Wireless Communications Security

Prepared for Multi-Sector Crisis Management Consortium Workshop

L. Owens
January 14, 2002
“Those who cannot remember their past are condemned to repeat it.”

George Santayana
19th Century Philosopher
Outline

• Background on Security Attacks and Threats
• Case Studies of Wireless Security Problems
  ▪ First Generation Cellular Communications
  ▪ 802.11b Wireless LAN
• Wireless Security Problem Definition
• What is required?
• Wireless Technologies
• Wireless Security Approaches
• Open Discussion (Q&A)
Background on Attacks and Threats
Attack Taxonomy

Attacks

Passive Attacks

Eavesdropping

Traffic Analysis

Active Attacks

Masquerade

Replay

Message Modification

Denial-of-Service
Passive Attacks

- Basically eavesdropping (“snooping” or “sniffing”) on transmissions
- Traffic analysis
  - By monitoring frequency and length of messages, even encrypted, nature of communication may be guessed
- These attacks are difficult to detect
- These attacks can be prevented
Active Attacks

- Masquerade
  - Pretending to be a different entity
- Replay
  - Sending messages from a previous time from a legitimate sender
- Modification of messages
- Denial of service
  - These attacks are easy to detect
  - Detection may lead to deterrent
  - These attacks are hard to prevent
Typical Adversaries (threats)

- Insiders
  - Malicious employees
  - Disgruntled employees
- Hackers
- Crackers
- Professional Thieves
- Competitors
- Foreign Governments
- Terrorists
What drives the adversaries?

- For financial gain
- For revenge
- For giggles and grins
- For anonymity
- For military purposes
- For a challenge
- To impress
- To be destructive
Case Studies
1G Cellular Authentication

Wireless Interface (Radio Path)

ESN: 82345AC5
MIN: 508-351-9702

Subscriber

(212)-273-2345
Distinguishing the legitimate subscriber
Typical Class C Counterfeiting

- IBM-Compatible PC
- Telephone with Vulnerable Operating Software
- Hardware/Software and Instruction Manuals
- Disassembly and EPROM Programming Software
- EPROM Programmer and Chips

Adversaries are sophisticated and share information
**Simplified 802.11b Wireless LAN (WLAN) Architecture**

- Adds mobility to an enterprise
- Very inexpensive to deploy
- May be deployed very quickly
- May get very good performance – same as wired LAN
- Avoids wiring hassles in older buildings
- Facilitates changing organizations
- Excellent for transient groups

802.11b is experiencing explosive growth
WLAN War-driving

FalseSenseofSecurity Corp Security Director

Internet

LAN

FSOS Corp. Enterprise LAN

802.11 Access Point

Laptop w/ 802.11 NIC

802.11 Sniffer and collection system

6/26/2002

Copyright 2002 Vectara Innovations, LLC
Security of 802.11b is example of bad cryptography
Wireless Security
Problem Definition
Wireless means radio → radio is insecure
Problem Definition

“...Wireless brings increased productivity gains for the mobile workers and the enterprise” – IDC 2000

Wireless is valuable for a number of reasons

- **Wireless must be secured** – it is inherently insecure
  - Confidentiality (privacy) of communications
  - Message integrity
  - User and message authentication
  - Protection against loss of availability

- **Devices are constrained**
  - Limited code and memory space
  - Limited bandwidth
  - Limited processing power
  - Limited power
Fundamental Security Requirements

- Confidentiality – data only accessible for reading by authorized parties (privacy)
- Integrity – data can be modified by authorized parties only
- Authentication – must be able to verify user identity to prevent unauthorized use
- Availability – data available to authorized parties
Additional Wireless Requirements

- Interoperable – wireless may need to be interoperable with other systems

- Seamless – connectivity may need to occur transparently to user

- Efficient – bottleneck cannot be created or long delays experienced; plus security technology must fit packaging and not drain power
What is required?
Tools in the security toolbox

- Computer Security Toolbox
  - Security Training
  - Firewalls
  - Passwords
  - Audit
  - IDS

Copyright 2002 Vectara Innovations, LLC
Cryptography is a critical tool

Encryption / Decryption Key

Plain Text

Easy to read information

Cipher Text

Xcdfrt458&lk$lkdd^tg
Classical Cryptosystem (Symmetric)

- Security is based on the secret key, not on the encryption algorithm
- Involves the sharing of secret keys
- Strengths: Fast, good for encrypting large amounts of data
- Weaknesses: Key delivery
- Example algorithms: DES, 3DES, RC4, CAST, IDEA.

