Security in SDR and Cognitive Radio: Will History Repeat?

Global Regulatory Summit on SDR and Cognitive Radio–Fairmont-Washington Hotel
June 20, 2005 –Washington, DC

Leslie D. Owens, Booz Allen Hamilton
For additional information contact:

Les Owens
Owens_les@bah.com
703-902-7091
Information Assurance for DoD
Booz Allen Hamilton
“Those who cannot remember the past are condemned to repeat it.”

George Santayana, 1863 - 1952
Spanish-born American poet and philosopher
The Life of Reason
Outline

- 1G / 2G Cellular Security
- Wi-Fi Security
- Lessons-Learned from Mobile & Wireless Security
- Security in SDR and Cognitive Radio
- Questions and Answers
1G / 2G Cellular Security
The Cellular Concept

Desired cell

7-cell reuse structure

Co-channel cell causing interference

For distance, the Friis equation applies.
1st Generation Cellular Identification System

Wireless Interface (Radio Path)

ESN: 82345AC5
MIN: 703-835-2902

Dialed digits: (212)-731-4321

Subscriber
Cellular Cloning: The Approach

Legitimate Customer – “Good Guy”

Key Motivators
- Anonymity
- Mobility
- Status
Wireless Fraud Was a Major Problem

Clone Fraud
This type of theft of service was a major problem worldwide for several years. This was because the original cellular system had no security.

Classic example of system totally without security.

Subs increasing – fraud too!
Estimated Cellular Growth in US

Source: Cellular Telecommunications Industry Association and Donaldson, Lufkin & Jenrette

Dated material – For illustrative purposes only
Concept of Handoff

Base Station 1

Base Station 2

Handoff point

Halfway point

D = 2 kilometers

移动

Halfway point

d_1

d_2

D = 2 kilometers
Taxonomy of Fraud Control Techniques

Fraud Control Techniques

Less Effective

Fraud Detection Techniques

Profiler

Intelligent Switch

More Effective

Fraud Prevention Techniques

Weak Fraud Prevention Techniques

Static PINs

Multiple PINs

RF Fingerprinting

Voice Verification

Strong Fraud Prevention Techniques

Dynamic PINs

Authentication

Booz | Allen | Hamilton
Principle of Profiling System – “clone detector”

1. **Cellular Switch**
   - Subscriber Database
   - ESN/MIN
   - Call Detail Formatting
   - Call Details
     - Call Origination
     - Call Destination
     - Call Duration
     - Call time
     - etc.

2. **Clone Detection System**
   - Subscriber Database
   - Profile Analysis
   - Profile Analyze
   - Call Detail (CDRs)
   - Profile Analysis
     - Call collision/overlap
     - Velocity checks
     - Long duration calls
     - Usage change
     - Typical bill Threshold
     - Abnormal pattern
     - Abnormal originations
     - Abnormal destinations
     - Hot numbers
   - Profiles Match
     - Yes
     - Fraud likely
   - Fraud unlikely
   - Human Interdiction

 Hmm...Dr. Smith does not usually call Columbia at 2A.M. and talk for 25 minutes. Let’s watch this one....
Principle of “Challenge-Response” Cellular Authentication

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Switch</th>
<th>AC</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESN and MIN</td>
<td>Random Number Generator</td>
<td>A-Key Database</td>
</tr>
<tr>
<td>Key</td>
<td>CAVE Algorithm</td>
<td>CAVE Algorithm</td>
</tr>
<tr>
<td>ESN, MIN, SSD, A-Key</td>
<td>Authentication Response</td>
<td>Authentication Response</td>
</tr>
</tbody>
</table>

- Reduced fraud dramatically

Booz | Allen | Hamilton
1G / 2G Cellular Theft of Service in US

Reported Semi-Annual Cloning Losses

Source: Cellular Telecommunications Industry Association
Authentication on Mobile Registrations

