King Fahd University of Petroleum & Minerals Computer Engineering Dept

COE 543 – Mobile and Wireless Networks

Term 032

Dr. Ashraf S. Hasan Mahmoud

Rm 22-148-3

Ext. 1724

Email: ashraf@ccse.kfupm.edu.sa

Lecture Contents

1.

Main References

- K. Pahlavan and P. Krishnamurthy, A Unified Approach: Principles of Wireless Networks, Prentice Hall, 2002 – Section 6.4
- J. Wilkes, "Privacy and Authentication Needs for PCS," IEEE Personal Communications, August 1995, pp. 11-15
- J. Williams, "The IEEE802.11b Security Problem, Part 1," IT Professional, November-December 2001, pp. 91-95 (and the references therein)

Wireless Media

- RF is a shared media
  - Wireless communication is more susceptible to eaves dropping
- No privacy
- The presence of the communication request does not uniquely identify the originator

- Need for Privacy and Authentication

None Cryptographic Means

- Number Assigned Module (NAM) and Electronic Serial Number (ESN)
  - Used for authentication
- Using the > 900 MHz band
  - Outside the range of typical scanners

- Which is more secure FDMA, TDMA, or CDMA?

- None cryptographic methods usually do not provide the proper solution

---

http://www.philzimmermann.com/

Levels of Privacy

- Level 0: None – with no privacy enabled
  - Anyone with digital scanner can monitor calls
  - A "lack of privacy" indicator should be provided – a public trust issue
- Level 1: Equivalent to Wireline
  - Most people assume wireline calls are secure – eaves dropping can be detected – not as in wireless
  - Used for routine every day calls
  - Would take a year or so to break encryption – would require same effort to break every call
- Level 2: Commercially Secure
  - For proprietary info
  - Would take 10~25 yrs to break encryption – would require same effort to break every call
- Level 3: Military/Government Secure
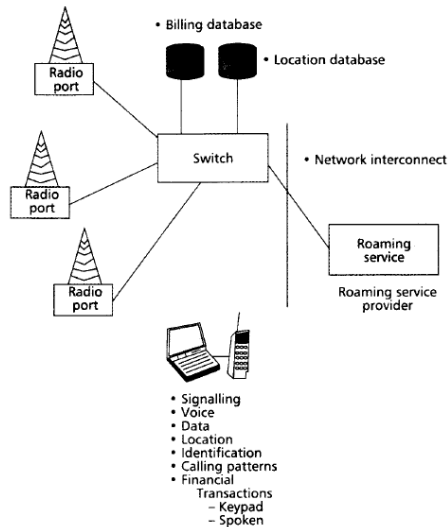 - None breakable?

Privacy Requirements

- Privacy of Call Setup Information
  - Calling #, calling card #, type of service, etc.
- Privacy of Speech
  - Must be encoded and none interceptable
- Privacy of Data
  - Must be encoded and none interceptable
- Privacy of User Location
  - Location should not be disclosed – encrypting user id
  - Remember HLR and VLR have this info – must not be subject to attacks

Privacy Requirements – cont'd

- Privacy of User ID
  - User ID may be encrypted
  - Prevents analysis of calling patterns for this ID – VERY IMPORTANT
- Privacy of Calling Patterns
  - No info sent from mobile should allow traffic analysis
  - This info: calling #, frequency of use, caller identity
- Financial Transactions
  - Visa card # or bank transactions over the air!!
  - Securing the DTMF

Privacy Requirements

- Billing database
- Location database
- Network interconnect

Radio port

Switch

Roaming service

Roaming service provider

- Signalling
- Voice
- Data
- Location
- Identification
- Calling patterns
- Financial
  Transactions
  – Keypad
  – Spoken

Theft Resistance Requirements

- Cryptographic design should make the reuse of stolen personal terminal difficult
  - Even if registered to a new legitimate account
- Clone Resistant Design
  - Mobile unique info must not be compromised
    - Over the air – eaves dropping
    - From the network – secure databases
    - From network interconnect – info passed between systems for security checking of roaming mobiles must have enough info to authenticate the mobile and not enough info to clone it!!
    - From users cloning their own mobiles

