server



EAP's Basic Assumptions

- EAP works over a *Secure line*
  - In this case, *Secure line* is not a strictly technical term
  - A *Secure line* is a line where the probability of a third party listening to the line, injecting or modifying existing traffic is 'low enough'
- A client may not support all authentication methods so EAP must support authentication method negotiation
- To allow expandability, a NAS should be able to function without knowing all of the EAP authentication methods
- The physical layer under the link layer may not be reliable

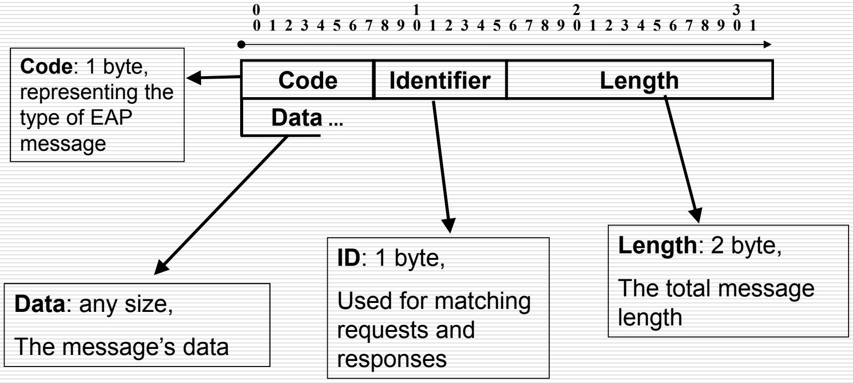


EAP Protocol

- The EAP protocol is a one sided authentication protocol - the PEER must identify himself to the AUTHENTICATOR
- EAP allows for mutual authentication by running the protocol in both directions
- A request-response protocol
- Uses 4 different kinds of messages:
  - EAP Request
  - EAP Response
  - EAP Success
  - EAP Failure

EAP Messages

- **All EAP messages have a common format:**



Code: 1 byte, representing the type of EAP message

Data: any size,

The message's data

ID: 1 byte,

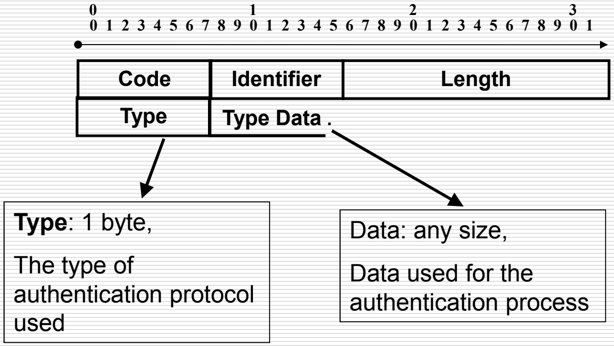
Used for matching requests and responses

Length: 2 byte,

The total message length

EAP Messages Contd…

- **EAP request and response messages have the same format, with code=1 for requests and code=2 for responses**

