IEEE 802.11 Security and 802.1X

Dan Simon
dansimon@microsoft.com
Bernard Aboba
bernarda@microsoft.com
Tim Moore
timmoore@microsoft.com
Microsoft Corporation

IEEE 802.11

- Attempts to provide “privacy of a wire”
- RC4 stream cipher used for encryption
  - Invented at RSA Laboratories
  - RC4 encryption stream derived from WEP key + initialization vector
- No per-packet authentication
  - ICV provides integrity protection, but does not depend on the WEP key

Types of Attacks

- Physical
  - Theft of hardware
- Impersonation
  - Attacker masquerades as another person
- Integrity
  - Undetected modification of data
- Disclosure
  - Unintended exposure of data
- Denial of service
  - Keep valid users from access

Physical Threats

- User loses 802.11 NIC, doesn't report it
  - Attacker with physical possession of NIC may be capable of accessing the network
    - Implementation could encrypt WEP key on machine, require password to unlock before plumbing
    - Creates problems for machines accessible by more than one user, users who move between machines
  - With global keys, large scale re-keying required
- Without user identification and centralized authentication, accounting and auditing, difficult to detect unusual activity
  - Users who don't log on for periods of time
  - Users who transfer too much data, stay on too long
  - Multiple simultaneous logins
  - Logins from the "wrong" machine account

Impersonation: User Identification

- 802.11 does not identify users, only NICs
- Problems
  - MAC may represent more than one user
    - Multi-user machines becoming common; which user is logged on with which MAC?
  - Users may move between machines
    - Machine may allow logins by other users within the domain
    - Issue for wireless kiosks, public use clusters
  - Per-user or even machine authorization not possible
  - Not possible to authorize guest and Administrator differently

Impersonation: Rogue APs

- 802.11 shared authentication not mutual
  - Client authenticates to Access Point
  - Access Point does not authenticate to client
- Enables rogue access points
  - Denial of service attacks possible
- Solution
  - Mutual authentication
    - Require both sides to demonstrate knowledge of key

Integrity: Known Plaintext Attack

- WEP supports per-packet encryption, integrity, but not per-packet authentication
  - ICV not a keyed MIC
    - Protects against random “bit flips”, but knowledge of WEP key not required to construct it
- Given a known packet (ARP, DHCP, TCP ACK, etc.), possible to recover RC4 stream
  - Enables spoofing of packets until IV changes
    - Can insert a packet, calculate ICV, encrypt with known RC4 stream
    - Must be able to insert or modify packets in the 802.11 stream
  - Enables decryption of packets until IV changes
- Solution
  - Add a keyed message integrity check
  - Change the IV every packet

Disclosure: Passive Monitoring

- By monitoring the 802.11 control and data channels information about the Access Point and client can be obtained
  - Client and Access Point MAC addresses
    - Needed to deliver packets; disclosed by all protocols
  - MAC addresses of internal hosts
  - Time of association/disassociation
- Enables traffic analysis, long term profiling
  - Unlike IP address, MAC address is static
    - Makes it easy to attribute traffic to a user, albeit imperfectly
  - Layer 3 traffic analysis more interesting than layer 2
- Solution
  - None

Disclosure: Global Keys

- Per-user keys enabled by WEP
  - However, without dynamic key management, difficult to manage per-user keys
- Problems with static global keys
  - A secret shared by more than two is not a secret
  - Enables rogue Access Point attacks
  - Enables anyone with access to the global key to decrypt other conversations
  - Global key change requires large scale re-key

Denial of Service: Disassociation Attacks

- 802.11 associate/disassociate messages unencrypted and unauthenticated
  - Enables forging of disassociation messages
  - Creates vulnerability to denial of service attacks
- Solution
  - Keyed message integrity check

Denial of Service: Integrity Verification

- Message integrity check typically calculated on encrypted data
  - Enables receiver to see if payload has been modified before decrypting it
  - In 802.11, ICV is calculated, *then* payload is encrypted
  - Not much of an issue for RC4, AES which are very efficient in hardware and software
  - Would be an issue for more computationally intensive ciphers such as 3DES.