Theft Resistance Requirements – cont'd

- Installation Fraud
  - Cryptographic system must be designed to that installation cloning is reduced or eliminated
- Repair Fraud
- Unique User ID
  - Identify the correct person using the mobile for billing purposes
- Unique mobile ID
  - Different than user ID
  - Smart card or PCMCIA card containing all security info

Radio System Requirements

- Multipath Fading
  - Immune to sever burst errors
- Thermal Noise/Interference
  - The modulation scheme and the cryptographic system must be designed so that interference with shared users of the spectrum does not compromise the security of the system
- Jamming
  - Should work in the face of jamming – does not break
- Support for Handovers

Other Requirements

- Lifetime of ~20 years:
  - An algorithm that is secure today may be breakable in 5 to 10 years
- Physical Requirements:
  - Mass production
  - Exported and Imported
  - Minimal impact on handset size, weight, power consumption, etc.
  - Low-cost Level 1 implementation

Other Requirements – cont'd

- Law Enforcement Requirements
  - With the right court order, the law enforcement should be able to tap into the wireless calls
  - Over the air:
    - No encryption – easy
    - Breakable encryption
    - Strong encryption – problematic – need to obtain key
  - Wiretap at switch:
    - Preferred method – easiest

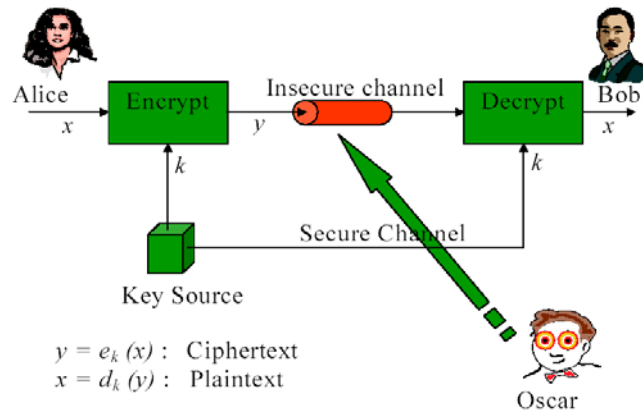# Network Security - Services

- (Def): Specific measures employing security mechanisms that combat security attacks on a network
- Include:
    - <u>Confidentiality or Privacy</u>: resistance to interception
    - <u>Message Authentication</u>: integrity of message and a guarantee that the sender is who he/she claims to be – Attacks: message modification or impersonation of sender
    - <u>Nonrepudiation</u>: service against denial by either party of creating or acknowledging a message – similar to digital signatures based on public key encryption – Attacks: fabrication
    - <u>Access Control</u>: only authorized entities can access – Attacks Masquerading
    - <u>Availability</u>: access to resources is not prevented by malicious entities (remember www.aljazeera.net!!) – Attacks: denial of service

Privacy

- Encryption
    - one way of providing most of the previously listed services
    - SHOULD be computationally secure – non breakable ideally
- Terms:
    - Message – plaintext or cleartext
    - Encoded version – ciphertext
    - Key – k
- Time and Cost to break the scheme should be significant relative to protected value
    - Should assume interceptor has access to plaintext-ciphertext pairs

Conventional Encryption Model

- Secret-Key Algorithm

$y = e_k (x)$:   Ciphertext
$x = d_k (y)$:   Plaintext

Secret Key Algorithms

- Example: Data Encryption Standard (DES)
- A symmetric key algorithm
  - Key used for encryption is the same as that used for decryption
- Two Principles:
  - Confusion ←→ scrambling of original data
  - Diffusion ←→ creating randomness – can not relate changes to plaintext to those of ciphertext
- Most secret-key algorithms are unbreakable except by brute-force
  - Key length of n bits → at least 2^{n-1} steps to break encryption – why?
- Main advantage – fast; appropriate for fast data streams
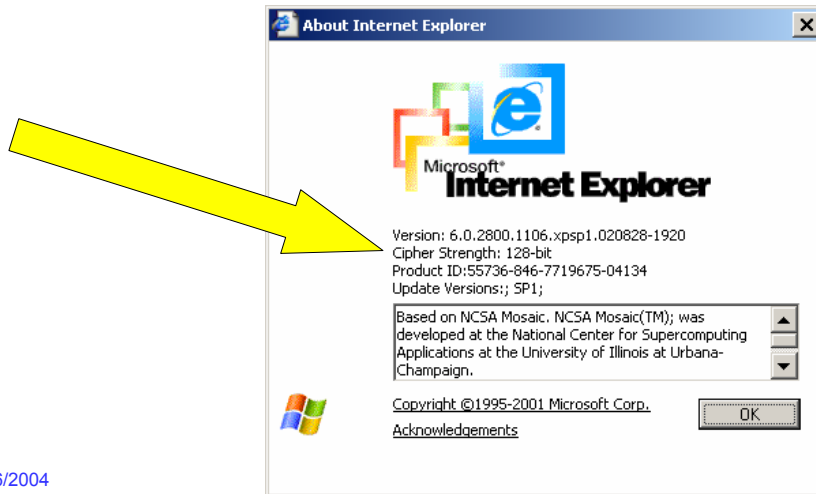 - Compared to public-key algorithms

