Securing Your Wireless Devices: Fundamental Principles and Enabling Technologies

Vireshwar Kumar, Jung-Min (Jerry) Park
Bradley Department of Electrical and Computer Engineering

Wireless@VT Symposium
May 28, 2015
1. Introduction to Wireless Security

2. Attack Model

3. Countermeasure
   a) Advanced Encryption Standard (AES)
   b) IEEE 802.11i Standard

4. Security in Wireless Networks with Spectrum Sharing

5. Summary
1. Introduction to Wireless Security

(a) Need for Wireless Security
### Security Breaches Across Industries

#### Banking & finance
- No incidents: 20%
- Identity theft: 20%
- Customer records compromised or stolen: 23%
- Financial Losses: 23%
- Denial of service attacks: 29%
- Financial Fraud: 36%

#### Government
- No incidents: 16%
- Confidential records (trade secrets or IP) compromised or stolen: 19%
- Identity theft: 19%
- Denial of service attacks: 22%
- Operating systems/files altered: 24%
- Unauthorized access/use of data, systems, networks: 24%

#### Information & telecom
- Software applications altered: 11%
- Unauthorized access/use of data, systems, networks: 19%
- Operating systems/files altered: 20%
- No incidents: 28%
- Denial of service attacks: 28%
- E-mail or other applications unavailable: 33%

@ US cybercrime: Rising risks, reduced readiness Key findings from the 2014 US State of Cybercrime Survey
82% of companies with high performing security practices collaborate with others to deepen their knowledge of security and threat trends

69% of US executives are worried that cyber threats will impact growth

59% of respondents said that they were more concerned about cybersecurity threats this year than in the past

49% of all respondents have a plan for responding to threats
Contributing Factors to Security Incidents

- Lack of awareness of threats and risks

- **Wide open network policies**
  - Vast majority of Internet traffic is unencrypted and can be captured and/or monitored

- Lack of security in the TCP/IP protocol suite

- **Complexity of security management and administration**
  - Bloated and buggy software
  - Increased availability of hacking tools
Role of Wireless Environment

- **Channel**
  - Susceptible to eavesdropping and jamming
  - Vulnerable to active attacks that exploit vulnerabilities in protocols

- **Mobility**
  - Wireless devices are portable and mobile
  - This mobility results in a number of risks

- **Resources**
  - Wireless devices, such as smartphones and tablets, have sophisticated operating systems but limited memory and processing resources with which to counter threats, including denial of service and malware

- **Accessibility**
  - Some wireless devices, such as sensors and robots, may be left unattended in remote and/or hostile locations
1. Introduction to Wireless Security

(b) Meaning of Security
Security objectives according to NIST standard FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems)

- **Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal *privacy* and *proprietary information*.

- **Integrity**: Guarding against improper information modification or destruction, including ensuring info. *nonrepudiation* and *authenticity*.

- **Availability**: Ensuring timely and reliable access to and use of information.

Also called the “CIA triad”.

Confidentiality

Integrity

Availability

Secure
Concepts that are often discussed in addition to the CIA

- **Authenticity**: The property of being genuine and being able to be verified and trusted; confidence in the validity of a TX, a message, or message originator.
  - FIPS 199 includes authenticity under integrity

- **Accountability**: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.
  - This supports **nonrepudiation**, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
  - Ability to trace a security breach to a responsible party.
Security Models for Evaluating Cryptographic Primitives & Protocols

- Unconditional security
  - Information theoretic measure of security
  - Adversary has unlimited computational resources

- Complexity-theoretic security
  - Adversaries are modeled as having polynomial computational power
  - A proof of security relative to an appropriate model of computation is defined

- Provable security
  - Difficulty of defeating a primitive can be shown to be essentially as difficult as solving a well-known difficult problem

- Computational security
  - Measures the amount of computational effort required, by the best currently-known methods, to defeat a system

- Ad hoc security
  - Convincing arguments that every successful attack requires a resource level greater than the fixed resources of a perceived adversary
1. Introduction to Wireless Security

(c) Illustrative Examples of Security Attacks in Wireless Local Area Network (WLAN)
Ex. 1 - Sniffing Attacks

- Sniffing: An attacker eavesdrops on wireless traffic
- Easy to do and the risk of detection is low
- Theoretically the distance from which an eavesdropper can eavesdrop traffic from an access point (AP) is ~200 feet
- Directional antennas can dramatically increase the effective range
Ex. 2 - Evil Twin Attack