RAND_CHALLENGE | ESN | AUTH_DATA
---|---|---
RAND 32 | ESN 32 | IMSI_SI 24

Auth_Signature Procedure

AUTHR 18

Use of a proprietary algorithm

Booz | Allen | Hamilton
Cellular Family Evolution

Wireless Network Technologies: Projected Migration Paths

**Protocol Family**

**First Generation 1980s - mid 1990s**
- **AMPS**
  - basic voice, very limited data, analog circuit.

**Second Generation (2G) mid 1990s - present**
- **AMPS**
  - basic voice, very limited data, analog circuit.

**2.5 Generation late 2000 - 2001**
- **CDMA**
  - Caller ID, voicemail, SMS
  - 9.6 kbps data rate
  - digital circuit
- **1XRTT**
  - simultaneous voice and data
  - 144 - 153 kbps data rate
  - digital circuit
- **TDMA**
  - Caller ID, voicemail, SMS
  - 9.6 kbps data rate
  - digital circuit
- **GSM**
  - Caller ID, voicemail, SMS
  - 9.6 kbps data rate
  - digital circuit
- **GPRS**
  - always-on connection
  - 115 kbps data rate
  - digital packet

**Third Generation (3G) 2002 - 2003**
- **3XRTT & CDMA2000**
  - always-on connection
  - 2 Mbps data rate (stationary)
  - digital packet
- **EDGE / WCDMA**
  - always-on connection
  - 384 kbps EDGE, 2 mbps WCDMA
  - digital packet

**Dated material – For illustrative purposes only**

**Protocol Family**

**AMPS**
- Advanced Mobile Phone Service
  - Sprint PCS, BellSouth, Verizon

**CDMA**
- Code Division Multiple Access
  - AT&T Wireless, SBC, BellSouth

**TDMA**
- Time Division Multiple Access

**GSM**
- General System for Mobile Communications
  - VoiceStream, BellSouth, SBC

Source: Forrester & Wasserstein Perella estimates.
IS-54B / IS-136 Voice Privacy – Conceptually

SSD-B

CAVE KG

VPM

200 ms Voice Input

Voice Coding

Digitized voice

plaintext

260-bits

keystream

260-bits

ciphertext

260-bits

Fixed key XOR makes for bad privacy
SSD Update: Key Update

**MOBILE STATION**
- RANSSD
- A-Key
  - SSD_Generation Procedure
    - SSD_B_NEW
    - SSD_A_NEW

**BASE STATION**
- RANSSD
  - A-Key
  - SSD_Generation Procedure
    - SSD_B_NEW
    - SSD_A_NEW

**SSD Update Message**
- (RANSSD)

**Auth_Signature Procedure**
- RANDBS
  - Base Station Challenge Order (RANDBS)
  - Auth_Signature Procedure
    - AUTHBS
      - AUTHBS = AUTHBS?

**Base Stations Challenge Confirmation Order**
- (AUTHBS)
  - SSD Update Confirmation Order (success)
  - SSD Update Rejection Order (failure)
2nd Generation Cellular Key Hierarchy

A - Key
- Infrequent
- 64-bits

SSD-A
- Infrequent / after roaming
- “Challenge-Response” key
- 64-bits

SSD-B
- 64-bits

VPM
- Per call
- 520-bits

CMEA Key
- 64-bits

Data Key
- 32-bits

Data Mask
- Per call
- 192-bits / variable

Secret “seed” key

Key distribution was missing
Wi-Fi Security
Typical Residential Wi-Fi Deployment

Internet

Cable/DSL Modem

Access Point

Home computers
(with client adapter)
Explosive growth of Wi-Fi

Benefits of Wi-Fi

- Adds mobility to an enterprise
- Very inexpensive to deploy
- May be deployed very quickly
- Provides good performance—same as wired LAN
- Avoids wiring hassles and is particularly attractive in older buildings
- Facilitates change in organizations
- Excellent for transient groups such as standards organizations and conferences
Wi-Fi (IEEE802.11 WLAN) Security

No Security or provided through other means

802.11 Security

Security for air-interface only
Wired Equivalent Privacy (WEP) / Entity Authentication – Flawed

- Authentication is not enabled; only simple SSID identification occurs
- The cryptographic keyspace is too small (keys are short)
- Cryptographic keys are shared and are not changed frequently
- Initialization Vectors (IV) are short or fixed (or are reset inappropriately)
- Mutual authentication (bilateral) does not occur
IEEE802.11 Entity Authentication is Not Adequate

IEEE802.11Authentication

Open System Authentication
1-stage Challenge-Response

Non-cryptographic
Does not use RC4

A station is allowed to join a network without any identity verification.