Disclosure: Dictionary Attacks

- In some implementations, WEP keys are derived from passwords
  - Makes it much easier to break keys by brute force
- Attacker uses a large list of words to try to guess a password and derive the key
  - Two types of dictionary attacks: pre-computed and online
  - Pre-computed assumes fixed mapping between password and key
    - Encrypted password compared against all words in list (also encrypted) until match found
  - If an nonce is included in the key derivation, then pre-computed attack more difficult

Dictionary Attacks (cont'd)

- Most password-based authentication methods vulnerable
  - Known vulnerabilities of Kerberos V
    - AS_REQ includes PADATA encrypted with a password-derived client key
      - Enables rogue access point to mount dictionary attack
    - AS_REP encrypted with password-derived client key
      - Enables passive attacker to mount online attack
- Solutions
  - Use non-password authentication
  - Don't generate WEP keys from passwords
  - If you need password-based key derivation, use EKE
    - Password-derived key used to encrypt Diffie-Helman key exchange

Password Entropy Issues

- Keys derived from user passwords are likely to be weak
  - If password is poorly chosen, the resulting key will be relatively weak and easy to break
  - Even if password is well chosen, if password entropy < key length then effective key strength is reduced
- English = 1.3 bits of entropy/character
  - 10 character password = 13 bit key!
  - Dictionary attacks easy on English passwords
- Passwords SHOULD mix upper/lower case letters, numbers, punctuation
- Random passwords
  - 6.5 bits entropy/character = log2 (52 alpha + 10 numeric + 30 specials)
  - 20 random characters required for 128 bits of entropy (22 * 6.5 > 128)

Summary of 802.11 Vulnerabilities

Vulnerability	802.11 w/per packet IV	Addition of keyed Integrity check	3DES instead of RC4	802.11 w/MIC Kerb + DES
Impersonation	vulnerable	vulnerable	vulnerable	fixed
NIC theft	vulnerable	vulnerable	vulnerable	fixed
Brute force attack (40/56 bit key	vulnerable	vulnerable	fixed	vulnerable
Packet spoofing	vulnerable	fixed	vulnerable	fixed
Rogue Access Points	vulnerable	vulnerable	vulnerable	fixed
Disassociation spoofing	vulnerable	fixed	vulnerable	fixed
Passive monitoring	vulnerable	vulnerable	vulnerable	vulnerable
Global keying issues	vulnerable	vulnerable	vulnerable	fixed
Pre-computed dictionary attack	implementation	implementation	implementation	fixed
Online dictionary attack	vulnerable	vulnerable	vulnerable	vulnerable

How To Address Security Issues?

- Addition of new 802.11 authentication methods
  - Hardware changes needed for each new method
    - Creates incentive to limit number of authentication methods supported, make new methods optional
    - Result: No upgrade path to extended authentication
  - "Hard coding" authentication methods makes it difficult to respond to security vulnerabilities
- Lessons from the school of hard knocks
  - Security vulnerabilities often found after the fact
  - Quick rollout of fixes frequently required
  - "Hard wiring" support for particular authentication technique a bad idea
    - Drives up cost of hardware
    - Prevents flexible response to security vulnerabilities
    - Inhibits introduction of new security technologies

802.1X Security Philosophy

- The solution: a flexible security framework
  - Implement security framework in upper layers
  - Enable plug-in of new authentication, key management methods without changing NIC or Access Point
  - Leverage main CPU resources for cryptographic calculations
- How it works
  - Security conversation carried out between supplicant and authentication server
  - NIC, Access Point acts as a pass through devices
- Advantages
  - Decreases hardware cost and complexity
  - Enables customers to choose their own security solution
  - Can implement the latest, most sophisticated authentication and key management techniques with modest hardware
  - Enables rapid response to security issues