Date Encryption Standard (DES) – cont'd

- Usually a key size of 128 bits is recommended

5/16/2004

Example 6.20: Breaking DES

- DES is a block cipher: encrypts blocks of 64-bits of data using keys (56 bit long).
- Using brute force:
  - Use 500 MHz chip (each cost $20)
- How much time and money does it cost to break DES?

- **Solution:**
- Total # of keys = 2^{56} = 7.2×10^{16}
  - On average half the keys will be tried → 2^{55} keys
- If it takes one clock cycle to test every key → time needed = 2^{55} / (500 X 10^6) /(60X60X24) = 834 days
- If 834 chips are used in parallel → code can be broken in one day
- Cost = $20 X 834 = $16,680

5/16/2004   Dr. Ashraf S. Hasan Mahmoud   20

Example 6.21: Moore's Law

- Processor or chip speed doubles every 18 months ➔ Strength of *any* encryption technique is weakened by time.

- DES algorithm using 112 bit keys can be broken in a day in 100 years from now!!

Example 6.21: Key Sizes

- IEEE802.11 – Wired-equivalent privacy (WEP): 40-bit key

- IS-136 – 64-bit key – more secure but still considered weak

Public-key Algorithms

- Every pair of users have to have a key
    - A network of N users require the distribution of N(N-1)/2 keys!
    - Large and impractical for large N

- Key distribution schemes:
    - E.g: Needham-Schroeder – Kerberos
    - Involves several handshaking steps – start with a shared *master key*
- Concept introduced by Diffie and Hellman in 1977

Exploring Diffie-Hellman Encryption
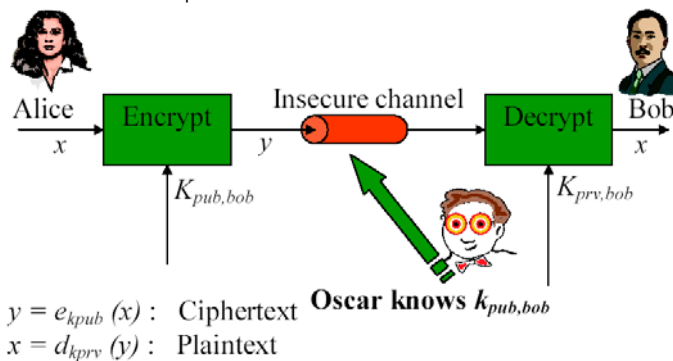Posted on Friday, August 16, 2002 by Jack Dennon
http://www.linuxjournal.com/article.php?sid=6131

Public-key Algorithms – cont'd

- It is extremely easy to compute $y = f(k_{pub}, x)$
- Given k_{pub}, and y, it is computationally not feasible to determine $x = f^{-1}(k_{pub}, y)$
- With a knowledge of k_{prv} that is related to k_{pub}, it is easy to determine $x = f^{-1}(k_{prv}, y)$

$y = e_{kpub}(x)$: Ciphertext
$x = d_{kprv}(y)$: Plaintext

Oscar knows $k_{pub,bob}$

Public-key Algorithms – cont'd

- *f(.)* ~ belongs to a group of functions referred to
as a trapdoor one-way function - e.g:
    - Factorization:
        - It is easy to find 7 x 17 x 109 x 151 = 195, 821;
        - but it is quite difficult to split 30,616,693 into its prime number factors
    - Discrete logarithm:
        - It is easy to determine 2^{23} mod 109 is 77;
        - But it is difficult to find out u such that 2^u mode 109 is 68