Copyright 2002 Vectara Innovations, LLC
Asymmetric Crypto System (Public Key Algorithm)

- Public key encryption involves two mathematically related keys.
- Any of the keys can be used to encipher.
- One of the keys can be made public and the other one private.
- Strengths: Less key delivery issues; can be used for non-repudiation
- Weaknesses: Slow, inefficient for large amounts of data
- Example algorithms: RSA (Rivest Shamir Adleman), Diffie-Hellman

Copyright 2002 Vectara Innovations, LLC
Hash Functions

- Also called *message digest*
- Hash functions take information of arbitrary size and produce a fixed sized output (\(\geq 128\) bits)
- Hashes compute ‘fast’
- Hashes have two key security properties:
  - Cannot randomly choose input to obtain same hash
  - Cannot reveal input (1-way)
- MD-5 and SHA-1 are two hash functions
Some order to Cryptography

Encryption

Symmetric Key
- DES
- RC4
- IDEA
- CAST
- 3 DES
- BLOWFISH
- TWO FISH

Digital Signatures

Public Key
- RSA
- EL GAMAL
- ECC

Hash
- MD5
- SHA - 1

Key Management
- IKE
- DIFFIE - HELLMAN
- SKIP

Key management is critical: scalable and secure
Overview of Wireless Technologies
Three Layers of Wireless Technology

Wireless Personal Area Network (WPAN)
- Personal or Location specific
- Proximity based services / info sync / queue elimination / voice & data inter-working

Wireless Local Area Network (WLAN)
- Building or Campus
- Enterprise / premises advanced voice & data network extension

Wireless Wide Area Network (WWAN)
- Metro/Geographical area
- Ubiquitous public connectivity with virtual private networks

APPLICATIONS

WPAN
- IrDA (Infrared)
- 802.15 (Bluetooth)

WLAN
- CT2
- UPCS
- DECT
- PHS
- 802.11
- 802.11b
- 802.11a
- HiperLAN2

WWAN
- TDMA
- CDMA
- GSM
- CDPD
- 3G
- UMTS
- 1xRTT
- GPRS

Copyright 2002 Vectara Innovations, LLC

6/26/2002
Wireless Technologies

- Infrared
- Bluetooth
- Hyperlan2
- HomeRF (10Mbps)
- 802.11b (11Mbps)
- 802.11a (54Mbps)
- Beyond 802.11a
- 2.5G Cellular
- 3G Cellular
- CDPD
- WAP
- i-Mode
- GPRS
- SMS
- UMTS
Wireless Technologies: Other

- Ricochet
- RIM/Blackberry
- Mesh Networks
- Ad Hoc Networks
- Mobile IP
- Satellite
- Special-purpose wireless
- UWB

Many different security approaches are used
Wireless Network Parameters

- Coverage – line-of-site, point-to-point, in-building, national, and global
- Bandwidth – 9.5kbps to 2Mbps and beyond
- Cost – very low (IR) to expensive (satellite)
- Common use – PAN to campus to global coverage
- Standard and protocols
Wireless Security Approaches
1G Cellular Authentication – Not Mutual-Authentication

Cellular Telephone

- ESN / MIN
- Dialed Digits
- SSD-A
- A-Key
  - 64-bits
- CAVE Algorithm
- Challenge (RAND)
  - 32-bits
- Response (AUTH)
  - 18-bits
- =?

Cellular Network

- Random Number Generator
- Dialed Digits
- ESN / MIN
- SSD / A-Key Database
- SSD-A
  - 64-bits
- =?
  - Y: Accept
  - N: Reject

Copyright 2002 Vectara Innovations, LLC
Custom 802.11 Security Solution

1. **Client associates with access point**

2. **Access point blocks all user requests to access LAN**

3. **User performs network log-on (User ID and password)**

4. **RADIUS server and client mutually authenticate and derive WEP session key**

5. **RADIUS server delivers session key to access point**

6. **Client and access point activate WEP.**

7. **Client and access point use WEP and key for protection of transmissions.**
VPN-based Security

Enterprise Network

Private Network - Unencrypted
Public Network - Encrypted

Contivity

802.11 APs

802.11 terminals

Copyright 2002 Vectara Innovations, LLC
Remote Access VPNs

Access to corporate network via a broad range of access technologies

Copyright 2002 Vectara Innovations, LLC
IPSec Mode and Protocol Summary

- **Tunnel Mode**
  - New IP Header
  - Header AH
  - Original IP Header

- **Transport Mode**
  - Original IP Header
  - Header AH

- **ESP**
  - New IP Header
  - Header ESP
  - Original IP Header

- **AH**
  - New IP Header
  - Header AH
  - Original IP Header

Authentication / Integrity

Encrypted
Summary and Conclusions

• Active and passive attacks exist
• Adversaries and motivations are numerous
• Security requirements include confidentiality, integrity, authentication and availability
• Wireless, a constrained environment, introduces some additional challenges
• Cryptography is the most important security tool
• Integrity may be more important than privacy
• Key Management needs to be carefully considered from the beginning
Summary and Conclusions

• Cannot underestimate the capabilities of the adversaries
• There are many ways to “skin the cat” but successes should be leveraged
• End-to-end cryptography is optimal
• Must learn from history
  ▪ Build security into system from the beginning
  ▪ Use “good cryptography”
  ▪ Design security to anticipate changes in threats and “Moore’s Law”
Open Discussion

Questions & Answers
Presenter Information

Leslie D. Owens (Les)
Founder and CTO, Vectara Innovations, LLC
Adjunct Assistant Professor, Georgetown University
Technical Editor, Wireless Security Perspectives

703/267-3077
703/980-3877 (cellular)
703/757-8174 (fax)
les.owens@worldnet.att.net (email)
Vectara Innovations, LLC

Wireless and security solutions