Advanced Topics in Security

Claude Castelluccia – INRIA – 2010
Claude.castelluccia@inria.fr
(most slides borrowed from Srdjan Čapkun- ETHZ)
Course Outline (lectures)

1. Introduction to Wireless Network Security (06/01)
   - basics stuff

2. Security of WiFi networks (13/01)
   - 802.11 architecture and protocols
   - (un)authorized access: MAC filtering, WEP, WPA, 802.1X, 802.11i

3. WEP Cracking LAB (20/01)

4. Ubiquitous Security (27/01)
   - Secure RFID systems
     - security issues: privacy, forgery, sabotage
     - RFID security protocols
     - Secure Wireless Sensor Network

5. Network Privacy (10/02)
   - privacy definition
   - anonymisation techniques
   - TOR...
Class Organisation

- From 13:45 to 15:30: lecture (or LAB)
- From 15:45 to 17:45: paper presentation
Grading (for this part of the class!)

- Paper mini-review: 50%
  Paper presentation: 50%

- There is no mid-term or final exam.
Grading (for this part of the class!)

- Paper mini-review: 50%
  Paper presentation: 50%

- There is no mid-term or final exam.
Grading (for this part of the class!)

- You need to write a mini-review/summary (~4 pages) of it. This mini-review/summary can include:
  - Problem domain: background, motivation, why this problem is important/novel/interesting
  - Summary of the paper:
    - assumption, main techniques, results
    - Possible future work/direction
    - Pros, cons of the paper (your conclusion)
- The mini-review has to be sent to me 2 days prior to the corresponding lecture (or before the last class i.e. 10/02).
- You then need to present the mini-review during the class (~20-25 min).
- This is an individual work. **Plagiarism will result in a mark of zero for the assignment.**
- Don’t ask me to postpone your presentation!!!!
A note on Plagiarism

• Plagiarism (from wikipedia)
  – submitting a copied article as his or her own work
  – In the academic world, plagiarism by students is a very serious offense that can result in punishments such as a failing grade on the particular assignment

• Mini-project Plagiarism
  – Failing grade for the class
  – Very easy to detect
  – Mini-project must be your own work!
  – We are very strict about it...
Wireless Networks
An age of wireless communication ...
Ad Hoc(mesh) networks

mesh networks

from I.F. Akyildiz et al. / Computer Networks 47 (2005)
Wireless, mobile robots

Amigobots
Vehicular Networks
Sensor/Actuator networks

From monitoring avalanches ...

... to monitoring the structural integrity of buildings

building automation (WSN)
Numerous Applications

- Environmental Monitoring
- Interactive VR Game
- Wearable Computing
- Disaster Recovery
- Earth Science & Exploration
- Immerse Environments
- Context-Aware Computing
- Biological Monitoring
- Smart Environment
- Linear Structure Protection
- Military Surveillance
- Road Safety
- Hazard Detection
- Wireless Sensor Networks
- Interactive VR Game
- Wearable Computing
- Disaster Recovery
- Earth Science & Exploration
- Immerse Environments
- Context-Aware Computing
- Biological Monitoring
- Smart Environment
- Linear Structure Protection
- Military Surveillance
- Road Safety
- Hazard Detection

Wireless Sensor Networks
Technologies enabling wireless networks

- **GSM/UMTS** (800, 1900MHz, ...)
- **802.11** (WiFi) (LAN) Wireless Fidelity
  - 2.4 GHz, 54Mbps, 100mW-1W, 30m range
- **802.16** (WiMAX)
  - 10-66 GHz, < 10km coverage
  - 2-11GHz, < 20km coverage
  - 75Mbps (theoretical), 20km, 5Mbps (typically, 5km)
- **UWB**
  - 3.1 - 10.6 GHz, short-range Gbps communication
  - lower speed, longer range, localization (<2km outdoor)
- **802.15.4** (Zigbee) (WPAN) (Sensor networks)
  - 868 MHz in Europe, 915 MHz in the USA and 2.4 GHz
  - 250kbps, 1mW, ~100m range
  - 4 MHz 8-bit processors
- **RFIDs**
  - short range identification tags (UHF 868-956 MHz)
Applications of Wireless Networks

- **Infrastructure-based**
  - Cellular - ANY DATA
  - WiFi access – ANY DATA
  - GPS – LOCATION, TIME
  - Local Area (Indoor) Navigation – LOCATION, TIME

- **Infrastructure-less** (multi-hop)
  - Sensor networks – ENVIRONMENTAL (SENSED) VALUES
  - Ad hoc (e.g. vehicular network) – ANY DATA
  - Mesh networks (e.g., home networks) – ANY DATA

- RFID tags – IDENTITY
Application-specific constraints and security goals

Cellular networks
- infrastructure based
- single-hop (to the BS)

Informally: to communicate privately!!!
confidentiality is the prime security goal

Sensor Networks
- infrastructureless
- multihop
- node compromise
- node sabotage
- displacement
- ...