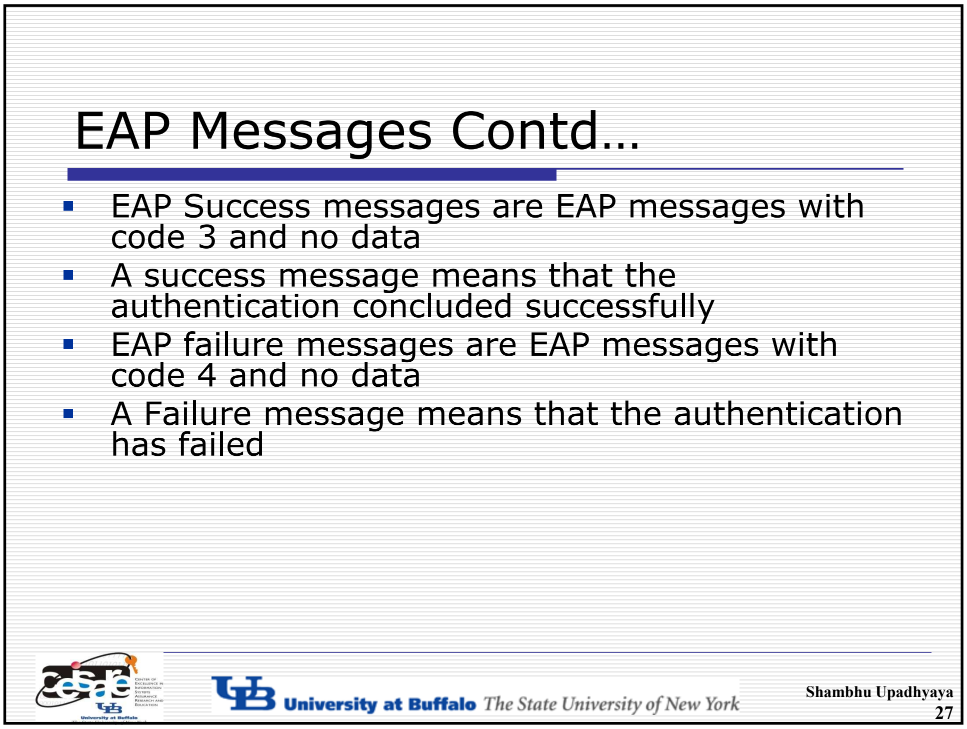


Type: 1 byte,

The type of authentication protocol used

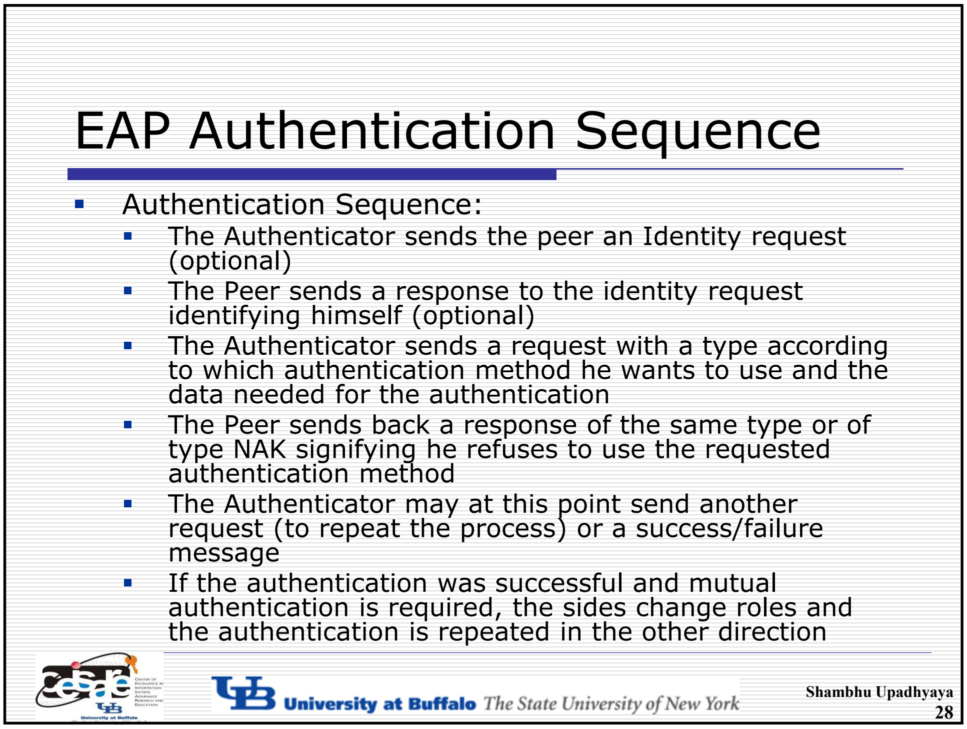
Data: any size,

Data used for the authentication process



EAP Messages Contd…

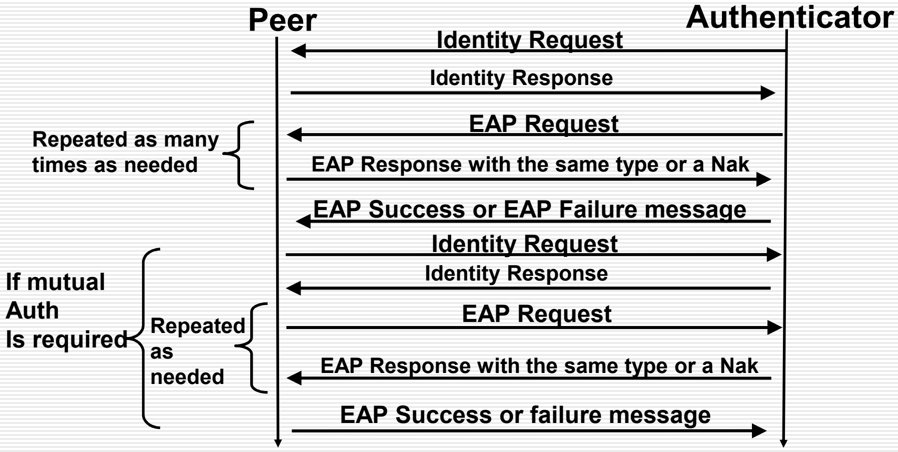
- EAP Success messages are EAP messages with code 3 and no data
- A success message means that the authentication concluded successfully
- EAP failure messages are EAP messages with code 4 and no data
- A Failure message means that the authentication has failed



EAP Authentication Sequence

- Authentication Sequence:
  - The Authenticator sends the peer an Identity request (optional)
  - The Peer sends a response to the identity request identifying himself (optional)
  - The Authenticator sends a request with a type according to which authentication method he wants to use and the data needed for the authentication
  - The Peer sends back a response of the same type or of type NAK signifying he refuses to use the requested authentication method
  - The Authenticator may at this point send another request (to repeat the process) or a success/failure message
  - If the authentication was successful and mutual authentication is required, the sides change roles and the authentication is repeated in the other direction

Generic EAP Example



Peer

Authenticator

Identity Request

Identity Response

Repeated as many times as needed

EAP Request

EAP Response with the same type or a Nak

EAP Success or EAP Failure message

If mutual Auth Is required

Identity Request

Identity Response

Repeated as needed

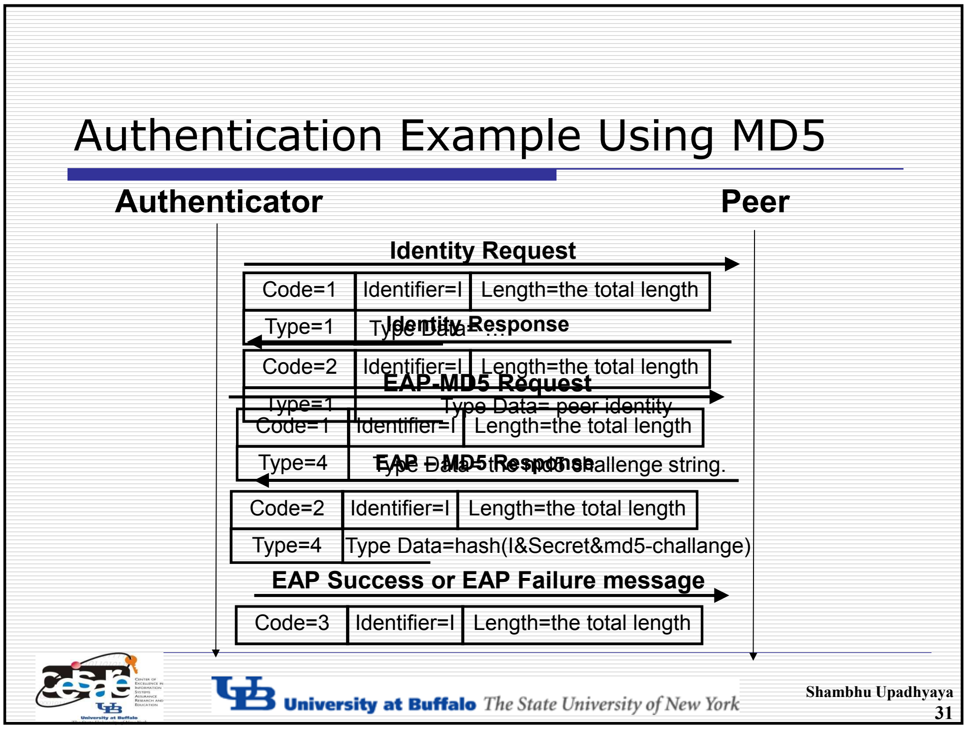
EAP Request

EAP Response with the same type or a Nak

EAP Success or failure message

Basic EAP Methods

- In the initial definition of EAP, included are several built in authentication methods:
  - Identity - request the other side to identify itself
  - Notification - to send notifications to the other side
  - Nak - peer refuses to use the authentication method
  - MD5-Challenge - an implementation of chap over EAP
  - One Time Password - used for one time passwords
  - Generic Token Card - used for generic token cards
  - Vendor Specific



Authentication Example Using MD5

Authenticator

Peer

Identity Request

Code=1	Identifier=I	Length=the total length
Type=1	Type Data= …	

Identity Response

Code=2	Identifier=I	Length=the total length
Type=1	Type Data= peer identity	

EAP-MD5 Request

Code=1	Identifier=I	Length=the total length
Type=4	Type Data= the md5 challenge string.	

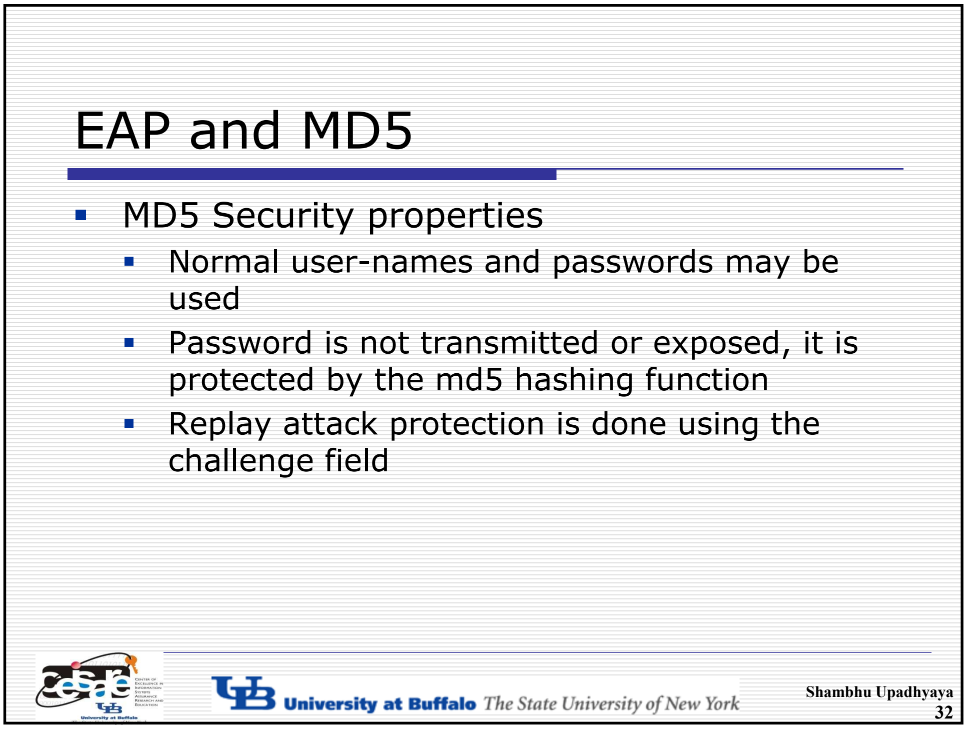
EAP - MD5 Response

Code=2	Identifier=I	Length=the total length
Type=4	Type Data=hash(I&Secret&md5-challange)	

