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

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

“Those who cannot remember the past are condemned to repeat it.”

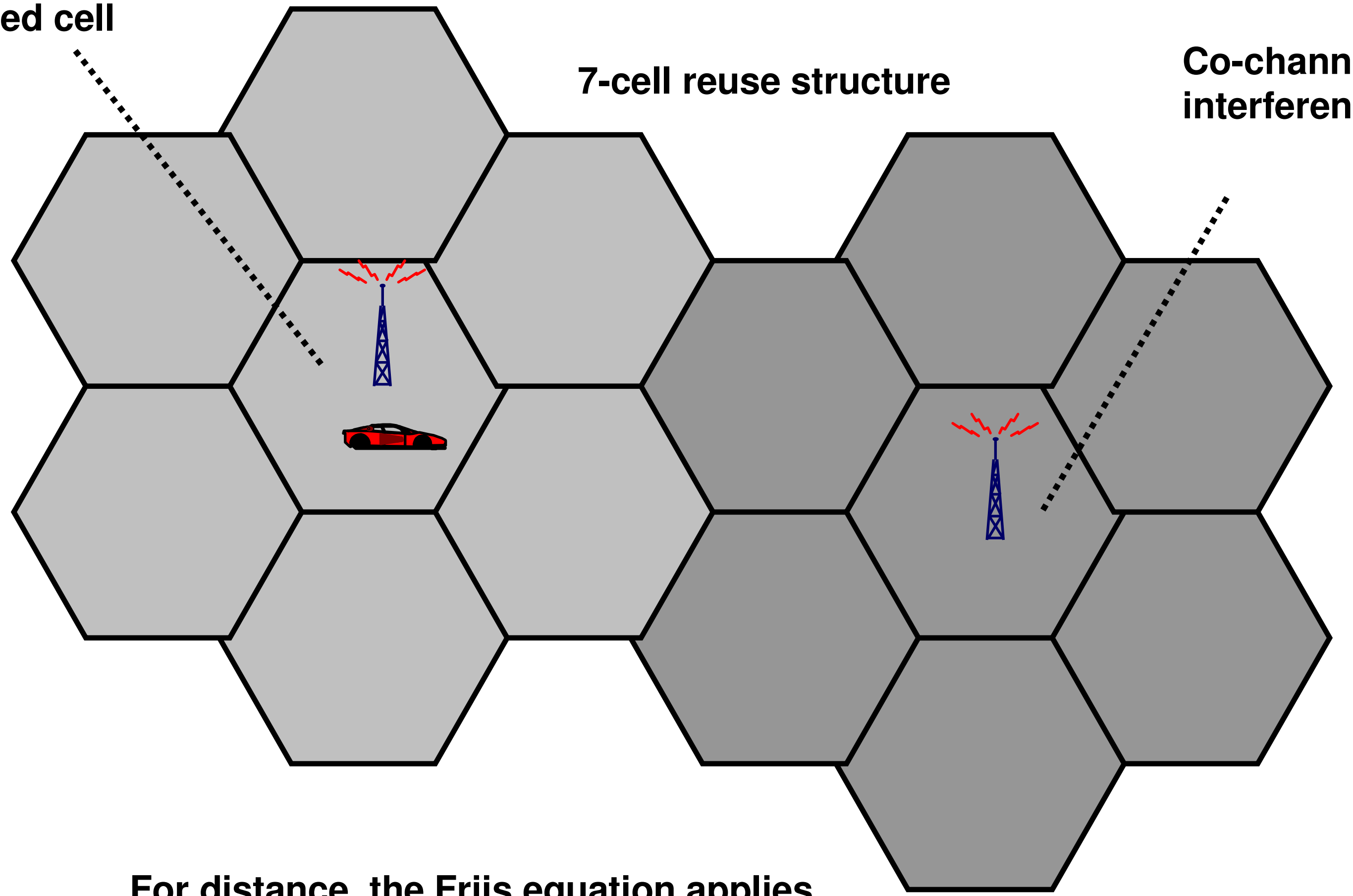
George Santayana, 1863 - 1952
Spanish-born American poet and philosopher
The Life of Reason