- Since k_{pub} is available and the method is based on a mathematical structure ➔ need to be 3 to 15 times larger than the secret-key counter parts
- Elliptic Mathematics (refer to: http://world.std.com/~dpj/elliptic.html) provides a mean to use smaller keys with same level of security

Public-key Algorithms – Examples

- Rivest-Shamir-Adelman (RSA)
    - Employs integer factorization
    - Most popular
- Diffie-Hellman key-exchange
    - Based on discrete logarithm
    - Wireless networks
    - Used for key exchange for web transactions, e-commerce, IP security.
    - See appendix 6A for details
- Digital Signature Standard (DSS)
    - Based on discrete logarithms

Public-key Algorithms – Characteristics

- Computationally intensive
- Encryption rates quite small
- Rarely used for bulk data transfer
- Usually used to exchange a *session* key – to use a secret-key algorithm for later communications
    - Different session key each time!

Cost Equivelant Key Lengths (in Bits) of Various Encryption Schemes

Secret-key Algorithm	Elliptic Curve	RSA	Time to Break	Memory
56	112	430	Less than 5 mins	Trivial
80	160	760	600 months	4 Gb
96	192	1,020	3 million years	170 Gb
128	256	1,620	10^{16} years	120 Tb

Block vs. Stream Ciphers

- Block Ciphers – DES and Advanced Encryption Standard (AES)
    - Encrypt blocks of data at a time
    - Requires buffering and padding
- Stream Ciphers – no need for buffering
    - More suitable for a jitter-sensitive service
    - Usually a simple XOR operation is used
- Example:
    - IEEE802.11 employs the encryption algorithm RC-4 to generate a pseudorandom key stream using a 40-bit master key and an initial vector (IV)
    - Data is simply XORed with the key to create ciphertext

Message Authentication

- Involved:
    - Sender authentication
    - Message integrity

- This is accomplished using a message digest (MD) and a message authentication code (MAC)
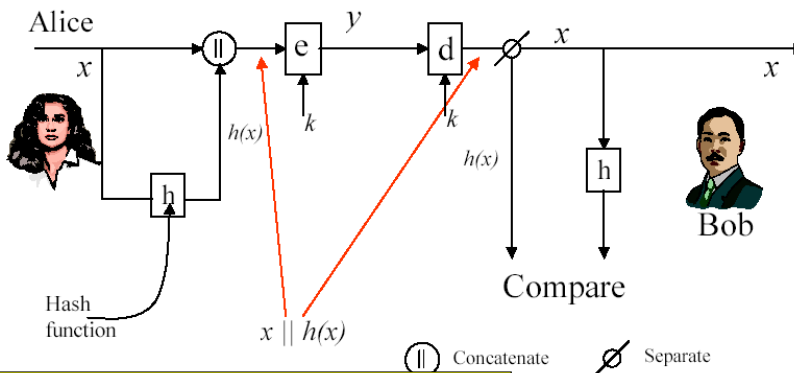
Message Authentication Code (MAC)

- MAC creates a fixed-length sequence of bits that depend on the message and the secret key
  - Not a function of message size
  - It is computationally infeasible to generate the MAC without the original message and key
- Message is then delivered (with the MAC) to destination
- Receiver computes MAC again based on received message
- New MAC is equal to old MAC IFF message was not tampered with (remember secret key is a secret!)

Message Digest (MD)

- MD depends only on the message x
- A hash function, h, is used to create the MD, h(x)
- The MD is appended to the message x ➔ x || h(x)
- The newly overall message x || h(x) is encrypted using the secret-key
- h(x) has to be sufficiently long
  - For a b bit h(x) ➔ a fake message with same h(x) can be generated in $2^{b/2}$ trails

Message Authentication with Hash Functions

Alice

x

Hash function

$h(x)$

$x \parallel h(x)$

y

$e \leftarrow k$

$d \leftarrow k$

$h(x)$

x

h

Bob

Compare

$\parallel$ Concatenate $\emptyset$ Separate

What is a hash function? Refer to http://www.rsasecurity.com/rsalabs/faq/2-1-6.html
- some of the hash function properties:
- The input can be of any length.
- The output has a fixed length.
- $H(x)$ is relatively easy to compute for any given x.
- $H(x)$ is one-way.
- $H(x)$ is collision-free.