EAP Success or EAP Failure message

Code=3	Identifier=I	Length=the total length

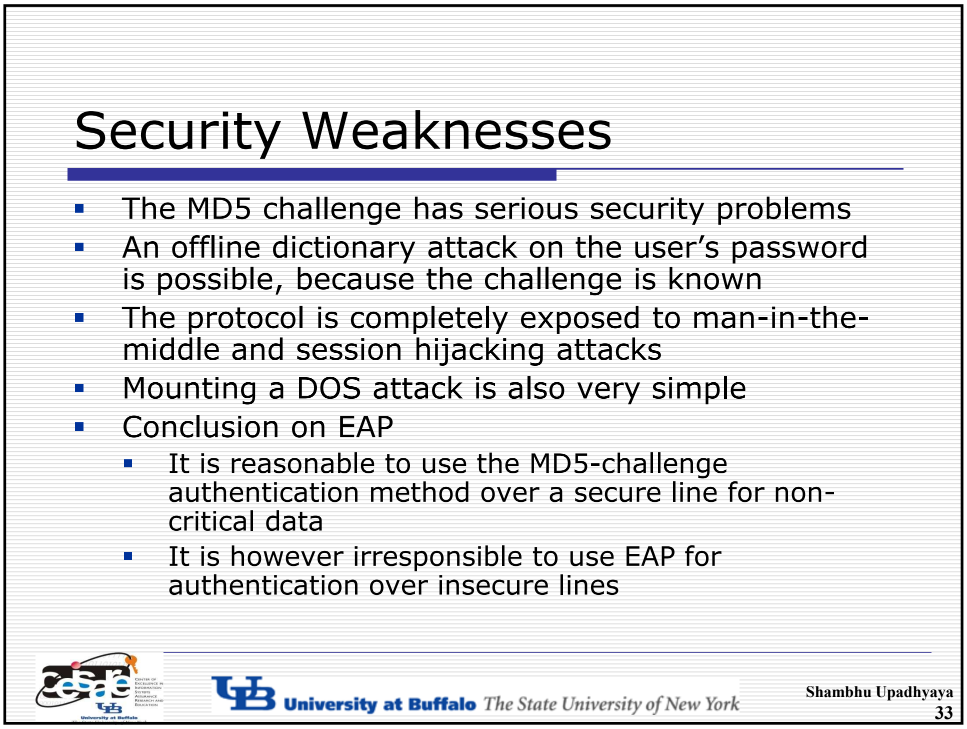
University at Buffalo *The State University of New York*



EAP and MD5

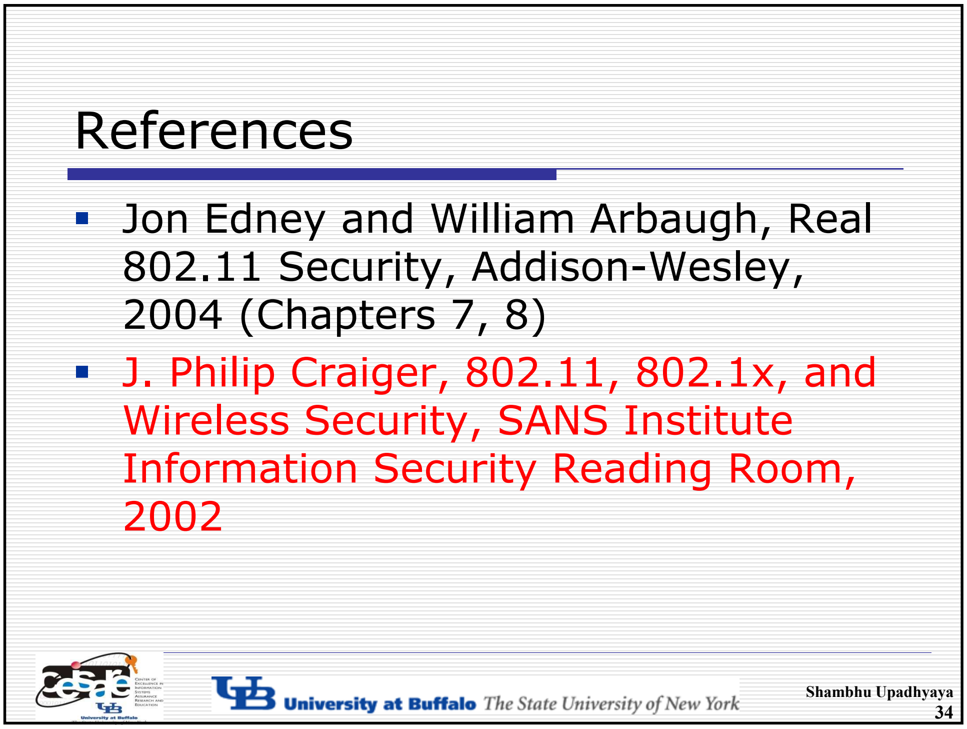
- MD5 Security properties
  - Normal user-names and passwords may be used
  - Password is not transmitted or exposed, it is protected by the md5 hashing function
  - Replay attack protection is done using the challenge field

University at Buffalo *The State University of New York*



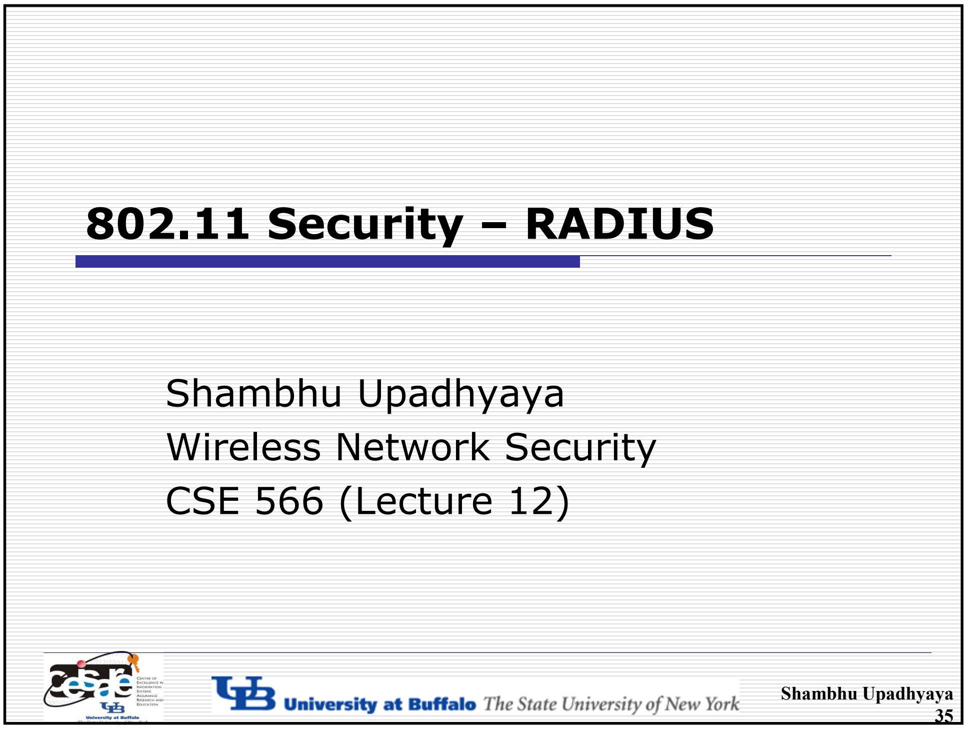
Security Weaknesses

- The MD5 challenge has serious security problems
- An offline dictionary attack on the user's password is possible, because the challenge is known
- The protocol is completely exposed to man-in-the-middle and session hijacking attacks
- Mounting a DOS attack is also very simple
- Conclusion on EAP
  - It is reasonable to use the MD5-challenge authentication method over a secure line for non-critical data
  - It is however irresponsible to use EAP for authentication over insecure lines



