Lecture Contents

1.
Main References

- 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

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 – eavesdropping 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?

http://www.philzimmermann.com/
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

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:
  - Confidentiality or Privacy: resistance to interception
  - Message Authentication: integrity of message and a guarantee that the sender is who he/she claims to be – Attacks: message modification or impersonation of sender
  - Nonrepudiation: service against denial by either party of creating or acknowledging a message – similar to digital signatures based on public key encryption – Attacks: fabrication
  - Access Control: only authorized entities can access – Attacks Masquerading
  - Availability: 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

\[ y = e_k(x) : \text{Ciphertext} \]
\[ x = d_k(y) : \text{Plaintext} \]

Date Encryption Standard (DES)

- A symmetric key algorithm
  - Key used for encryption is the same as that used for decryption
- Two Principles:
  - Confusion \( \leftrightarrow \) scrambling of original data
  - Diffusion \( \leftrightarrow \) 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 \( \rightarrow \) at least \( 2^{n-1} \) steps to break encryption
- 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

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:
  - Needham-Schroeder
  - Kerberos

- Concept introduced by Diffie and Hellman in 1977
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 \( x = f^{-1}(k_{prv}, y) \)

\[ y = e_{k_{pub}}(x) : \text{Ciphertext} \]
\[ x = d_{k_{prv}}(y) : \text{Plaintext} \]

Oscar knows \( k_{pub, bob} \)

Public-key Algorithms – cont’d

• \( f \approx \) belongs to a group of functions referred to as a trapdoor one-way function - e.g. factorization problem and discrete logarithm

• Since \( k_{pub} \) is available and the method is based on a mathematical structure \( \Rightarrow \) 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](http://world.std.com/~dpj/elliptic.html)) provides a mean to use smaller keys with same level of secuirty
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 Equivalent Key Lengths (in Bits) of Various Encryption Schemes

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

### 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 \( \Rightarrow x \ || \ h(x) \)
- 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) \( \Rightarrow \) a fake message with same h(x) can be generated in \( 2^b/2 \) trails

Message Authentication with Hash Functions

What is a hash function?
Refer to http://www.rsasecurity.com/rsalabs/faq/2-1-6.html
MD and HMAC C++ code


- **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.

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

Example:
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

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
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](http://www.cs.umd.edu/~waa/wireless.html) and the references therein especially the following paper: "Your 802.11 network has no clothes."

MAC Frame Format

- General MAC frame format & Control Field
- WEP = 1 → data bits are encrypted (refer to chapter 11 of Pahlavan)
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
  3. Access Control List (MAC address filtering)
     - MAC address based
     - Not scalable – requires manual setting
- Not available for ad-hoc

Authentication Schemes for IEEE802.11

<table>
<thead>
<tr>
<th>Request: authentication algorithm ID</th>
<th>Authentication Mgt request frame</th>
</tr>
</thead>
<tbody>
<tr>
<td>Response: results of request</td>
<td>Challenge text (128 B)</td>
</tr>
<tr>
<td></td>
<td>Encrypted challenge text</td>
</tr>
<tr>
<td></td>
<td>Authentication result</td>
</tr>
</tbody>
</table>

Terminal AP

**Open System Authentication**

**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.
Privacy in IEEE802.11

![Diagram of Privacy in IEEE802.11]

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