ud   33

MD and HMAC C++ code

- From http://njet.org/doc/Doc/$24$24native/anvil/crypto.html

- **Message Digest (MD)** provides applications the functionality of a message digest algorithm, such as MD5 or SHA. Message digests are secure one-way hash functions that take arbitrary-sized data and output a fixed-length hash value.
- **Message Authentication Code (MAC)** Since everyone can generate the message digest, it may not be suitable for some security related applications. Because of this, Anvil[+] also supports HMAC (rfc2104), which is a mechanism for message authentication using a (secret) key. So you can use a key with a hash algorithm to produce hashes that can only be verified using the same key.

[+] Anvil is a crypto library that can create message hash codes or checksums from any data. It is posted on the webpage listed above.

Digital Signature

- Def: a 'message digest' encrypted using the sender's private key
  - The receiver can verify the identity of the sender and the integrity of message by first decrypting the signature using the sender's public key – and then by reproducing the message digest and comparing it with the one received with message.

- What if a public key is not valid?
  - Use of Certificate Authority
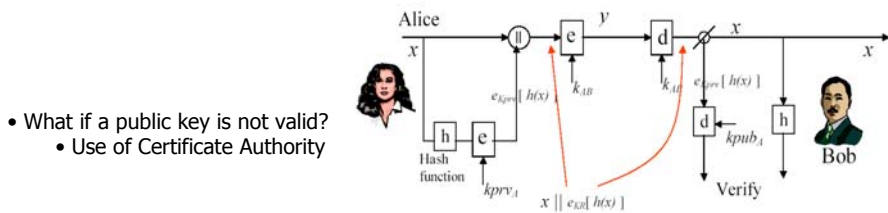
Methods for Providing Security for Mobile Wide Area Networks

- MIN/ESN
- Shared Secret (Key) Data
- Security Triplets (Token Based)
- Public Key

MIN/ESN Authentication

- MIN = Mobile Identification Number (e.g. 10-digits)
- ESN = Electronic Serial Number (e.g. 32-bit)
- Data is shared between systems on bad MINs, ESNs, and MIN/ESN pairs
- When a roaming phone places a call, the bad list is checked, and then a message is sent to home system to validate the MIN/ESN (using SS7 on IS-41)

Shared Secret Data (SSD) Authentication

- Developed for TDMA systems (IS-54 and its derivatives)
- Utilizes a common authentication key in the mobile telephone and the network.
- When phone is placed in service a 64-bit A-key is entered into phone and network (HLR)
- From A-key two keys are derived: SSD-A and SSD-B – these are used to authenticate the phone and establish the voice privacy key
- Mobile is assigned a Temporary IMSI (TIMSI) when roaming into a foreign network – its identity (IMSI) is kept secret
- Mobile is authenticated by calculating AUTHR (an encrypted version of RAND sent by basestation) – encryption is done using SSD-A
- Mobile also possess a call-counter profile – every time the mobile makes a call, the counter is increments
    - A measure against cloning
- Procedures:
    - Shared Secret Key Registration
    - Shared Secret Key Global Challenge
    - Shared Secret Key Unique Challenge

All mobiles are assigned:
- ESN
- 15-digit International Mobile Subscriber Identity (IMSI)
- An A-key
- Plus other info

Token Based Authentication – GSM

- Triplets:
    - pseudorandom number RAND;
    - its corresponding response, SRES, generated by authentication algorithm;
    - Temporary encryption key, Kc, used for data, signaling and voice privacy
- Triplets are requested by the visitor system from the home system
    - Computed and stored in the mobile, home authentication centre and the visited VLR
- Procedure: MS sends registration request – network sends unique challenge – MS calculates challenge response and sends message back to network. VLR contains list of triplets – compares with response from MS
    - The just-used triplet is discarded
    - After all triplets are used – VLR query HLR for a new set
- Anonymity is handled using IMSI/TIMSI
- No call history counter for GSM – no clone detection is possible
- Subscriber Identity Module (SIM) – microprocessor-based secure system

Public-Key-Based Authentication

- Public-key method – two user keys are used
    - Public (USERPUB) for encrypting
    - Private (USERPRIV) for decrypting
- The network also has NETPUB and NETPRIV

