Security Protocols for Wireless Communication

Susanne Wetzel
Stevens Institute of Technology
Department of Computer Science
Holoken, NJ, USA

(Joint work with Burt Kaliski, Jan-Ove Larsson und Markus Jakobsson)

Scenario and Motivation

Bluetooth Attacks

Countermeasures

Current/Future Work

Security Protocols for Wireless Communication 2

Scenario

Setting

Wireless Network

Ordinary network

Gateway

Bluetooth, 802.11

Gateway

WAP

WAP Internet

Internet

Security Protocols for Wireless Communication 3

Security Protocols for Wireless Communication 4

Motivation

Introduction (1)

• Bluetooth is a recently proposed standard for local wireless communication
• Bluetooth SIG was formed in 1998
• Promoter Group (Ericsson, IBM, Intel, Nokia, Toshiba, 3Com, Lucent, Microsoft, Motorola)
• More than 1,800 adopters
• Specification 1.0 B was released in December 1999

Security Protocols for Wireless Communication 5

Security Protocols for Wireless Communication 6
Introduction (2)

Bluetooth wireless technology:
- low power
- low cost
- short range
- allows for rapid ad hoc/automatic connections

double-edged sword: provides user with increased possibilities and criminals with powerful weapons

State-of-the-Art

The secret key is K!

Ahat Uwe Schult just passed by!

Operation of Bluetooth Devices

Ideal:
- Unique identifying information is used
- Encryption of information is supported (complying with local jurisdiction)
- User privacy is guaranteed

State-of-the-Art:
- Addressing by means of the unique Bluetooth device address, device access code (DAC), channel access code (CAC)
- Various device modes
- Various keys (unit key, link key, encryption key)

Details of Specification (1)

- Channel Access Code (CAC):
  - deterministically derived from the unique Bluetooth device address
  - used for point-to-(multi)point communication
- Keys:
  - Unit Key:
    - unique symmetric long-term private key of a device
  - Link Key:
    - temporary symmetric key, unique for a pair of devices
    - is either the unit key of one of the devices or a derived key
  - Encryption Key

Details of Specification (2)

Establishment of Initialization Key

Device A

Device B

Generate initialization key

Generate link key

Generate encryption key
Verification of Initialization Key

Device A

BD_ADDR_B Kinit RND

SRES

Verifer

Device B

BD_ADDR_B Kinit RND

RND

SRES

Claimant

Establishment of Link Key (1)

• Link key of devices A and B = unit key $K_A$ of device A

Device A

Device B

Establishment of Link Key (2)

• Link key of devices A and B = combination key $K_{AB}$

Device A

Device B

Eavesdropping and Impersonation

• Unit key $K_A = link key of devices A and B$

  $\Rightarrow$ allows device B to impersonate device A and eavesdrop on all of A's communication

• Combination key

  $\Rightarrow$ knowledge of initialization key allows attacker to determine link as well as encryption keys thus allowing eavesdropping and middle-person attack

  $\Rightarrow$ Secrecy of the initialization key depends on the PIN:
  - between 8 and 128 bits
  - fixed or arbitrarily selected
  - default value: zero

Offline PIN Crunching

• Eavesdropping on key establishment process:
  - attacker guesses a PIN
  - correctness is checked by performing the verification step

• Stealing participation:
  - attacker guesses a PIN
  - initiates the verification
  - obtained challenge-response transcript used to check the guesses

  attacker benefits from back-off method

Location Attack

• Devices in discoverable mode:

  - response to inquiries reveals device identity

    attacker can determine location and movements of victim devices

• In general:

  - CAC is a deterministic function of the device identity

    CAC's associated with each message allow indexing of victim devices
Further Attacks

- **“Hopping Along”**
  - Listening to all bands in parallel
  - Listening to a particular communication by synchronizing to the hopping sequence of the piconet

- **Combined Attack**
  - Obtain unit/link keys
  - Eavesdrop on the communication by hopping along

Counter-Measures

- Pseudonyms against CAC location attacks
- Protecting unit keys
- Physical protection
- Policies protecting against middle-person attack
- Application layer security
- PIN length
- Bitwise verification
- Pairing based on Diffie-Hellman key exchange

Security in 802.11

- Relies on a secret key that is shared between a mobile station and an access point
- Key is used both for encryption and authentication
- Integrity checks of packets with CRCs
- Weaknesses:
  - Standard does not discuss key establishment
  - Most implementations use one single key for all stations and access points
  - No mutual authentication of stations and access points
  - Short keys
  - Use of the stream cipher RC4

- 802.1X: Port based network access control:
  - Man-in-the-middle attack
  - Session hijacking

The Problem of Pairing

- $K_A = K_B$?
- man-in-the-middle?

Bitwise Verification (simplified)

Method based on Diffie-Hellman Key Exchange (simplified)
Current/Future Work

- Efficiency
- Secure roaming
- Misuse of desired application functionality
- Viruses etc.

Privacy: A Good Starting Point