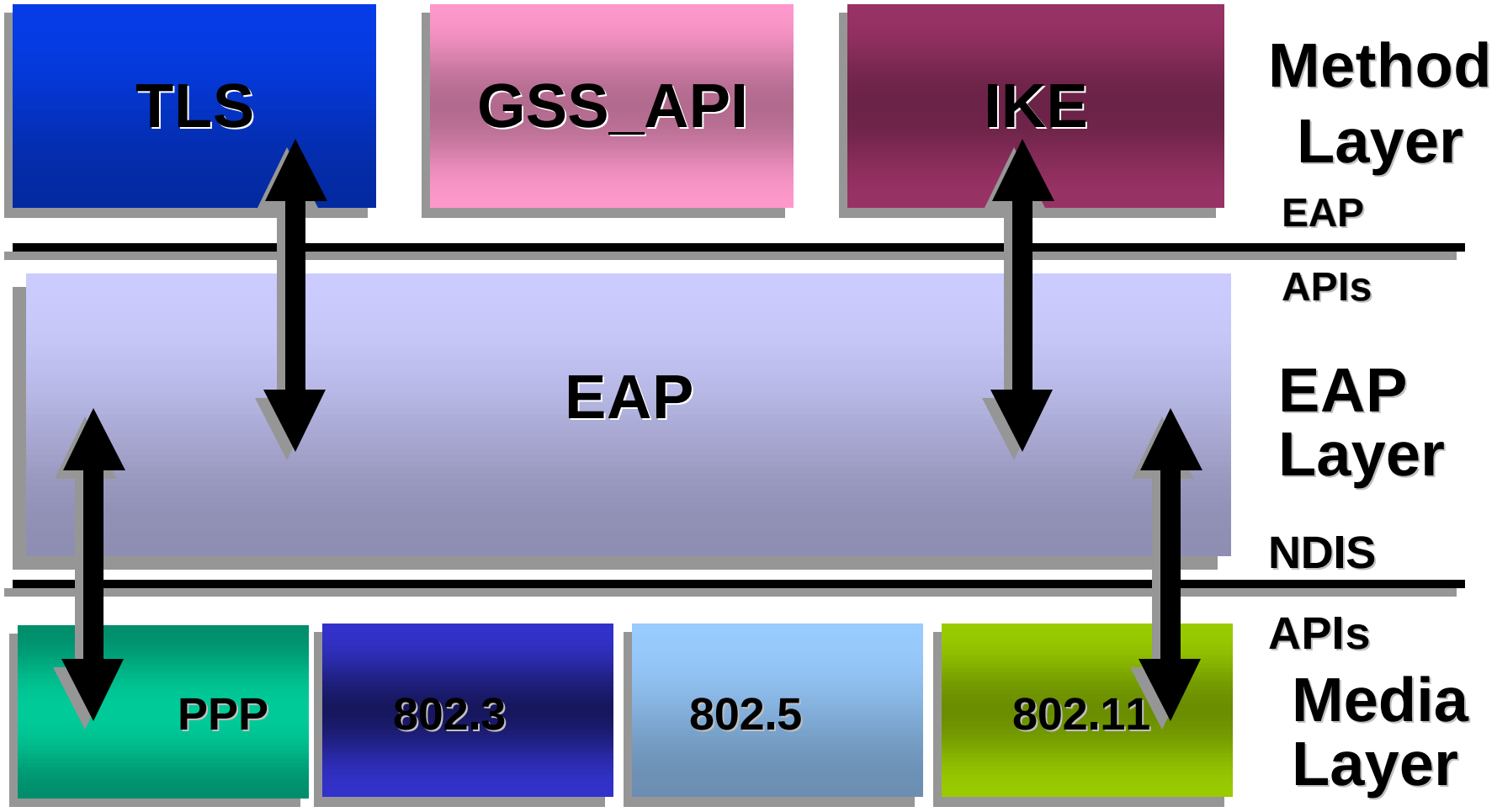
How 802.1X Addresses 802.11 Security Issues

- EAP Framework
- User Identification & Strong authentication
- Dynamic key derivation
- Mutual authentication
- Per-packet authentication
- Dictionary attack precautions

EAP Framework

- EAP provides a flexible link layer security framework
  - Simple encapsulation protocol
    - No dependency on IP
    - ACK/NAK, no windowing
    - No fragmentation support
  - Few link layer assumptions
    - Can run over any link layer (PPP, 802.3, etc.)
    - Does not assume physically secure link
      - Methods provide security services
    - Assumes no re-ordering
    - Can run over lossy or lossless media
      - Retransmission responsibility of authenticator (not needed for 802.1X or 802.11)
- EAP methods based on IETF standards
  - Transport Level Security (TLS) (supported in Windows 2000)
  - Internet Key Exchange (IKE)
  - GSS_API (including Kerberos)

EAP Architecture



User Identification & Strong Authentication

- 802.1X users identified by usernames, not MAC addresses
  - Enables user-based authentication, authorization, accounting
- 802.1X designed to support extended authentication
  - Focus is non-password based authentication
    - Public-key certificates and smartcards
    - IKE
    - Biometrics
    - Token cards
  - However, password-based authentication also supported
    - One-time Passwords
    - Any GSS_API method (includes Kerberos)