- Used in PACS

Summary of Authentication Methods*

	Type of Authentication				
Air Interface	MIN/ESN	SSD	Token-Based	Public Key	Type of Voice Privacy Supported
AMPS	x	x			None
CDMA		x			Strong
GSM			x		Strong
PACS		x		x	Strong
PCS-2000		x	x		Strong
TDMA		x			Weak
W-CDMA		x			Strong

•From V. Garg and J Wilkes, Wireless And Personal Communications Systems, Printice Hall PTR, 1996 – chapter 10

Identification Schemes

- Need:
    - Access to an automatic teller machine
    - Logging on to a computer
    - Identifying a user of a cellular phone
    - Etc.
- Identification = entity authentication
    - A password or a pin compared to a securely stored hash value
    - Susceptible to replay attacks if transmitted over-the-air in an insecure manner
- Challenge-Response identification or Strong identification
    - Used in wireless networks
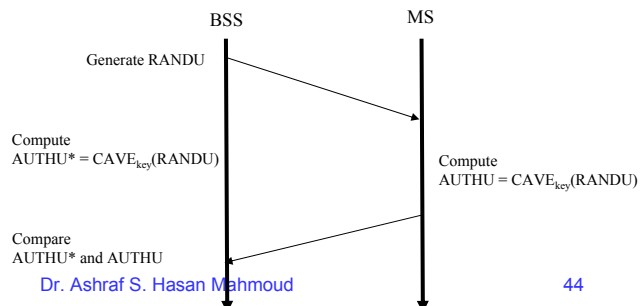
Identification Schemes – cont'd

- ## A nonce: a value employed no more than once for the same purpose
  - ## Eliminates *replay* attacks

Identification Schemes – cont'd

Example: Challenge-Response mechanism in IS-41

1. Consider an IS-136 digital TDMA network
2. The network (BSS) generates a random # RANDU and sends it over the air to mobile
3. Mobile computes a value AUTHU using the encryption algorithm Cellular Authentication and Voice Encryption (CAVE)
4. AUTHU is sent to network and compared with a computed version at the network
5. If the two AUTHU match ➔ the mobile is authenticated – using IS-41 terminology

```
           BSS                              MS

Generate RANDU

Compute
AUTHU* = CAVE_key(RANDU)
                                    Compute
                                    AUTHU = CAVE_key(RANDU)

Compare
AUTHU* and AUTHU
```

$AUTHU^* = CAVE_{key}(RANDU)$
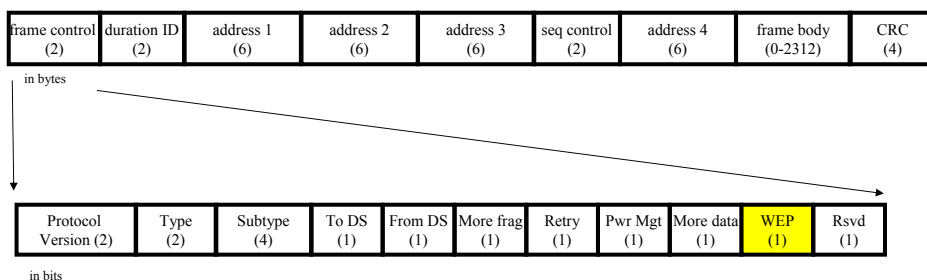
$AUTHU = CAVE_{key}(RANDU)$

IEEE802.11 Security & Privacy

- Objectives:
  - To provide a wired equivalent privacy (WEP)
  - To protect against
    - Eavesdropping
    - Unauthorized access

1. http://www.cs.umd.edu/~waa/wireless.html and the references therein especially the following paper: "Your 802.11 network has no clothes,"
2. http://www.mobileinfo.com/Security/index.htm