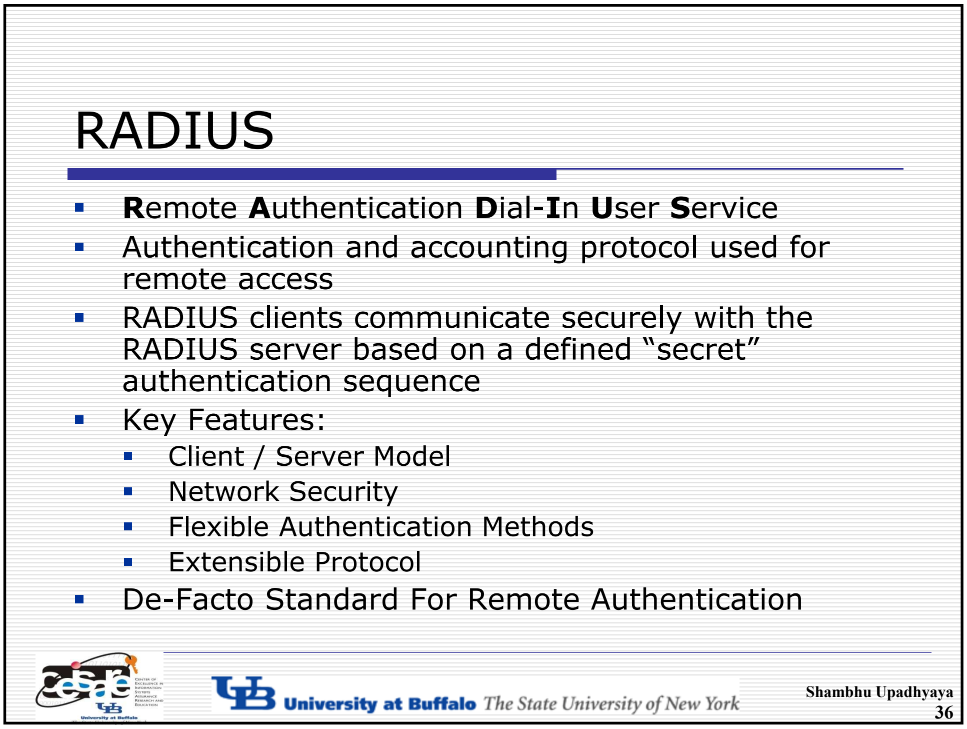
References

- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004 (Chapters 7, 8)
- J. Philip Craiger, 802.11, 802.1x, and Wireless Security, SANS Institute Information Security Reading Room, 2002



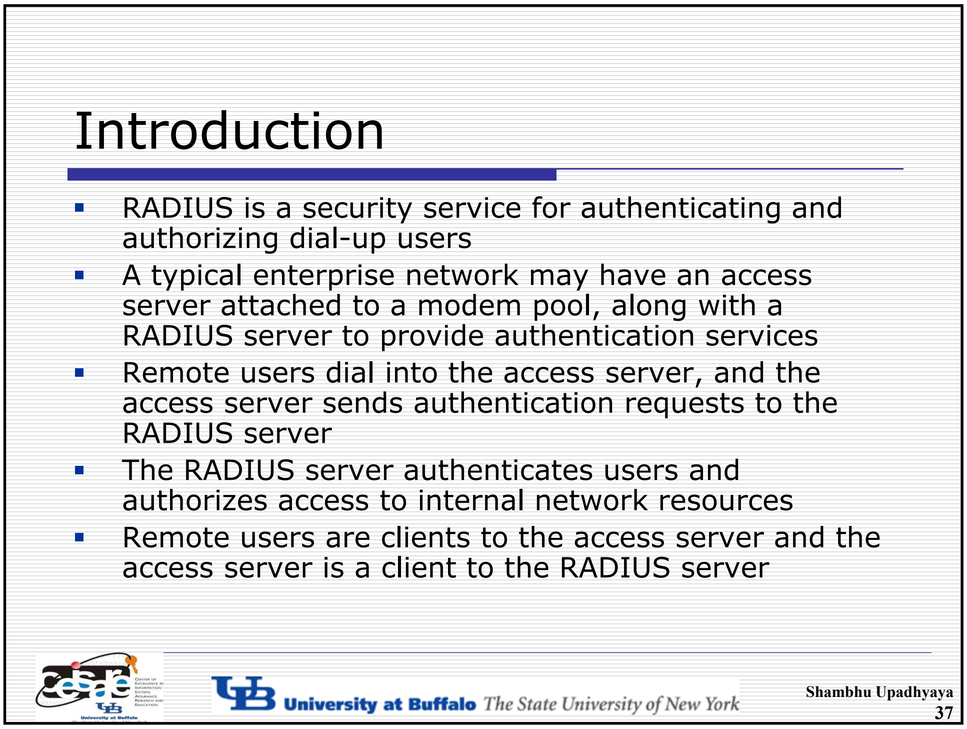
802.11 Security – RADIUS

Shambhu Upadhyaya
Wireless Network Security
CSE 566 (Lecture 12)



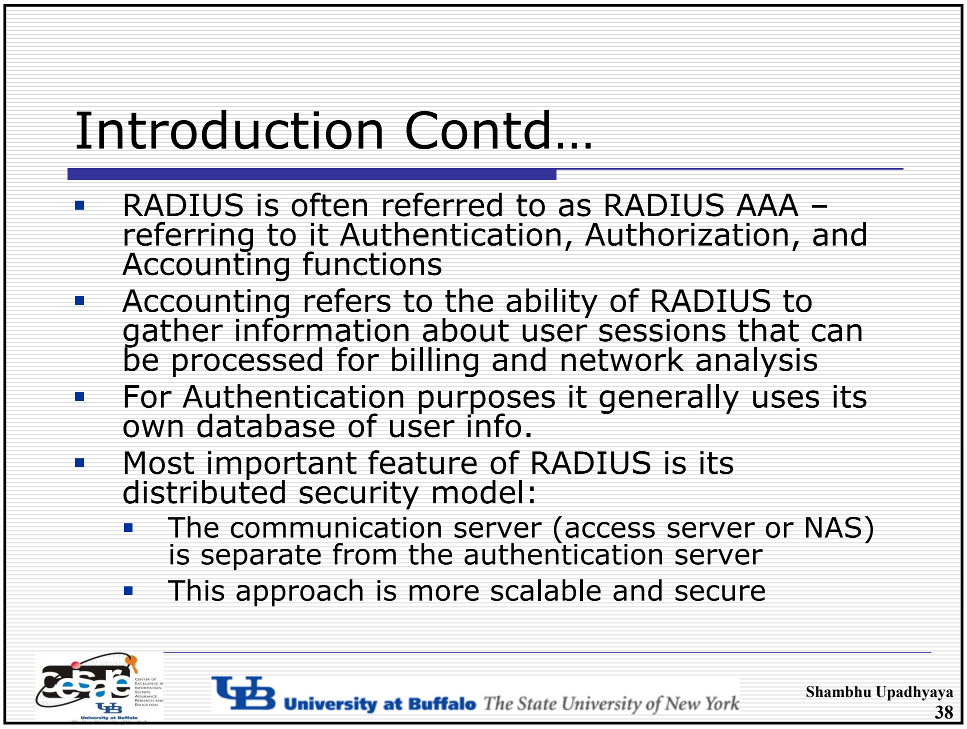
RADIUS

- **R**emote **A**uthentication **D**ial-**I**n **U**ser **S**ervice
- Authentication and accounting protocol used for remote access
- RADIUS clients communicate securely with the RADIUS server based on a defined “secret” authentication sequence
- Key Features:
  - Client / Server Model
  - Network Security
  - Flexible Authentication Methods
  - Extensible Protocol
- De-Facto Standard For Remote Authentication



Introduction

- RADIUS is a security service for authenticating and authorizing dial-up users
- A typical enterprise network may have an access server attached to a modem pool, along with a RADIUS server to provide authentication services
- Remote users dial into the access server, and the access server sends authentication requests to the RADIUS server
- The RADIUS server authenticates users and authorizes access to internal network resources
- Remote users are clients to the access server and the access server is a client to the RADIUS server