Per-User Session Keys

- 802.1X framework enables secure derivation of per-user session keys
  - Methods supporting dynamic key derivation and mutual authentication: TLS, IKE, GSS_API(Kerberos)
- Makes per-user WEP keys easy to administer
  - No longer need to store WEP keys on NIC, Access Point
- Provides improved security
  - Dynamic key derivation ensures that WEP key varies from session to session, makes attacks much more difficult
- Provides ability to securely change global keys
  - Global keys can be sent from Access Point to client, encrypted in session key

Mutual Authentication

- For use with 802.1X, EAP methods supporting mutual authentication are recommended
  - Need to mutually authenticate to guarantee key is transferred to the right entity
  - Prevents man-in-the-middle and rogue server attacks
- Common EAP methods support mutual authentication
  - TLS: server must supply a certificate, prove possession of private key
  - IKE: server must demonstrate possession of pre-shared key or private key (certificate authentication)
  - GSS_API (Kerberos): server must demonstrate knowledge of the session key

Dictionary Attack Precautions

- EAP created to support extended authentication
  - Primary focus is non-password based authentication
  - Token cards, Certificates, smartcards, one-time passwords, biometrics not vulnerable to dictionary attacks
  - Cleartext authentication not supported
  - EAP-MD5 included for minimum compatibility, but not useful for 802.11 (need mutual authentication and key derivation)
- EAP methods supporting password authentication should be carefully designed
  - Use nonces to increase entropy of key space, provide immunity against pre-computed dictionary attacks
  - Mutual authentication recommended
  - EKE recommended for maximum security in password authentication
    - Password-derived key used to encrypt Diffie-Helman exchange

Authentication & Integrity Protection

- EAP methods support per-packet authentication & integrity
  - TLS, IKE derive session key
    - TLS ciphersuite negotiations authenticated & integrity protected
    - IKE ciphersuite negotiations are encrypted, authenticated, integrity protected
    - GSS_API supports authentication, integrity protection for SPNEGO negotiated methods that support authentication and integrity protection
    - Kerberos tickets are encrypted, authenticated and integrity protected
- Authentication, Integrity protection not extended to all EAP messages
  - Notification, NAK, messages not authenticated, integrity protected
  - Identity authenticated, integrity protected in TLS, IKE (AM), Kerberos
  - Identity encrypted, authenticated, integrity protected in IKE (MM)
  - Possible to encrypt, authenticate and integrity protect Success, Failure messages using derived session key (via WEP)

Address Spoofing Attacks

- Rogue client can send EAP-Logoff message from another client's MAC address
  - Per-packet authentication required to avoid forgery
  - Access-Point needs to ensure EAP-Logoff messages come from the MAC address associated with the client key
- Rogue client can send EAP-Request messages to other STAs from Access Point MAC address
  - Access-Point should not forward packets with a source address of the access point MAC
  - Access-Point should not forward packets addressed to EAPOL multicast MAC address
    - Required by 802.1X
- Access point should check that unicast and shared keys are being used on the correct message types

Remaining Attacks

- Target Identification
  - Passive Monitoring
    - Identity messages not encrypted in EAP
    - Identity also not encrypted in TLS, Kerberos
    - Identity encrypted within IKE(MM) method so pre-method Identity disclosure not necessary in this case
- Denial of Service
  - "Bit flipping" attack on 802.11 data packets
    - 802.1X enables per-user session keys, but no keyed message integrity check in 802.11

Summary of 802.11/802.1X Vulnerabilities

	802.11 w/per packet IV	**802.1X, TLS & Key change**	**802.1X, TLS, Key Change, MIC**
Global keying	vulnerable	fixed	fixed
Impersonation	vulnerable	fixed	fixed
NIC theft	vulnerable	fixed	fixed
Brute force attack (40 bit key)	128-bit	128-bit	128-bit
Rogue Servers	vulnerable	fixed	fixed
Packet spoofing	vulnerable	vulnerable	fixed
Disassociation spoofing	vulnerable	vulnerable	fixed
Passive monitoring	MAC	Identity	Identity
Dictionary attacks	vulnerable	fixed	fixed