Informally: to accurately measure and deliver sensed data
confidentiality not an issue – data authentication is important
Wireless Communication Channel
Wireless channel

To calculate the received signal level (in dBm), add the transmitting antenna gain (in dB), subtract the link losses (in dB), and add the receiving antenna gain (in dB) to the transmitter power (in dBm).
Why security is more of a concern in wireless?

- no inherent physical protection
  - physical connections between devices are replaced by logical associations
  - sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
  - Attacker can be far away from network!

- broadcast communications
  - wireless usually means radio, which (generally) has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)
Different Types of Attacks

• Passive attacks
  – The attacker is just listening and is not actively taking part of the communication
    • E.g. eavesdropping or snooping...

  *Hard to detect in wireless com.....*

• Active attacks
  – The attacker is able to alter the channel and/or modify/inject messages to reach its goal
    • Message Forgery (send bogus data)
    • Message modification/Man in the Middle
    • Denial of Service (flooding, jamming)

  *Easier to perform in wireless com. (since no physical access control)....*
Different Types of Attacks

Most existing attacks combine passive and active technique....

- Let’s consider each of these attacks and identify the protection solution...

1. Snooping/eavesdropping attacks:
   - the attacker is listening to the communication in order to access private information (emails, secrets,...)
Eavesdropping/snooping Attack

- Straightforward
- Precondition:
  - The attacker knows the frequency/modulation/coding on/by which the communicating parties exchange their information.
Snooping attack (passive attack)

- The proposed solution is encryption *(WEP, 802.11i)*!
- But is encryption enough?
  - No, an attacker can still perform *traffic analysis* on encrypted data!
  - It can, for exemple, identify the number of access point and wireless devices ...and eventually the network topology!
  - It can identify the traffic type (email, web browsing, VoIP,...) by looking at packet size and time information...
    - Even the VoIP language can be identified!
  - It can identify if someone is currently using the network (useful for robbery!)...this creates some privacy issue!

- Snooping is a major problem in wireless networks
  - An attacker can eavesdrop from very far with a directional antenna
Directionality vs Gain (snooping attack)

- Omnidirectional antennas
  - Gain: 2dB

- Directional antennas
  - Gain: 10-55dB
Implications of antenna directionality on security

- Attackers can eavesdrop communication from much longer distances than anticipated
  - Attacks on Bluetooth (designed for 10m range)
    Reported eavesdropping from 3 km (LOS) !!!
Modification Attacks (active attacks)

2. Modification attacks:
   - The attacker modifies:
     • The information contents (email, web, ...)
     • The IP destination address to *redirect* traffic somewhere....
     • The IP source address to *masquerade/impersonate* another host/user!!
   - There are at least 2 ways to modify a message:
     • The message is modified on the fly...
       - Difficult...
     • The message is intercepted, modified and then replayed: Man in the Middle (MiTM) attack!
Modification Attacks (active attacks)

- MiTM attacks is simple enough in wired networks
  - An attacker cuts the wire, receives all the data, modifies them and re-injects them
  - An attacker can corrupt a router...
- MiTM is more difficult in wireless networks! Why?
  - No wire to cut! The attacker must stop the receiver from getting the message on the initial transmission...
  - Difficult but not impossible!
Modification Attacks (active attacks)

- ATTACK1 (MiTM between *Mob* and *AP*):
  - Listen for a message from Mob to AP
  - Transmit a sudden burst of noise to corrupt the message (or Checkwork-CRC)- this causes AP to drop the message as invalid
  - Forge an ACK message with AP’s address and send it to Mob; now Mob thinks the message has been received by AP!
  - Modify message and send it to AP- AP thinks it came from Mob!
  - Wait for an ACK from AP and send a burst of noise so Mob ignores it and does not see 2 ACKs for the same packet!
  - Not easy...but possible!
Modification Attacks (active attacks)

- Another, more practical, technique exists...
- ATTACK2 (MiTM between Mob and AP):
  - Set-up a bogus AP, bAP
  - Mob associates to bAP (and eventually establish a key)
  - bAP gets messages, decrypts them, modifies them and sends them to the real AP!!

- So how to protect against Modification attacks??
- Mutual authentication!
  - Mob authenticates the AP’s messages
  - AP authenticicates Mob’s messages
Modification Attacks (active attacks)

- For example:
  - AP gets and verifies certificates/credentials from Mob
  - Mob gets and verifies certificates/credentials from AP
  - AP and Mob establish a secret key using Diffie-Hellman key exchange protocol
  - Messages are authenticated using a MAC (message authentication code)
    Or
  - Messages are signed....
Modification Attacks (active attacks)

- ATTACK1 is prevented
  - Attacker does not have the key so the modified message will be rejected by AP...since MAC will be incorrect!