- An attacker sets up an AP with the same SSID as a legitimate WLAN.
- If there is more than one AP with the same SSID, then the client will associate with the AP providing the strongest signal.
- Once the attacker has connected to the Evil Twin, the attacker can intercept traffic, replace data, harvest credentials, etc.
- It is possible to switch an 802.11 interface into infrastructure mode (ex: using “iwconfig” command in Linux).
Ex. 3 - Wired Equivalent Privacy (WEP) Cracking

- An attacker attempts to recover WEP encryption key
- WEP encrypts the payload of data frames using a pre-shared key (PSK)
  - PSK is never exposed on the network, and is shared in some out-of-band way between stations
  - RC4 (stream cipher) is the encryption algorithm
- Each station encrypts the payload w/ the PSK and a randomly selected initialization vector (IV), thus causing the encryption key to change for every frame
  - Encryption key (64 bits) = IV (24 bits) + PSK (40 bits)
- Stations supply the IV in plaintext
WEP Cracking (Continued)

- Each station adds a plaintext 24-bit IV to each frame
  - Given enough traffic, the randomized IV values are bound to repeat at some point
  - Because of the birthday paradox, it is likely that after only a few thousand packets, two will share the same IV

- Attackers can leverage “related-key attack” based on knowledge of some of the bits of the key: Similar to breaking Enigma in WW II

- Using published tools, attackers can force the generation of enough IVs to crack a WEP key in minutes
2. Attack Model
Classifications of Attack

- Active and passive attacks
- Inside and outside attacks
- Attacks according to the security mechanism that is targeted, e.g.,
  - attacks on encryption schemes
  - attacks on digital signatures
  - attacks on protocols
Passive Attacks

- Extraction of info. → eavesdropping
- Traffic analysis
Passive Attacks (Continued)

- **Malicious association**
  - In this situation, a wireless device is configured to appear to be a legitimate access point, enabling the operator to steal passwords from legitimate users and then penetrate a wired network through a legitimate wireless access point.

- **Identity theft (MAC spoofing)**
  - This occurs when an attacker is able to eavesdrop on network traffic and identify the MAC address of a computer with network privileges.
Active Attacks

- Masquerade/Impersonation attack
- Replay attack
- Modification of messages
Active Attacks (Continued)

- **Denial of service (DoS)**
  - This attack occurs when an attacker continually bombards a wireless access point or some other accessible wireless port with various protocol messages designed to consume system resources.
  - The wireless environment lends itself to this type of attack because it is so easy for the attacker to direct multiple wireless messages at the target.

- **Network injection**
  - This attack targets wireless access points that are exposed to nonfiltered network traffic, such as routing protocol messages or network management messages.

- **Man-in-the-middle attacks**
  - This attack involves persuading a user and an access point to believe that they are talking to each other when in fact the communication is going through an intermediate attacking device.
  - Wireless networks are particularly vulnerable to such attacks.
Inside & Outside Attacks

- Inside attack
  - Initiated by an entity inside the security perimeter ("insider").
  - Insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

- Outside attack
  - Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system ("outsider").
Attacks on Encryption Schemes

- Objective: Systematically recover plaintext from ciphertext or to deduce the decryption key

- Attack types
  - Ciphertext-only attack
  - Chosen-ciphertext attack
  - Adaptive chosen ciphertext attack
  - Known-plaintext attack
  - Chosen-plaintext attack
  - Adaptive chosen-plaintext attack
What is the birthday paradox?

- Birthday paradox states that in a group of 23 (or more) randomly chosen people, there is more than 50% probability that some pair of them will have the same birthday.

- How big does the group have to be in order for this probability to be greater than 99%?
3. Countermeasure

(a) Advanced Encryption Standard (AES)

Two requirements for secure use of symmetric encryption

- a strong encryption algorithm
  → assume encryption algorithm is known
- a secret key known only to sender / receiver
  → existence of a secure channel to distribute key
Ideal Block Cipher (n-bit General Substitution)