Shared-key Authentication
2-stage Challenge-Response

Cryptographic
Uses RC4

A station is allowed to join network if it proves WEP key is shared.
(Fundamental security based on knowledge of secret key)
(Not required)
Wi-Fi Brings Security Concerns

- This tetherless technology is attractive for numerous reasons.
- "Out of the box" technology has numerous flaws.
- Very risky without vigilance.
- Secure design and implementation is critical.
IEEE 802.11i Amendment – Enter Robust Security Networks

IEEE 802.11 Security

Pre-Robust Security Networks

- WEP
  - Confidentiality
  - Open System
  - Shared-Key
  - Authentication

Robust Security Networks

- 802.1X Port-based Access Control and Extensible Authentication Protocol
- Key Generation
- TKIP
  - “Security Methods” Confidentiality, Data Origin Authentication and Integrity
- CCMP

Confidentiality, Data Origin Authentication and Integrity

Authentication and Access Control

Authentication
IEEE802.1X Port-Based Access Control

Network/Enterprise Edge
- EAP Over LANs (EAPoL)
- Wireless Interface
- User Machine (With Client Adapter)

Enterprise Network
- EAP Over RADIUS
- Wired Ethernet LAN
- RADIUS Server
- Auth dB

Transmissions blocked at AP until successful authentication occurs
RSN Phases of Operation

Phase 1 – Discovery

Phase 2 – Authentication

Phase 3 – Key Generation and Distribution

Phase 4 – Protected Data Transfer

Phase 5 – Connection Termination

AS- AP Key Distribution
Pairwise Key Hierarchy

Out-of-band path

PSK
Pre-shared Key
256-bits

User defined cryptoperiod

EAP Method Path

AAAK
AAA Key
≥256-bits
When EAP Method authentication occurs

Following EAP authentication

EAPOL Key Encryption Key

EAP Method Path

EAPOL Key Confirmation Key

Pairwise Transient Key

Pairwise Master Key

PMK
256-bits

Pairwise Transient Key

PTK
384-bits (CCMP)
512-bits (TKIP)

After 4-way handshake and session authentication

KCK

EAPOL Key Confirmation Key
128-bits

KEK

EAPOL Key Encryption Key
128-bits

TK

Temporal Key
128-bits (CCMP)
256-bits (TKIP)

These keys are components of the PTK

Legend:

No modification
Possible truncation
PRF (Pseudo Random Function) using HMAC-SHA-1

≥

≥

≥

≥
IEEE 802.1X Flows – Management Frame Security being developed

- 802.1X EAP Probe Request
- 802.1X EAP Probe Response
- Access Request (EAP Request)
- Extensible Authentication Protocol Exchange
- Accept / EAP-Success Key Material
- 802.1X EAP Success
- 802.1X controlled port blocked
Data Confidentiality and Integrity Protocol (CMP Encapsulation)

MAC Header | Increment PN | KeyID | PN | PN | PN | A2, Priority | TK

Construct CCMP Header | Construct Nonce | KeyID | PN | PN | PN | A2, Priority

Construct AAD | AAD | Nonce | Data

CCM Encryption | AES | TK | 128-bit

128-bit | K=16, M=8, L=2

MAC Header | CCM Header | Encrypted Data | MIC

Plaintext MPDU

48-bit

48-bit

Booz | Allen | Hamilton
Lessons-Learned from Mobile & Wireless Security
Some Lessons-learned for Wireless – 1

- We must learn from our past mistakes
- Robust, well-implemented cryptography is a must
- Key distribution and management need to be considered carefully and cannot be ignored
- Existing, robust cryptographic algorithms must be leveraged
- Engineering designers must be “forward leaning” (e.g., with key sizes, algorithms, techniques)
- Build security into wireless system from the beginning – plan for security evolution
Some Lessons-learned for Wireless – 2