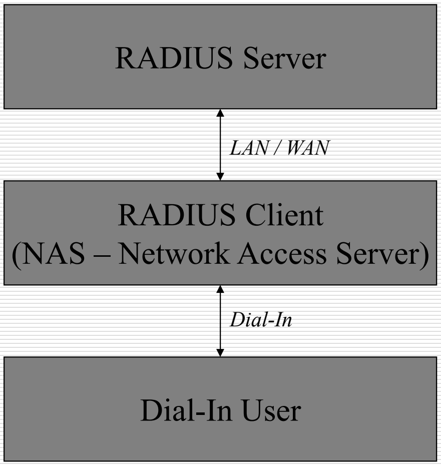
Introduction Contd…

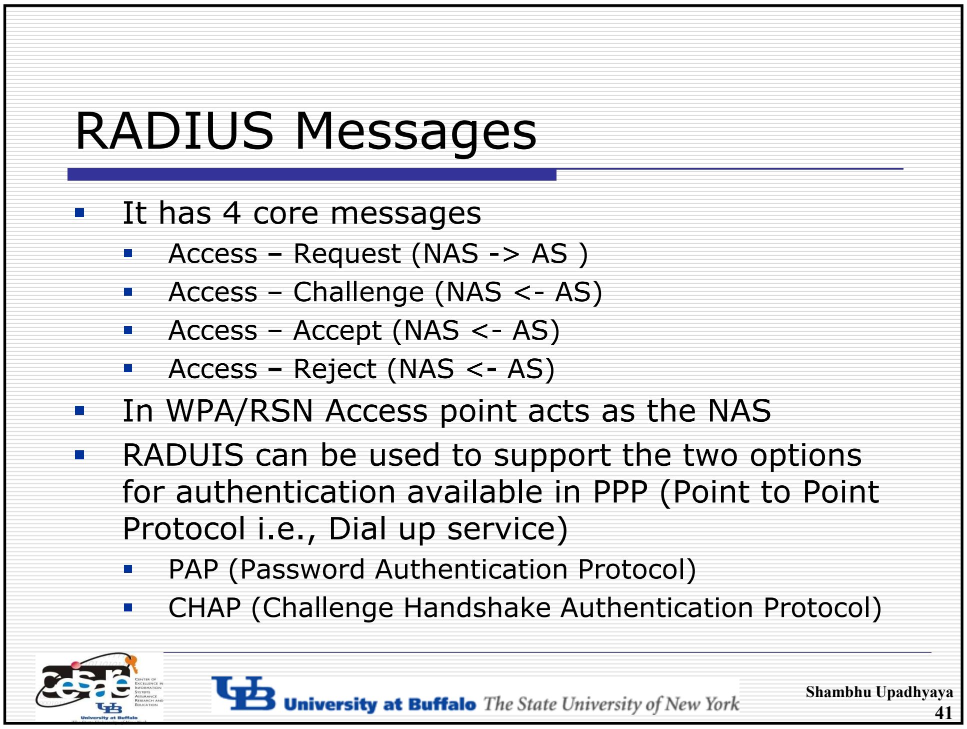
- RADIUS is often referred to as RADIUS AAA – referring to it Authentication, Authorization, and Accounting functions
- Accounting refers to the ability of RADIUS to gather information about user sessions that can be processed for billing and network analysis
- For Authentication purposes it generally uses its own database of user info.
- Most important feature of RADIUS is its distributed security model:
  - The communication server (access server or NAS) is separate from the authentication server
  - This approach is more scalable and secure

Introduction Contd…

- RADIUS defines two things
  - A set of functionality that should be common across authentication servers
  - A protocol that allows other devices to access those capabilities
- Useful to Wi-Fi LANs as
  - Access Points act as NAS
  - Spread across the coverage area
  - All can't have individual authentication databases
  - Hence, a RADIUS server can be used to provide centralized authentication decisions

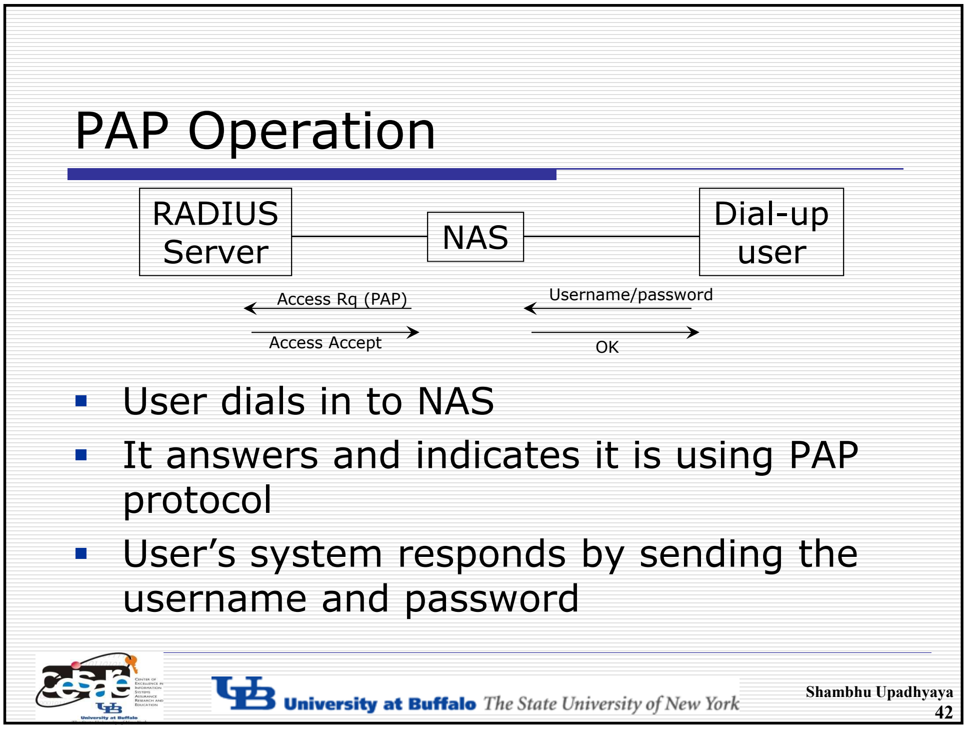
RADIUS Operation





RADIUS Messages

- It has 4 core messages
  - Access – Request (NAS -> AS)
  - Access – Challenge (NAS <- AS)
  - Access – Accept (NAS <- AS)
  - Access – Reject (NAS <- AS)
- In WPA/RSN Access point acts as the NAS
- RADUIS can be used to support the two options for authentication available in PPP (Point to Point Protocol i.e., Dial up service)
  - PAP (Password Authentication Protocol)
  - CHAP (Challenge Handshake Authentication Protocol)



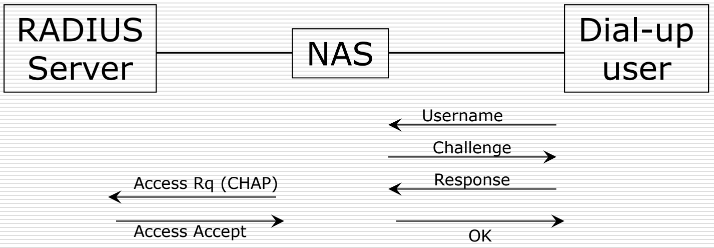
PAP Operation

- User dials in to NAS
- It answers and indicates it is using PAP protocol
- User's system responds by sending the username and password