Encryption Table

<table>
<thead>
<tr>
<th>Plaintext</th>
<th>Ciphertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>1110</td>
</tr>
<tr>
<td>0001</td>
<td>0100</td>
</tr>
<tr>
<td>0010</td>
<td>1101</td>
</tr>
<tr>
<td>0011</td>
<td>0001</td>
</tr>
<tr>
<td>0100</td>
<td>0010</td>
</tr>
<tr>
<td>0101</td>
<td>1111</td>
</tr>
<tr>
<td>0110</td>
<td>1011</td>
</tr>
<tr>
<td>0111</td>
<td>1000</td>
</tr>
<tr>
<td>1000</td>
<td>0011</td>
</tr>
<tr>
<td>1001</td>
<td>1010</td>
</tr>
<tr>
<td>1010</td>
<td>0110</td>
</tr>
<tr>
<td>1011</td>
<td>1100</td>
</tr>
<tr>
<td>1100</td>
<td>0101</td>
</tr>
<tr>
<td>1101</td>
<td>1001</td>
</tr>
<tr>
<td>1110</td>
<td>0000</td>
</tr>
<tr>
<td>1111</td>
<td>0111</td>
</tr>
</tbody>
</table>

Decryption Table

<table>
<thead>
<tr>
<th>Ciphertext</th>
<th>Plaintext</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>1110</td>
</tr>
<tr>
<td>0001</td>
<td>0011</td>
</tr>
<tr>
<td>0010</td>
<td>0100</td>
</tr>
<tr>
<td>0011</td>
<td>1000</td>
</tr>
<tr>
<td>0100</td>
<td>0001</td>
</tr>
<tr>
<td>0101</td>
<td>1011</td>
</tr>
<tr>
<td>0110</td>
<td>1111</td>
</tr>
<tr>
<td>0111</td>
<td>1101</td>
</tr>
<tr>
<td>1000</td>
<td>0111</td>
</tr>
<tr>
<td>1001</td>
<td>1101</td>
</tr>
<tr>
<td>1010</td>
<td>1011</td>
</tr>
<tr>
<td>1011</td>
<td>0110</td>
</tr>
<tr>
<td>1100</td>
<td>1011</td>
</tr>
<tr>
<td>1101</td>
<td>0010</td>
</tr>
<tr>
<td>1110</td>
<td>0000</td>
</tr>
<tr>
<td>1111</td>
<td>0101</td>
</tr>
</tbody>
</table>
Shannon’s Substitution-Permutation Cipher

- Claude Shannon introduced idea of substitution-permutation (S-P) networks in 1949

- S-P nets are based on the two primitive cryptographic operations:
  - substitution (S-box)
  - permutation (P-box)

- Shannon suggested combining S & P elements to obtain confusion & diffusion
  - S-box provides confusion: Make the relationship between the statistics of the ciphertext and the value of the encryption key as complex as possible
  - P-box and round function provide diffusion: Make the statistical relationship between the plaintext and ciphertext as complex as possible (each plaintext digit affects the value of many ciphertext digits)
Introduction to AES

- On Oct. 2, 2000, National Institute of Standards and Technology (NIST) selected Rijndael as the Advanced Encryption Standard (AES)

Description
- Rijndael was designed by Joan Daemen and Vincent Rijmen
- Rijndael is a block cipher with a variable block size and variable key size
- Key size and the block size can be independently specified to 128, 192 or 256 bits
- Resistance against all known attacks
- Speed and code compactness on a wide range of platforms
- Design simplicity

<table>
<thead>
<tr>
<th>Key Size (words/bytes/bits)</th>
<th>4/16/128</th>
<th>6/24/192</th>
<th>8/32/256</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext Block Size</td>
<td>4/16/128</td>
<td>4/16/128</td>
<td>4/16/128</td>
</tr>
<tr>
<td>Number of Rounds</td>
<td>10</td>
<td>12</td>
<td>14</td>
</tr>
<tr>
<td>Round Key Size</td>
<td>4/16/128</td>
<td>4/16/128</td>
<td>4/16/128</td>
</tr>
<tr>
<td>Expanded Key Size</td>
<td>44/176</td>
<td>52/208</td>
<td>60/240</td>
</tr>
</tbody>
</table>
Structural Features of AES (Animation)

- Block size – 128 bit
  - Input (plaintext or ciphertext) is a single 128-bit block which is segmented into 16 bytes
  - The key is also segmented into 16 bytes

- AES is comprised of multiple number of iterations of a basic unit of transformation, called a “round”
  - Round(State, RoundKey)
    - State (16 bytes): A round-message matrix, treated as both input and output
      - A state is an array of four 4-byte columns
    - RoundKey (16 bytes): A round-key matrix, derived from the input key
Structural Features of AES (Animation)