- Use the “right” people for the job
- Technology, for good and bad, will advance – remember Moore’s Law
- Don’t let IPR (e.g., patents), politics, bureaucracy and export controls get in the way of good security
- Don’t be surprised at what the adversary can do
- “Security thru obscurity” does not work for long
- There are many motivations for the adversaries – in particular, money and anonymity
Some Lessons-learned for Wireless – 3

- Look at security holistically
- Standardized solutions ultimately win out
- Designing robust security (i.e., algorithms and protocols) is difficult
- What didn’t work in the past may in the future
- Have a dedicated team with security as its focus (not an ad hoc group)
- Leverage the excellent work of other security practitioners (3GPP, AHAG, IETF, IEEE, TCG)
Some Lessons-learned for Wireless – 4

- *A priori* authentication is essential
- *A posteriori* detection is critical
- Policies need to drive the requirements
- Security is difficult to analyze, is clumsy and is expensive *after the fact*
- The ROI is better when security driven into standards
- With security – the devil is in the details
Security in SDR and Cognitive Radio
Software Defined Radio

“… to build flexible radio systems, multiservice, multistandard, reconfigurable and reprogrammable by software.”

Software Defined Radios: programmable radio transceivers that are able to self-configure to meet the needs of its user, which provide the ability to be “future-proof” and offer numerous wireless air interfaces and capabilities.
Benefits of SDR

- to allow users (subscribers) to roam from region to region with different air-interface standards
- to correct software “bugs” in existing equipment
- to provide software upgrades and to provide additional capabilities (“future-proof”)
- to provide value-added services
SDR as Mobility will serve critical needs...

**Supervisory Control and Data Acquisition (SCADA)**
- Remote telemetry for utilities and energy systems

**Informatics / Geolocation**
- Navigation, location-aware services, surveying, aviation, direction-finding

**Remote Sensing**
- Urban search and rescue, geology, environmental science, and civil engineering

**Point of Sale / Asset Tracking**
- Mobile commerce, inventory, border enforcement

---

Booz | Allen | Hamilton
Public Safety will be a beneficiary
Vulnerabilities in SDR: Related to Embedded Interfaces

- Software download Vulnerabilities
  - AMPS Vulnerabilities:
    - Financial Fraud
    - Loss of voice privacy
  - Wi-Fi Vulnerabilities:
    - Unauthorized access
    - Loss of data privacy
- Platform Vulnerabilities

SDR inherits the vulnerabilities of the radios interfaces
Software Download

“Software download” is the protocol and transfer of configurations, features, functions, waveforms, protocols, or applications to enable the reconfigurability of SDR. As such it is a key enabler for SDR.

Three basic requirements:
- should occur as fast as possible
- should occur without error
- should be easy to perform

Techniques for Software Download:
- Over the terminal’s primary wireless air-interface
- Via a memory card, SIM (subscriber identity module) or other Smart Card
- Via a kiosk or through some other device / mechanism
Wireless Technology Alternatives

- Bluetooth
- 802.11a, b, g
- 2.5 / 3G Cellular
- WAP
- GPRS
- Hyperlan2 /HomeRF
- SMS
- 802.16
- Satellite
- UWB
- Blackberry
- CDPD
- MANETs
- Near field communications
- 802.20
- Custom waveforms

Wireless is more than cellular and Wi-Fi
High-level Taxonomy of Attacks on SDR

- Interception (Confidentiality)
  - software piracy
  - loss of anonymity
  - private configuration exposure

- Interruption (Availability)
  - jamming
  - malicious code
  - resource exhaustion

- Modification (Integrity)
  - unit malfunction
  - change of preferences
  - security function circumvention

- Fabrication (Authenticity)
  - rogue terminal
  - financial fraud
  - network impersonation

Passive attacks

Active attacks

Software Defined Radio Attack Taxonomy
What are the required services for the SDR / CR environment?