- ATTACK2 is prevented
  - Mob will be able to detect the bogus AP (since its certificate/credential will be invalid)!!

  - Mutual authentication is efficient in most of the cases ...but not always 😞
Message replay

- Door access control - Does authentication help?

Who are you?

Hi, I am C.Castelluccia

prove it, $N_B$

sign$_A$\{N$_B$, B\}

verifies A’s signature using A’s public_key and open the door!

Who are you?

I am C. Castelluccia

prove it, C, N$_C$

sign$_A$\{N$_C$, C\}

verifies A’s signature using A’s public_key and open the door!

Authentication does not help!
3. Denial of Service Attacks.
   - The goal of the attacker is to cause damage by preventing operation of the networks
   - DDoS: flooding a host with a huge number of packets...
   - In wireless networks, the most important DoS attack is jamming...
     • Add physical noise on the channel to corrupt messages...
   - These attacks are simple and very difficult (if not impossible) to prevent...
Adversarial interference: jamming

- Transmitting a signal on the same frequency on which the honest parties communicate
- Blocks the reception of the message at the receiver B

Simple amplitude modulation example
Jamming Chirp Signals

- Narrow-band is not good
- Partial jamming can be used ...
- Spread Spectrum techniques help a bit...
Direct Sequence Spread Spectrum

message
spreading code
spread message

used in 802.11, GPS ...
There are two basic spread spectrum techniques:
• Direct Sequence Spread Spectrum (DSSS):
  - the signal is multiplied by a spreading code in the time domain
  - the spreading code is a pseudo random sequence that looks like noise
• Frequency Hopping Spread Spectrum (FHSS)
  - the signal changes of carrier frequency
  - sequence of frequency changes is determined via a pseudo random sequence
DSSS Technology

• The initial application of spread-spectrum (SS) techniques was for military applications
• SS investigation was motivated primarily by the desire to achieve highly jam-resistant communication systems
• It is now used in civil applications
  - Multiple Access (ex: CDMA) / Modulation
  - coordinated systems coexistence (ex: SS UMTS)
  - uncoordinated systems coexistence (ISM bands)

• A system is defined to be a SS system if the signal occupies a bandwidth much in excess of the minimum bandwidth necessary to send the information
DSSS Technology (2)

- The consequences of pulse duration reduction...

- by reducing the pulse duration $T$, the frequency is spread.

\[ T \cdot \text{Sinc}(f,T) = \frac{T \cdot \sin(\pi f T)}{\pi f T} \]
DSSS Technology (3)

- The spreading signal is controlled by a pseudo-random sequence (called PN) or pseudo-random code
- A PN sequence is a random binary sequence:
  - nearly equal number of 0s or 1s
  - very low correlation with shifted versions of the sequence

- Principle:
  - multiplication by the PN code once spreads the signal bandwidth
  - multiplication by the PN code twice, recovers the original signal
  - at a receiver, the desired signal gets multiplied twice, but the interference signal (if any) gets multiplied only once...

- Once spread, a signal looks like noise
Spread spectrum Benefits (1)

interference suppression

- Spreading by the source
- Added interference during transmission
- Despreading by the receiver
- Spread signal
- Spread interference
Spread spectrum Benefits (2)

**multi access capability**

Signal *Despreading at the receiver*

- with code1

- with code2
Spread spectrum Benefits (3)

Other benefits

• improved confidentiality
  - a receiver that doesn’t know the code only sees white noise

• anti-jamming capability
  - jamming deliberately injected in the system is filtered just like interferences are
  - especially true with narrow-band jamming

• low probability of interception
  - because of its low power density the signal is difficult to detect and intercept by a hostile listener
DSSS – (more) difficult to DETECT, MODIFY and JAMM

- Secret spreading code – DSSS **HIDES** THE SIGNAL
- Signal detection is now more difficult
  - signal “hidden” in the noise
- Signal interception/modification difficult (off-line processing!) - LPI
- Jamming
  - narrowband jamming now requires much higher power
  - broadband jamming still effective
802.11 physical layer security issues

- 802.11 PHY cannot cope with active jamming
  - it was not designed to be resistant to jamming
  - easy intercept
  - easy DoS attacks
  - the attacker still needs a high-power transmitter to cover a large area
  - an attacker with an directional antenna can ‘aim’ at the victim AP and disable it (line of sight (LoS))
GPS jamming/spoofing

- Received GPS radio signal has a strength is about $1 \times 10^{-16}$ W at the Earth’s surface.