- Input key is expanded into an array of 44 32-bit words, \( w[i] \). 4 distinct words (128 bits) serve as a round key.
- Each round (other than the final round) is composed of 4 different transformations (stages)

\[
\text{Round}(\text{State}, \text{RoundKey}) \{
\text{SubstituteBytes}(\text{State}); \\
\text{ShiftRows}(\text{State}); \\
\text{MixColumns}(\text{State}); \\
\text{AddRoundKey}(\text{State}, \text{RoundKey});
\}
\]

- Each stage is reversible
Overall Structure of AES

(a) Encryption

(b) Decryption
AES Implementation Aspects

- AES can be efficiently implemented on 8-bit CPU
  - Byte substitution works on bytes using a table of 256 entries
  - Shift rows is simple byte shift
  - Add round key works on byte XOR’s
  - Mix columns requires matrix multiply which works on byte values

- AES can be efficiently implemented on 32-bit CPU
  - Redefine steps to use 32-bit words
  - Can pre-compute 4 tables of 256-words
  - Each column in each round can be computed using 4 table lookups + 4 XORs
  - At a cost of 4Kb to store tables
3. Countermeasure

(b) IEEE 802.11i Standard
Securing Your Wireless Transmission

- Use encryption
- Use antivirus, antisyware software and a firewall
- Turn off identifier broadcasting
- Change the identifier on your router from the default
- Change your router’s pre-set password for administration
- Allow only specific computers to access your wireless network
Motivation for IEEE 802.11i Standard

- **Original 802.11 spec**
  - Wired Equivalent Privacy (WEP) algorithm
  - Contained major weaknesses: WEP Cracking

- **Wi-Fi Protected Access (WPA)**
  - Steps for dealing w/ weaknesses of WEP
  - Uses the Temporal Key Integrity Protocol (TKIP)

- **Robust Security Network (RSN)**
  - Final IEEE 802.11i standard
  - Certification under the WPA2 program

- **WPA2**
  - Currently considered secure (if implemented correctly)
  - Implements the mandatory elements of 802.11i
  - Uses **AES-CCMP** (Counter Mode - Cipher Block Chaining - Message Authentication Code - Protocol)
Cipher Block Chaining

(a) Encryption

(b) Decryption
802.11i RSN Services and Protocols
An 802.11 Packet Capture Displayed in Wireshark

WPA2 packet: Indicates that the packet uses AES-CCMP
802.11i Phases of Operation

- **STA**: Wireless station
- **AP**: Access point
- **AS**: Authentication server
- **End station**: Entity on a wired/wireless network

**Phase 1 - Discovery**

**Phase 2 - Authentication**

**Phase 3 - Key Management**

**Phase 4 - Protected Data Transfer**

**Phase 5 - Connection Termination**
802.11i Discovery and Authentication Phases

- **Discovery phase**
  - Network & security capability discovery
  - Open system authentication
  - Association

- **Authentication phase**
  - Connect to AS
  - EAP exchange
  - Delivery of the master session key (MSK) from AS to STA via AP
802.11i Key Management Phase

802.11i key hierarchy
802.11i Key Management Phase

Message 1 delivers a nonce to the STA so that it can generate the PTK.

Message 2 delivers another nonce to the AP so that it can also generate the PTK. It demonstrates to the AP that the STA is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.

Message 3 demonstrates to the STA that the authenticator is alive, ensures that the PTK is fresh (new) and that there is no man-in-the-middle.

Message 4 serves as an acknowledgement to Message 3. It serves no cryptographic function. This message also ensures the reliable start of the group key handshake.

AP’s 802.1X controlled port unblocked for unicast traffic.
802.11i Protected Data Transfer Phase

- Temporal Key Integrity Protocol (TKIP)
  - Software changes only to older WEP implementations
  - Adds 64-bit Michael message integrity code (MIC)
  - Use RC4

- AES Counter Cipher Mode-CBC MAC Protocol (CCMP)
  - Intended for newer 802.11 devices that have the required h/w
  - Uses the cipher block chaining message authentication code (CBC-MAC) for integrity
  - Uses the counter block cipher mode of operation
  - Same 128 bit AES key is used for both integrity & confidentiality
4. Security in Wireless Networks with Spectrum Sharing