- Access Control
- Audit
- Authentication
- Availability
- Confidentiality (privacy)
- Integrity
- Key Management
- Non-repudiation
PKC Software Download

Manufacturer

01010111010101010101010101010101010101010101010101010101010101010101010000000001101

Random key, K

Secure Key generator

Public key certificate of SDR radio

Software upgrade

C

Secure Key

generator

Public key certificate of manufacturer

Manufacturer

Disassemble software load: s, E_k(C), E_k(K)

RSA Verify

s

E_k(C)

E_k(K)

Private key of SDR radio

AES Decrypt

recovered key, K

SHA-256

recovered Software upgrade

C

01010111010101010101010101010101010101010101010101010101010101010101010000000001101

Hashes match?

Yes

Install software – no modifications, tampering

No

Abort load – bad software

Install new software in memory, hardware, etc.

Hasseas?

Transmit load from manufacturer to SDR

Assemble software load: s, E_k(C), E_k(K)

RSA Encrypt

S

E_k(C)

E_k(K)

SDR public key, K

Secure key storage

Private signing key of manufacturer

SHA-256

h

h'

Public key certificate of manufacturer

01010111010101010101010101010101010101010101010101010101010101010101010000000001101

RSA Sign

h

REv

AES Encrypt

s

E_k(C)

E_k(K)

Random key, K

Secure Key generator

Public key certificate of SDR radio

Manufacturer

Disassemble software load: s, E_k(C), E_k(K)

RSA Verify

s

E_k(C)

E_k(K)

Private key of SDR radio

AES Decrypt

recovered key, K

SHA-256

recovered Software upgrade

C

01010111010101010101010101010101010101010101010101010101010101010101010000000001101

Hashes match?

Yes

Install software – no modifications, tampering

No

Abort load – bad software

Install new software in memory, hardware, etc.

Hasseas?
Challenges due to Security in SDR / CR

- They generally are low power
- They generally have slower processors
- They generally have limited storage capability
Relationships: Security Policy to Security Mechanisms

Security Policy

Security Model / Requirements

Security Architecture

Security Mechanisms

<table>
<thead>
<tr>
<th>Passwords</th>
<th>Firewalls</th>
<th>Encryption</th>
<th>Audit Trails</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tokens/Smart Cards</td>
<td>Filters/Guards</td>
<td>Digital Signatures</td>
<td>MLS/Secure OSs</td>
</tr>
<tr>
<td>Biometrics</td>
<td>Intrusion Detection</td>
<td>Key Man’ment/PKI</td>
<td>Virus Detection</td>
</tr>
</tbody>
</table>
The Way Forward – Some Thoughts

- Early expert involvement is essential
- Establishing an architecture and CONOPS are critical
- Defining the vulnerabilities is important
- Studying the past is crucial
- Dreaming the impossible is wise
- Understanding the applicable policies is required
- Determining the requirements is mandatory
- Developing a security architecture is necessary
- Anticipating the future is prudent
Questions and Answers
“To err is human, to forgive divine.”

Alexander Pope, 1688 – 1744
English Poet and brilliant satirist

“Rules for being Human”

Rule #1: You will learn lessons.
Rule #2: There are no mistakes–only lessons.
Rule #3: A lesson is repeated until it is learned.
Rule #4: If you don’t learn the easy lessons, they get harder.
Rule #5: You’ll know you’ve learned a lesson when your actions change.
Booz | Allen | Hamilton

delivering results that endure

For additional information contact:

Les Owens
Owens_les@bah.com
703-902-7091
Information Assurance for DoD
Booz Allen Hamilton
Backup Material
To Probe Further

- IS-91, IS-136 and IS-95 family of standards available from TIA (Telecommunications Industry Association)

- Security Algorithms and Procedures are found in the TIA Common Cryptographic Algorithms (CCA) document

- The TIA TR-45 AHAG (Ad Hoc Authentication Group) still meets to discuss evolving security for 2G+/3G
US Cellular Families

- **AMPS – IS-91 family (analog voice)**
  - CMEA, CAVE authentication

- **TDMA – IS-54B, IS-136 family**
  - CMEA, XOR voice privacy, CAVE authentication, ORYX data security

- **CDMA – IS-95 / IS-95A family**
  - CMEA, private long code DSSS voice privacy, CAVE authentication, ORYX data security
Summary of 2G Cellular Security Services