- A stronger signal can *cover* GPS satellite signal and cause the device to register a position different from its true position.

Think GPS Cargo Tracking = High Security? Think Again,
Roger G. Johnston, Jon S. Warner, Los Alamos National Laboratory, 2004
Conclusion on Attacks

• Snooping attacks can be prevented with Encryption

• Modification attacks can be prevented with Authentication

• Denial of Service attacks is still an open problem
  – Gains achieved using spread spectrum techniques ...
  – Full protection is not really feasible (shared medium)

• Current wireless networks (802.11, GSM/UMTS,...) use encryption and authentication...
  – Therefore the previous attacks are difficult
  – The attacks will then try to recover the keys or by-pass the cryptographic functions (encryption-authentication).
Attacks on the Keys

- One goal of the attacker is to retrieve the key(s).
- Some terminology:
  - **Plaintext**: the data before encryption - what we want to protect from eavesdroppers!
  - **Ciphertext**: the encrypted version of the plaintext - this is what the attacker sees!
  - **Keys**: The secret value that is used to encrypt/decrypt the message.
  - **Cipher**: The algorithm and rules used to perform the encryption and decryption.
- Assumption about the attacker:
  - She knows the ciphertext (she is listening...)
  - She does not know the key ...this is what she is looking for!
  - What about the cipher and plaintext?
Attacks on keys (2)

- Modern cryptography assumes that the cipher is public
  - Security by obscurity is known to be a bad idea...why?
  - It is impossible to keep a secret forever...soon or later the algorithm will be revealed by a designer or by reverse-engineering.
  - Since the algorithm is secret, it is not fully analysed by security expert and might contains design flaws
    - This is what happened with 802.11 and WEP!
    - Btw, the encryption algorithm used is most European cellular was secret (A5/A8)...it was disclosed and broken!

- All the security relies on the key which must be secret
  - At least in theory
  - In practice, implementation bugs are often used!...
Attacks on keys (3)

- Does she know the plaintext?
  - Of course not...but she can guess some of them
    - TCP/IP header
    - If a person is accessing a Web site and the attacker can guess the website site...she can go to the same site and get the plaintext..
    - The attacker might be able (in some cases) to send messages to the mobile devices via the AP...for example, VoIP (Skype) invitation messages...
      - It is fair to assume that the attacker knows some (plaintext, ciphertext) pairs...

- How can the attacker recover the key?
Attacks on keys (4)

- Attacking the Keys Through Brute Force
  - Try all possible keys...
  - A WEP key was 40 bit long i.e. there are $2^{40}$ possible keys
  - i.e. an attacker has to test $2^{39}$ keys on average...
    - With a supercomputer, this is possible in less than one week!!
  - The key must be larger...i.e. $\sim > 90$ bits

- Attacking the keys through Dictionary Attacks
  - Keys are often define by a human...and a human is a bad random number generator ;-) 
  - He tends to use existing name as key (i.e. grenoble38)....
  - So instead of trying all the keys, the attacker only have to try keys that he thinks the user is likely to use (i.e. words from a dictionary)!
Attacks on keys (4)

- For example, the attacker can assume that the key is made up entirely of letters and numbers...
  - A 104 bit key is then only as effective as a 78-bit key since only 6 bits of every byte are used!!
- Be careful when generating a secret...

- **Attacking the key with Algorithm Attacks**
  - The attacker try to find a flaw in the algorithm
    - As with WEP!
  - The algorithm must be public and analysed by expert!
  - It is so easy to get it wrong!

- **Attacking the key from an implementation bug.**
  - The attacker makes used of a bug (e.g. buffer overflow) to perform an exploit and recover the key...
  - Hard to avoid....
Conclusions: Wireless communication security requirements

- confidentiality
  - messages sent over wireless links must be encrypted
- authenticity
  - origin of messages received over wireless links must be verified
- replay detection
  - freshness of messages received over wireless links must be checked
- integrity
  - modifying messages on-the-fly (during radio transmission) is not so easy, but possible ...
  - integrity of messages received over wireless links must be verified
Conclusions: Wireless communication security requirements (2)

- access control
  - access to the network services should be provided only to legitimate entities
  - access control should be permanent
- it is not enough to check the legitimacy of an entity only when it joins the network and its logical associations are established, because logical associations can be hijacked
- protection against jamming
Wireless Security is hard because the attackers do not have to physically compromise the network!

It is even harder for small wireless devices, such as RFID or sensor, that can’t perform expensive crypto. Operations and can be physically compromised!

Getting it right require a lot of work!
  - Never design your own algorithm... use an existing (secure) one instead...

In the following class, we give 2 examples:
  - What not to do! The WEP example!
  - How to do it...: 802.11i!