MAC Frame Format

- General MAC frame format & Control Field
- WEP = 1 ➔ data bits are encrypted (refer to chapter 11 of Pahlavan)

frame control (2)	duration ID (2)	address 1 (6)	address 2 (6)	address 3 (6)	seq control (2)	address 4 (6)	frame body (0-2312)	CRC (4)

in bytes

Protocol Version (2)	Type (2)	Subtype (4)	To DS (1)	From DS (1)	More frag (1)	Retry (1)	Pwr Mgt (1)	More data (1)	WEP (1)	Rsvd (1)

in bits

Authentication Schemes for IEEE802.11

- Three schemes:
    1. Open system authentication
        - Default – uses SSID as a password to gain access
        - NULL Authentication function – authenticates anyone requesting authentication
        - Not secure
    2. Shared key authentication (WEP based)
        - 40-bits key
        - Not very secure
        - Standard does not specify key management or where to get this key from!!
        - Optional for IEEE802.11 (required to be Wi-Fi certified by WECA)
    3. Access Control List (MAC address filtering)
        - MAC address based
        - Not scalable – requires manual setting
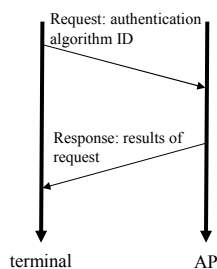- Not available for ad-hoc

http://www.cs.umd.edu/~waa/wireless.html (802.11 Security Vulnerabilities)
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Authentication Schemes for IEEE802.11

Request: authentication algorithm ID

Response: results of request

terminal   AP

Open System Authentication

Authentication Mgt request frame

Challenge text (128 B)

Encrypted challenge text

Authentication result

terminal   AP
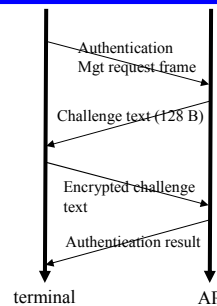
Shared-key Authentication

Challenge text: The challenge text is generated by using the WEP pseudo-random number generator (PRNG) with the "shared secret" and a random initialization vector (IV)

Challenge response: encrypted with WEP using the "shared secret" along with a new IV

Security Threats

- Theft of Hardware
  - Admin has to reprogram WEP keys
- Rogue Access Points
  - IEEE802.11b shared-key authentication is one way (i.e. AP authenticates mobile)
  - User can not authenticate AP ➔ rogue APs
- Per-packet encryption versus per-packet authentication ➔ to protect against spoofing and replay attacks
  - WEP keys may change frequently
  - Use per-session WEP keys

Privacy in IEEE802.11
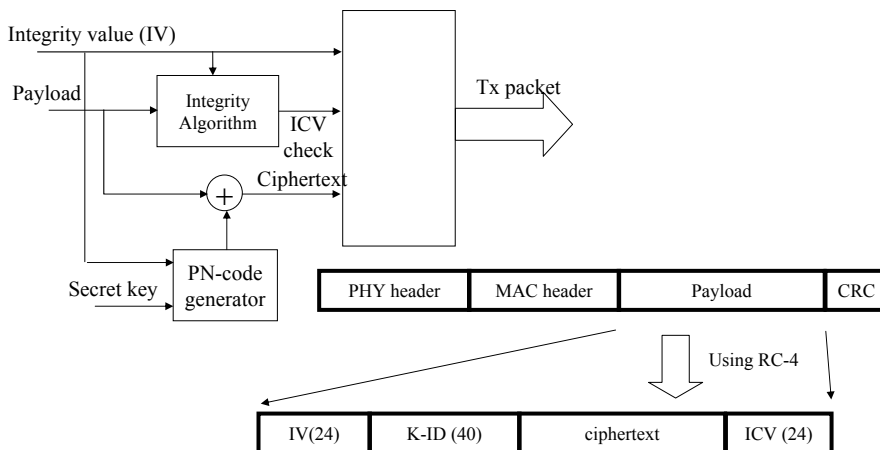
Note that the IV and the key-ID are sent in the clear!
Same shared key for uplink and downlink

RC4 Encryption (Stream Cipher)

- *Reasonable* strong:
  - A brute force attack on this algorithm is difficult since every frame is sent with a different IV
  - IV restarts the pseudo random number generator (PRNG) for each frame
- Self-Synchronizing:
  - Even if some intermediate frames are lost, the WEP algorithm resynchronizes at each frame

Encryption Keys

- Window of four keys
  - Can be manually configured – up to four keys
  - Each is 40 bits (5 ascii or 10 hex digits)
  - For all network
- Key-mapping table
  - Each unique MAC address has separate keys – one per device
  - Need to be configured manually
  - Most secure