- Access Control – through the authentication of users/terminals
- Audit – provided at the switch for billing
- Authentication – terminal authentication only (A-keys embedded in phones)
- Availability – not explicitly addressed
- Confidentiality (privacy) – done for voice, data and signaling
- Integrity – not performed explicitly
- Key Management – done out of band (manually, floppy disk/mail, EDI mailboxes)
- Non-repudiation – not done at all
Algorithms in 2G Cellular Security

- **CAVE (Cellular and Voice Encryption) Algorithm**: Used for “challenge-response” authentication and for key generation/update – developed by Louis Finkelstein / Motorola

- **CMEA (Cellular Message Encryption Algorithm)**: Used for signaling encryption – developed by AT&T Bell Labs
  - Caller ID / Called address messages
  - PIN messages

- **XOR**: Used for voice privacy – developed by TIA TR45.3 committee

- **ORYX**: Used for data security – developed by Jim Reeds / AT&T Bell Labs
NIST Special Publication 800-48

The document examines the benefits and security risks of 802.11 Wireless Local Area Networks (WLAN), Bluetooth Ad Hoc Networks, and Handheld Devices such as Personal Digital Assistants (PDA). The document also provides practical guidelines and recommendations for mitigating the risks associated with these technologies.

New NIST Special Publication

- NIST is currently drafting another Special Publication on Next Generation IEEE802.11 WLAN security (IEEE802.11i)
- Describes network components and “Principles of Operation” of Robust Security Networks
- Provides Detailed Overview of Security Features and Mechanisms
- Provides Security “Best Practices” with Checklists
- Provides Case Studies on secure implementations
- To publish in Summer 2005
Advanced Encryption Standard (AES)

- Is an iterated block cipher
- Will be used for confidentiality and integrity
- Is NIST’s latest approved cryptographic algorithm
- Defined by Federal Information Processing Standard (FIPS) 197
## History Repeats Itself

<table>
<thead>
<tr>
<th>WiFi</th>
<th>1st Generation Cellular</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time Period</strong></td>
<td>2002</td>
</tr>
<tr>
<td><strong>State of industry</strong></td>
<td>Exploding</td>
</tr>
<tr>
<td><strong>State of security</strong></td>
<td>Poor</td>
</tr>
<tr>
<td><strong>Buzzwords</strong></td>
<td>War-driving and war-chalking</td>
</tr>
<tr>
<td><strong>Tools of choice</strong></td>
<td>Netstumbler and Airsnort</td>
</tr>
<tr>
<td><strong>Detectability</strong></td>
<td>Difficult.</td>
</tr>
<tr>
<td><strong>Triage solution</strong></td>
<td>Patched WEP, VPNs</td>
</tr>
<tr>
<td><strong>“Hot” solution to the problem</strong></td>
<td>Switch-based security devices</td>
</tr>
</tbody>
</table>
Security Definitions

- **Access Control** – This security service ensures that controls exist for accessing computer system information. The controls may be provided by or for the system.

- **Audit** – ensures that transactions are recorded in a journal (audit trail). An audit trail is typically a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of events (environments and activities) leading to an operation, procedure, or event in a security-related transaction from beginning to end.
Security Definitions

- **Authentication** – ensures that the origin of a message or electronic document is correctly identified and provides assurance that the identity is correct. Authentication also means that an entity (e.g., a user, process, or computer system) is properly identified.

- **Authorization** – is the right or permission that is granted to a user, program, or process to access a system resource.
Security Definitions

- **Confidentiality** – ensures that only authorized individuals and parties can access information in a computer system or communications network. This access includes copying, displaying, printing, and other forms of disclosure.

- **Integrity** – ensures that only authorized individuals and parties can modify information in a computer system or communications network. Integrity includes changing, deleting, inserting, or delaying information in transmitted messages or stored messages.
Security Definitions

- **Key management** – is the process of handling cryptographic keys and related material (e.g., initialization values, counters) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the material. **N.B.**: this process (security service) is probably the most critical service a cryptographic system. It is oftentimes the most difficult part of cryptosystem design and operation; moreover, it is frequently poorly done or not done at all.
“There are no victories at bargain prices.”

General Dwight D. Eisenhower, 1890 - 1969
34th US President (’53-’61)
World War II Supreme Commander
Thank you!