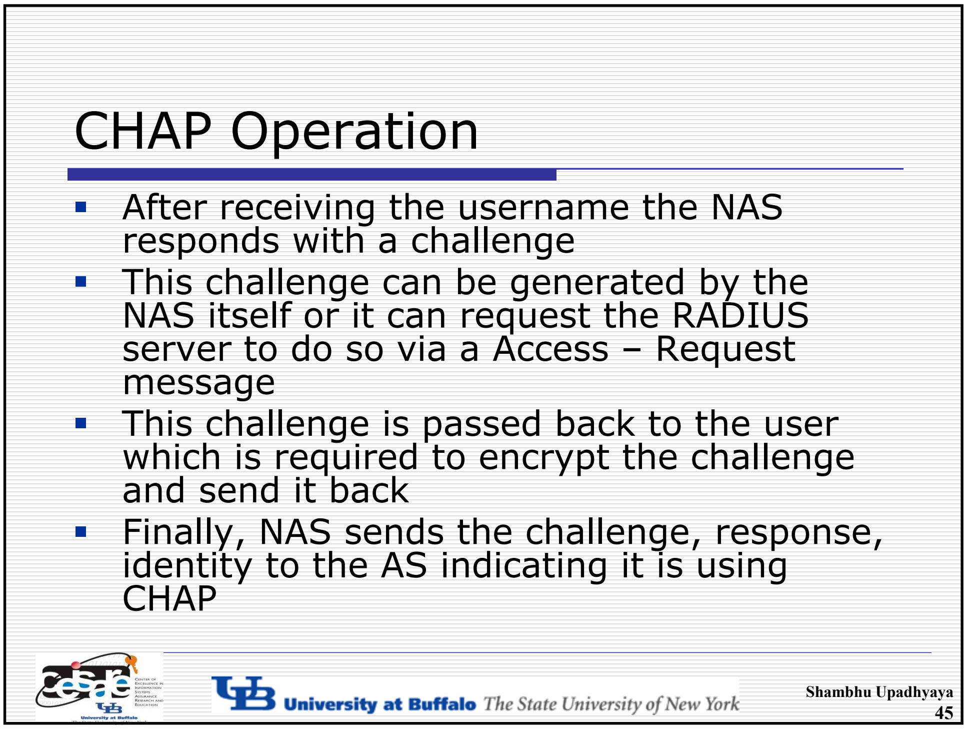
PAP Operation

- NAS now sends the Access-Request message to RADIUS server containing the username and password
- RADIUS server responds with either a Access-Accept or Access-Reject
- NAS acts accordingly
- Very simple approach but subjected to a wide range of attacks
- Password is sent unencrypted over phone line and hence can be easily captured

CHAP Operation

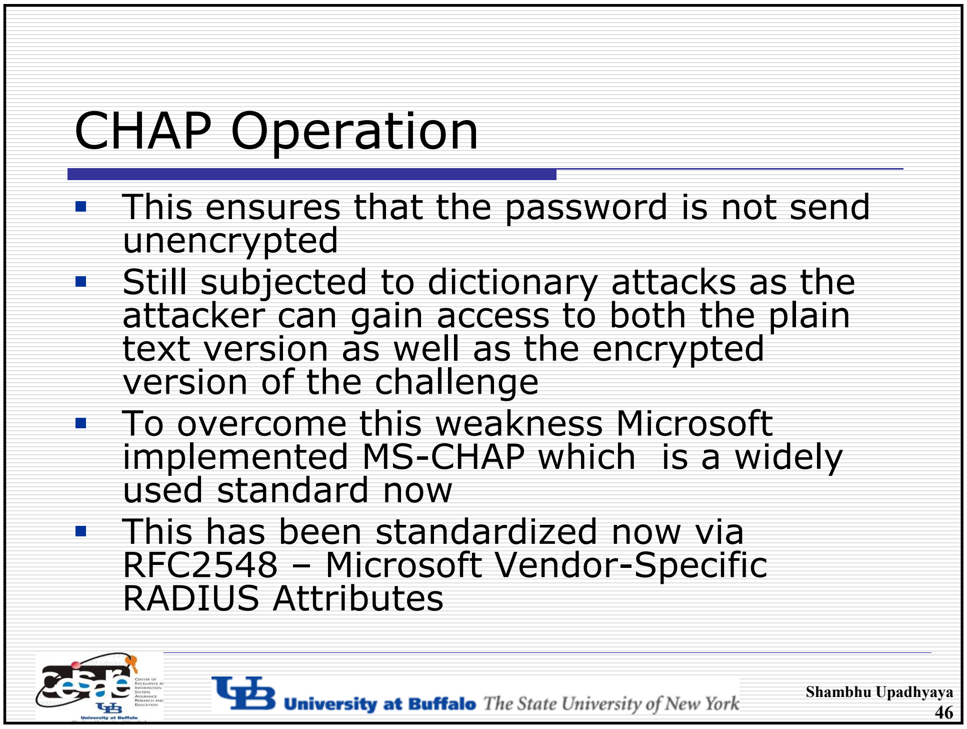


- Better than PAP and tries to provide secure authentication
- Rather than sending password unencrypted it just sends the username initially



CHAP Operation

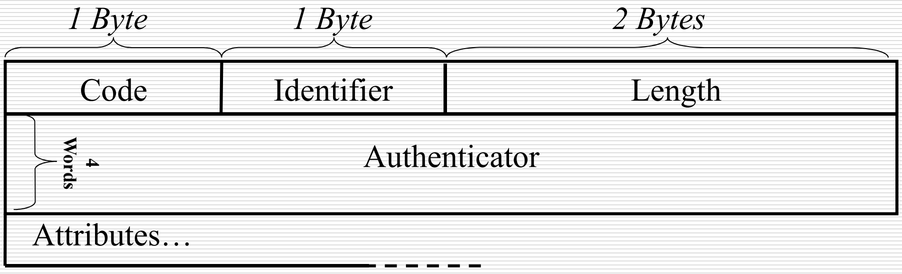
- After receiving the username the NAS responds with a challenge
- This challenge can be generated by the NAS itself or it can request the RADIUS server to do so via a Access – Request message
- This challenge is passed back to the user which is required to encrypt the challenge and send it back
- Finally, NAS sends the challenge, response, identity to the AS indicating it is using CHAP



CHAP Operation

- This ensures that the password is not send unencrypted
- Still subjected to dictionary attacks as the attacker can gain access to both the plain text version as well as the encrypted version of the challenge
- To overcome this weakness Microsoft implemented MS-CHAP which is a widely used standard now
- This has been standardized now via RFC2548 – Microsoft Vendor-Specific RADIUS Attributes

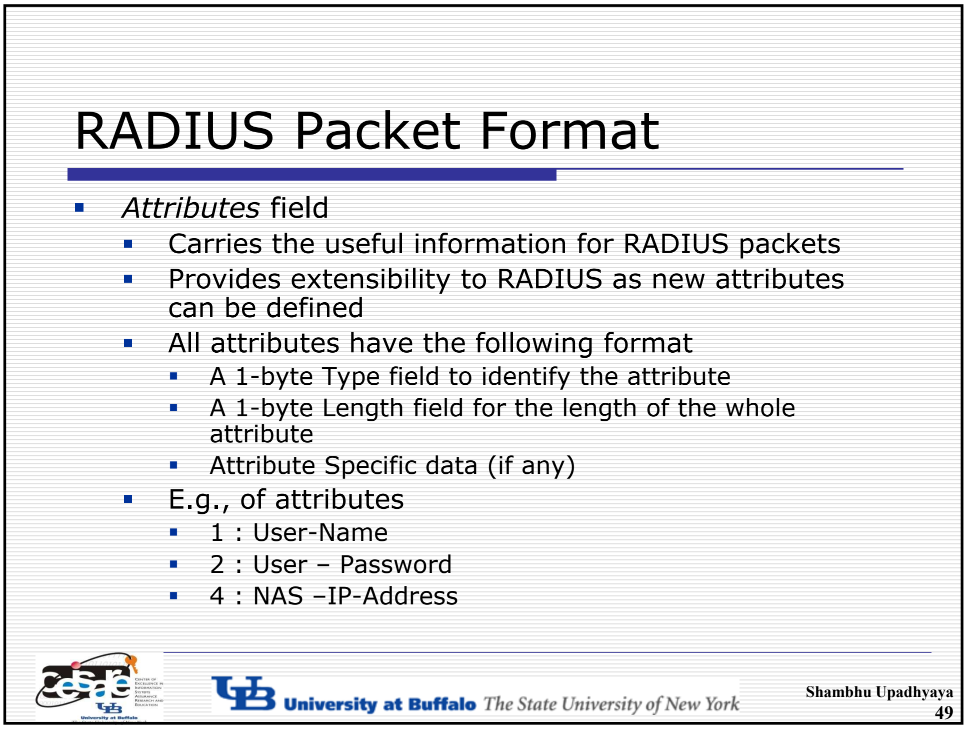
RADIUS Packet Format



- *Code* defines the message type
  - Access – Request : 1
  - Access – Accept : 2
  - Access – Reject : 3
  - Access – Challenge : 11