Threats to Spectrum Sharing

- Threats to Spectrum Sharing (T)
  - Threats to Sensing-Driven Spectrum Sharing (TS)
    - PHY-Layer Threats (TS-1)
    - MAC-Layer Threats (TS-2)
    - Cross-Layer Threats (TS-3)
  - Threats by Rogue Transmitters (TR)
  - Threats to Database-Driven Spectrum Sharing (TD)
    - Database Inference Attacks (TD-1)
      - Threats to Privacy of Primary Users (TD-1-1)
      - Threats to Privacy of Secondary Users (TD-1-2)
    - Threats to Database Access Protocols (TD-2)
Spectrum Security and Enforcement

- **Ex-ante (preventive) approach**: mechanisms for avoiding threats.
  - Privacy preserving mechanisms
  - *Interference protection using exclusion/protection zones*
  - Tamper-resistant radios
  - Hardware-based compliance modules

- **Ex-post (punitive) approach**: remedial mechanisms after an attack has occurred
  - Infrastructure for enforcement networks
  - Authentication scheme for identifying rogue transmitters
  - Localization of non-compliant transmitters
  - Adjudication procedures for non-compliant transmitters
    - Revocation of spectrum access rights
    - Economic penalties
4. Security in Wireless Networks with Spectrum Sharing

(a) Ex-Ante Approach – Interference Protection
Interference Protection: Exclusion Zones

- Protection/Exclusion zones (EZs) is the primary ex-ante enforcement scheme employed by the FCC and the NTIA to protect PUs.

- Existing definitions of EZs are overly conservative & rigid. Studies show that approximately 60% of the US population is covered by the EZs of ship-borne radar systems.

- Existing definition uses a fixed geographic contour around a PU that considers the union of worst-case interference scenarios.

- Cannot adapt to changing conditions (e.g., PU protection requirements, SU network conditions, spectrum availability, etc.)

- More flexible and dynamic definitions of EZs are needed
Interference Protection: Illustration

- The outer circle represents the current EZ (based on NTIA calculations)
- This covers three big cities and defeats the purpose of spectrum sharing
- If the EZ could be reduced to the inner circle, the remaining area (green annulus) would serve approx. 10 M population.
4. Security in Wireless Networks with Spectrum Sharing

(b) Ex-Post Approach – Blind Transmitter Authentication
Blind Transmitter Authentication (BTA)

- Characteristics
  - Enables a receiver to "blindly" authenticate at PHY-layer
    - The receiver may not be the intended receiver
    - Little or no knowledge of the transmission parameters
  - Incurs minimal overhead
    - Data-rate
    - Power
  - Robust under harsh channel conditions
    - Low signal-to-interference-plus-noise ratio
    - Fading
  - Ensures security against an adversary
Frequency offset Embedding for Authenticating Transmitters (FEAT)

- Generate the message signal as samples of the OFDM signal
- Generate the authentication signal in bits
- Embed the authentication signal in the form of embedded frequency offset (EFO) represented by $f_a$ in each frame of the message signal
  ![Diagram](https://via.placeholder.com/150)
  
  Allowed offset up to 25 ppm, i.e. 60 kHz for 2.4 GHz, due to inaccurate oscillators

  **No effect** on the decoding procedure of the message signal

  Intended receiver
  - Estimate EFO using preamble symbols, and the pilot samples
  - Utilize the estimated EFO to estimate authentication bits
Blind Estimation of Authentication Signal

- **Signal Detection and Sampling**
  - Center frequency and sampling frequency is assumed to be known

- **Symbol Synchronization**
  - Estimation of FFT size, cyclic prefix size, and sample offset
  - Utilizes the correlation induced due to cyclic prefix

- **Frame Synchronization**
  - Estimate number of symbols in a frame, and the symbol offset
  - Utilize the correlation induced due to the preamble symbols

- **Frame Frequency Estimation**
  - Estimate EFO and the authentication signal in each frame
  - Utilizes the correlation induced due to CP
Simulation Results

- $f_a$: Embedded frequency offset
- $N_f$: FFT size
- $N_c$: Cyclic prefix size
- $N_s$: Number of OFDM symbols in a frame
- $M$: Number of levels of frequency offset

Error performance of authentication signal with $N_f = 64$, $N_c = 16$, $N_s = 50$
Experimental Validation

- Universal Software Radio Peripheral (USRP) radios
- National Instruments' LabVIEW utilized as the system-design platform to configure the USRPs

LabVIEW VI illustrating the implementation of FEAT
5. Summary
Take Away

- Awareness about the security of your wireless network
- Security threats in wireless networks
- Security traits present in existing wireless networks
  - Advanced Encryption Standard (AES)
  - IEEE 802.11i Standard
- Security issues in wireless networks with spectrum sharing