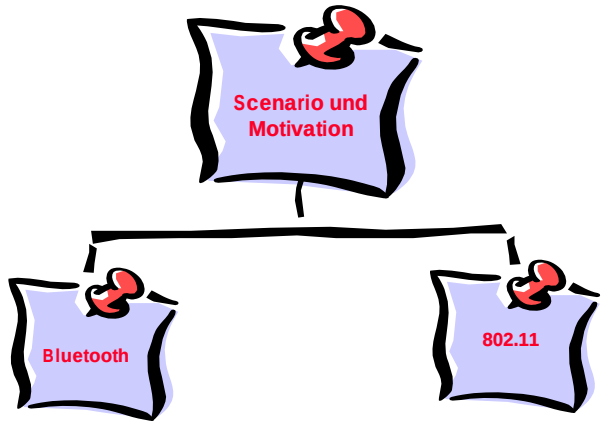
Wireless LANs and Domotics
- Security -

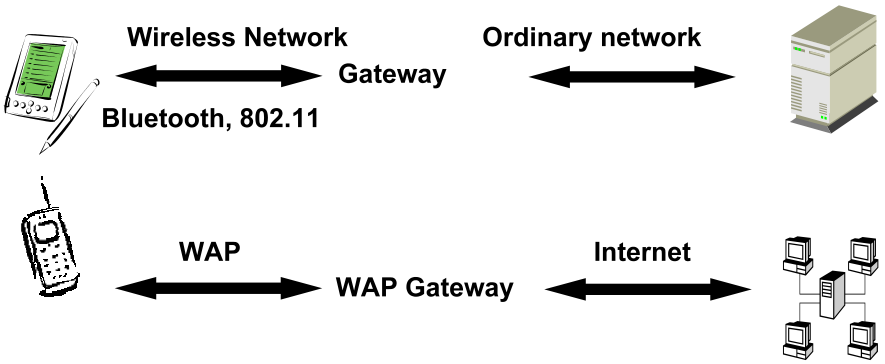
Susanne Wetzel

Stevens Institute of Technology
Department of Computer Science
Castle Point on Hudson
Hoboken, NJ, USA



Scenario

Setting



Security Objectives

- Privacy or confidentiality:

  Assurance to keep information from all but those authorized to have it
- Authentication

  Assurance of the identity
- Integrity

  Assurance to prevent unauthorized alterations of data
- Non-repudiation

  Assurance to prevent the denial of previous commitments of actions

Motivation

CommWeb

Where Telecom, Datacom and The Internet Converge

Buyer's Guide | Lab Tests | Case Studies | Events | Product Reviews | Tutorials | Chats/Forums | Subscriptions

Researchers Find Hole In 802.11 Security

Is your wireless LAN secure? Probably not, if you trust the wireless networking protocol.

First Wireless Virus Found

Sept. 25, 2000

The world's first wireless virus has been discovered in the Palm operating system, according to a report from McAfee

Networking

Wireless security flaws exposed

By Rupert Goodwins
ZDNet (UK)
February 19, 2002, 5:10 AM PT

A new set of security measures aimed at making 802.11-type wireless LAN hackers is fundamentally flawed, according to researchers from the ... Maryland.

Professor William Arbaugh and Arunesh Mishra say ... new 802.1X security system has two basic ... existing connection, and another where ... and steal access information ...

The New York Times ON THE WEB

Date: September 2, 2000, Saturday

Flaws in Digital Wireless Technology Said to Allow Eavesdropping

By JOHN MARKOFF

Two researchers have found flaws in a widely heralded new wireless technology that could permit an eavesdropper to listen in ...

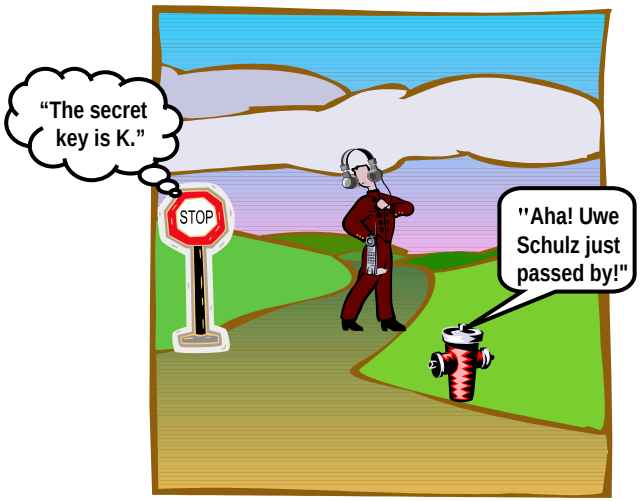
Bluetooth (1)

- General:
  - Recently proposed standard which operates in 2.4 GHz band
  - Low power and cost
  - Short range
  - Rapid ad-hoc conncections
- Applications:
  - Office/home environment, i.e., connecting printers, computers, fax machines, telephones
  - On the road, i.e., connecting cell phones to communication unit in the car, connecting PDA to devices in street signs or shops
  - ...

Bluetooth (2)

- Security:
  - Different modes: Clear mode to enforced security (”authentication” and encryption) on Bluetooth level
  - No data or entity integrity
  - Weaknesses:
    - Eavesdropping
    - Impersonation
    - Traffic analysis (geographic location)
    - Weakness in cipher

Security in Bluetooth: State-of-the-Art



Wireless LAN (1)

- General:
  - IEEE 802.11 standard
  - Provides flexibility and responsiveness to networking requirements and different applications
  - Operates in 2.4 GHz band
  - Range of up to a several hundred feet
- Applications:
  - Office/university environment
  - Hotels and other businesses
  - ...

Wireless LAN (2)

- Security:
  - 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

Privacy: A Good Starting Point