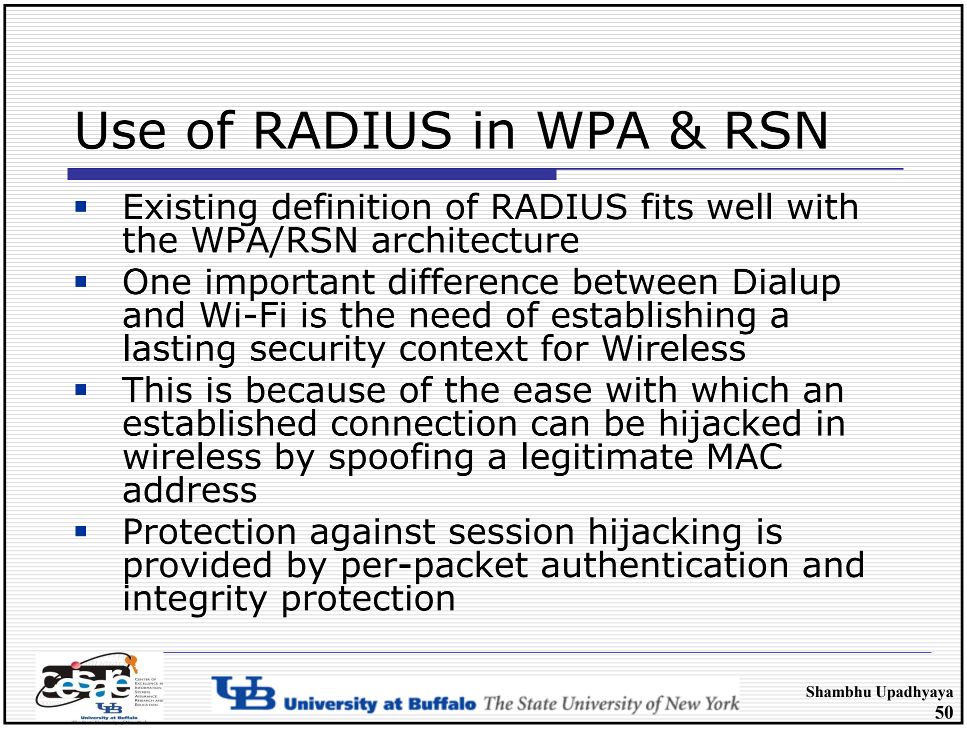
RADIUS Packet Format

- *Identifier* is an arbitrary number used to match up the request and replies
- *Length* indicates the total number of bytes in the message
- *Authenticator* field
  - Request Authenticator
    - Unpredictable and unique over the lifetime of a secret
    - Used for user-password hiding
  - Response Authenticator
    - Calculated by an MD-5 hash:
      MD5(Code + ID + Length + RequestAuth + Attributes + Secret)



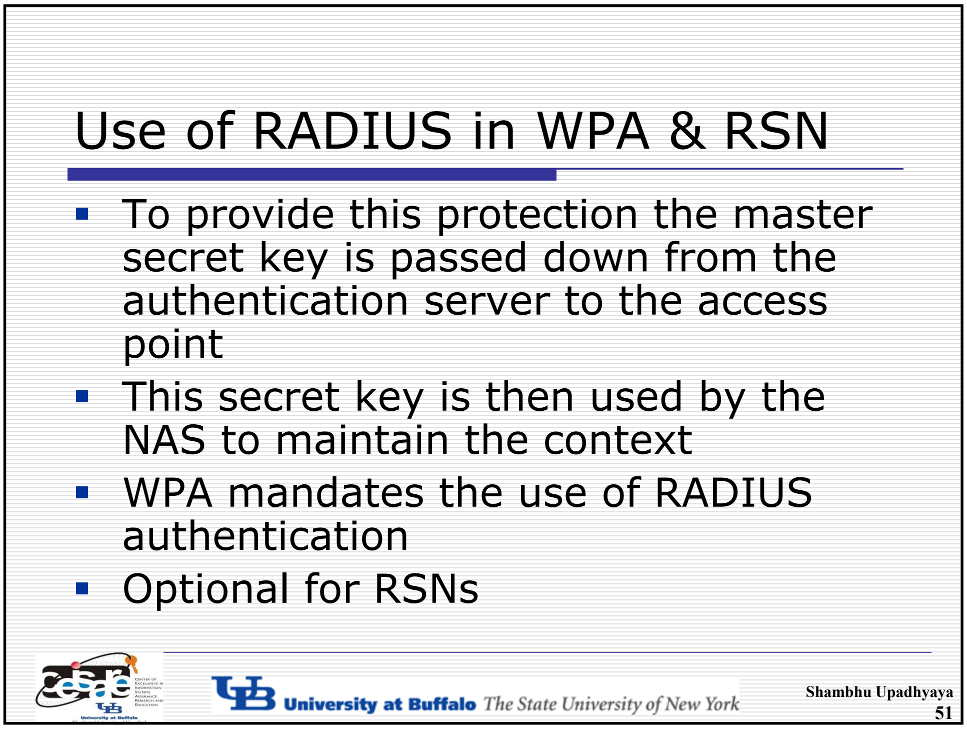
RADIUS Packet Format

- *Attributes* field
  - Carries the useful information for RADIUS packets
  - Provides extensibility to RADIUS as new attributes can be defined
  - All attributes have the following format
    - A 1-byte Type field to identify the attribute
    - A 1-byte Length field for the length of the whole attribute
    - Attribute Specific data (if any)
  - E.g., of attributes
    - 1 : User-Name
    - 2 : User – Password
    - 4 : NAS –IP-Address



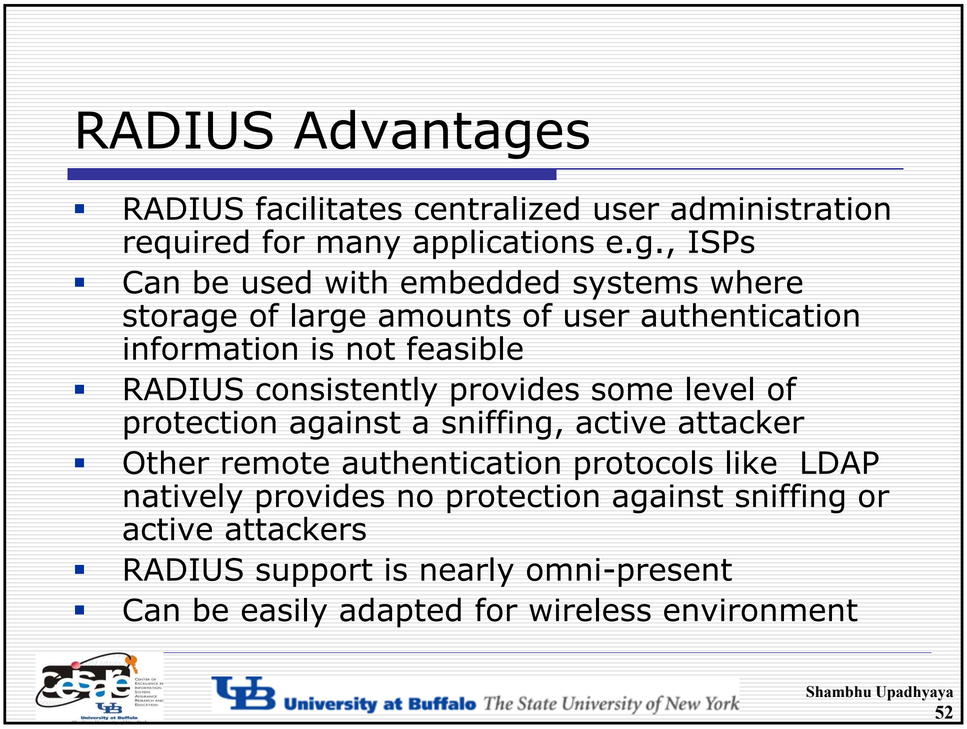
Use of RADIUS in WPA & RSN

- Existing definition of RADIUS fits well with the WPA/RSN architecture
- One important difference between Dialup and Wi-Fi is the need of establishing a lasting security context for Wireless
- This is because of the ease with which an established connection can be hijacked in wireless by spoofing a legitimate MAC address
- Protection against session hijacking is provided by per-packet authentication and integrity protection



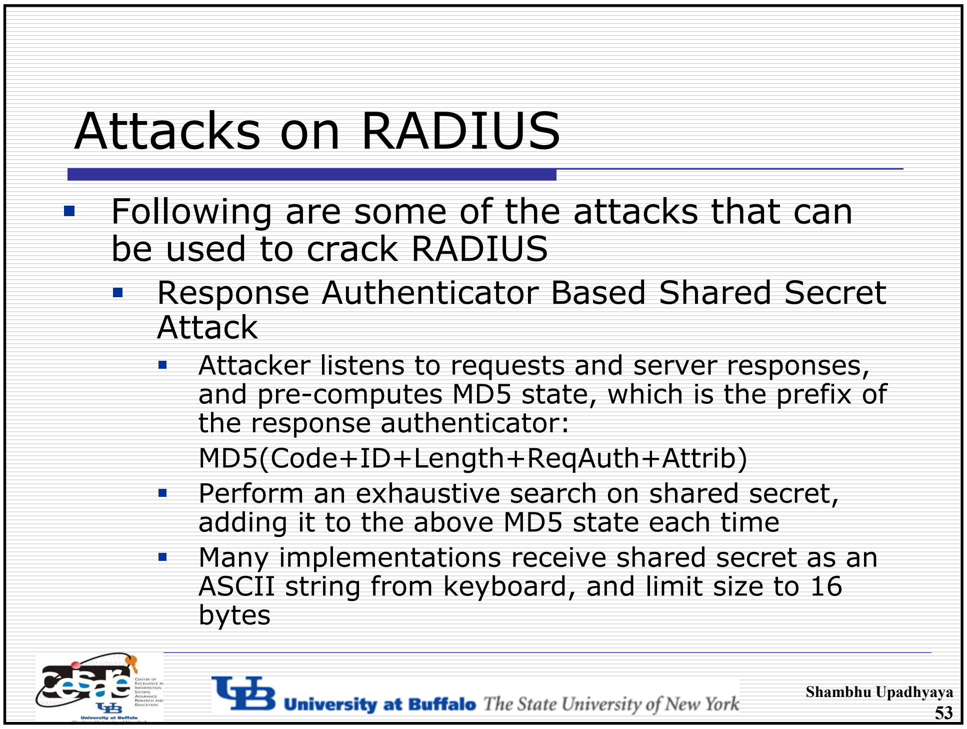
Use of RADIUS in WPA & RSN

- To provide this protection the master secret key is passed down from the authentication server to the access point
- This secret key is then used by the NAS to maintain the context
- WPA mandates the use of RADIUS authentication
- Optional for RSNs



RADIUS Advantages

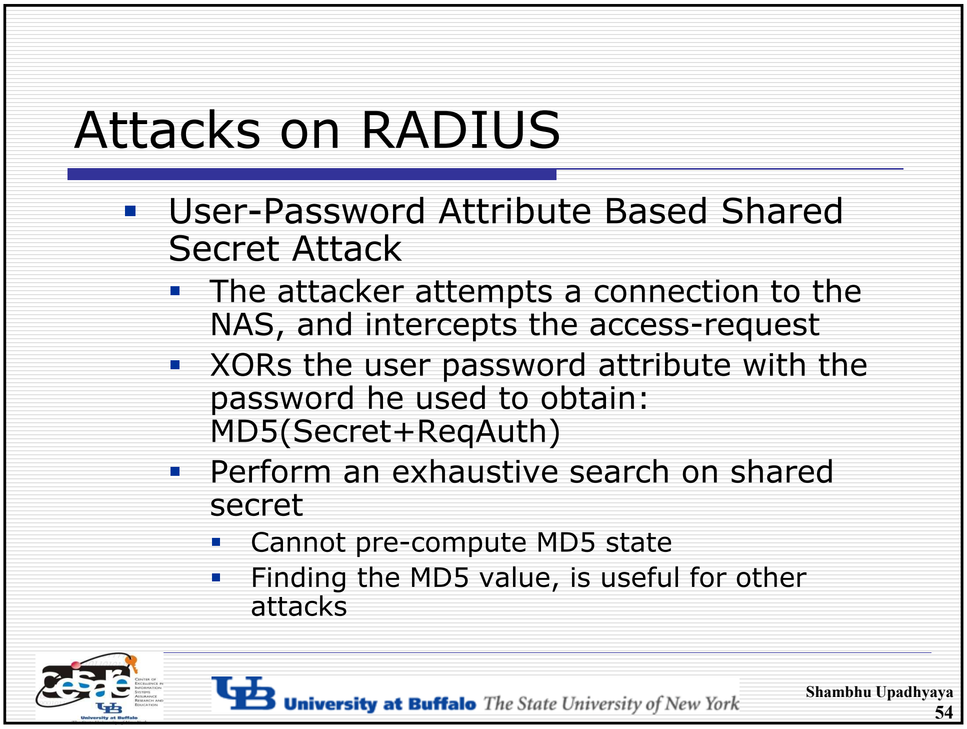
- RADIUS facilitates centralized user administration required for many applications e.g., ISPs
- Can be used with embedded systems where storage of large amounts of user authentication information is not feasible
- RADIUS consistently provides some level of protection against a sniffing, active attacker
- Other remote authentication protocols like LDAP natively provides no protection against sniffing or active attackers
- RADIUS support is nearly omni-present
- Can be easily adapted for wireless environment



Attacks on RADIUS

- Following are some of the attacks that can be used to crack RADIUS
  - Response Authenticator Based Shared Secret Attack
    - Attacker listens to requests and server responses, and pre-computes MD5 state, which is the prefix of the response authenticator:

      MD5(Code+ID+Length+ReqAuth+Attrib)
    - Perform an exhaustive search on shared secret, adding it to the above MD5 state each time
    - Many implementations receive shared secret as an ASCII string from keyboard, and limit size to 16 bytes



Attacks on RADIUS

- User-Password Attribute Based Shared Secret Attack
  - The attacker attempts a connection to the NAS, and intercepts the access-request
  - XORs the user password attribute with the password he used to obtain: MD5(Secret+ReqAuth)
  - Perform an exhaustive search on shared secret
    - Cannot pre-compute MD5 state
    - Finding the MD5 value, is useful for other attacks

Attacks on RADIUS

- Passive User-Password Compromise through Repeated Request Authenticators
  - Attacker builds a dictionary of ReqAuth and user-password attribute sent by NAS
  - When a ReqAuth repeats itself, attacker can XOR user-password attributes and obtain: password$_1$ XOR password$_2$
  - Perform a dictionary attack, combined with the fact that the ~~longer~~ shorter password is padded with 0's, causing the other password's characters XORed with it to remain unchanged

References

- Jon Edney and William Arbaugh, Real 802.11 Security, Addison-Wesley, 2004, Ch. 8
- http://www.untruth.org/~josh/security/radius/radius-auth.html