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



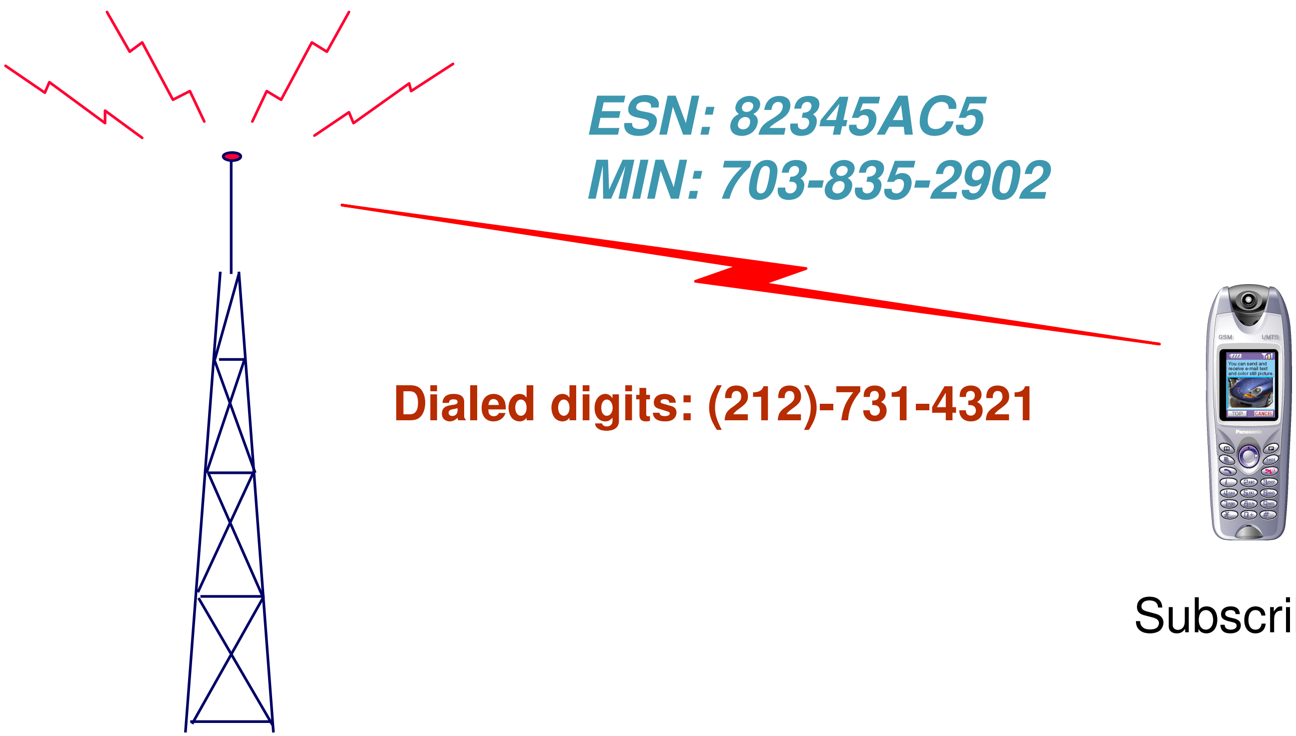
Desired cell

7-cell reuse structure

Co-channel cell causing interference

For distance, the Friis equation applies.

1st Generation Cellular Identification System



Wireless Interface (Radio Path)

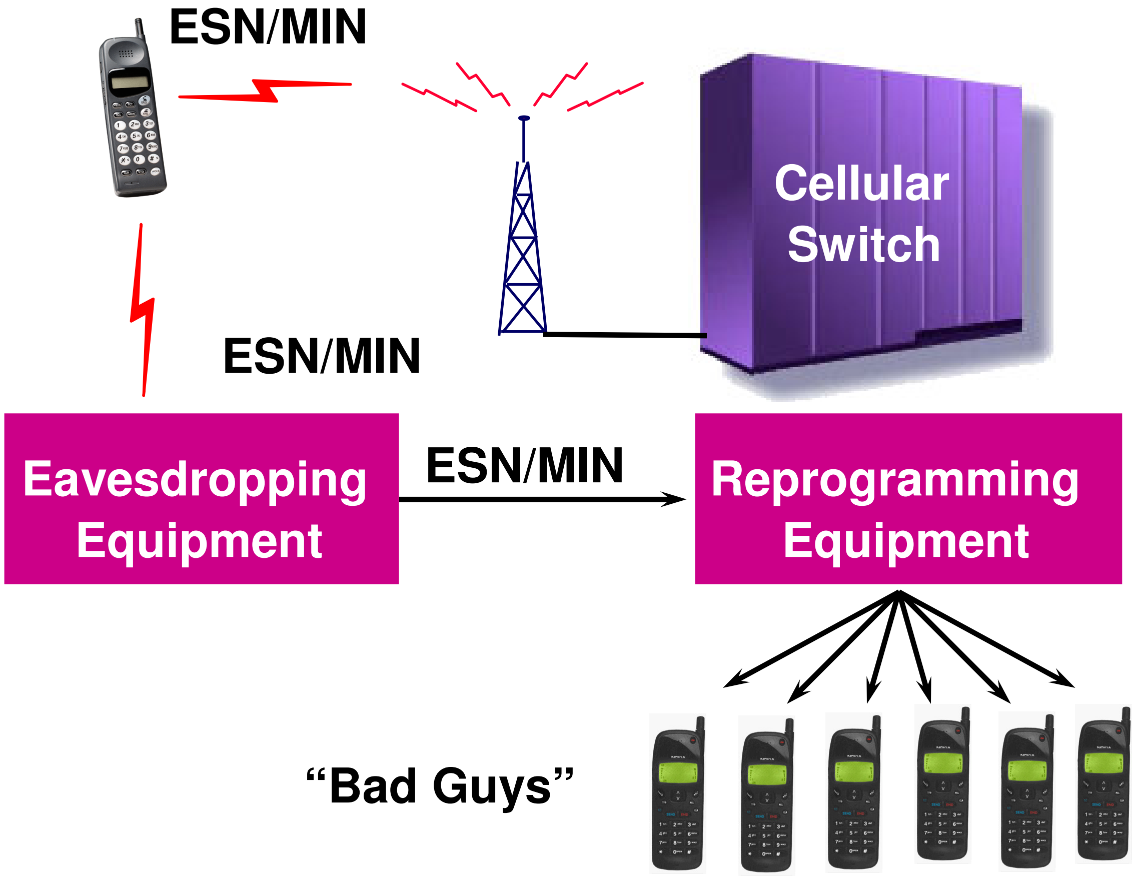
ESN: 82345AC5
MIN: 703-835-2902

Dialed digits: (212)-731-4321

Subscriber

Cellular Cloning: The Approach

Legitimate Customer – “Good Guy”



ESN/MIN

Cellular Switch

ESN/MIN

Eavesdropping Equipment

ESN/MIN

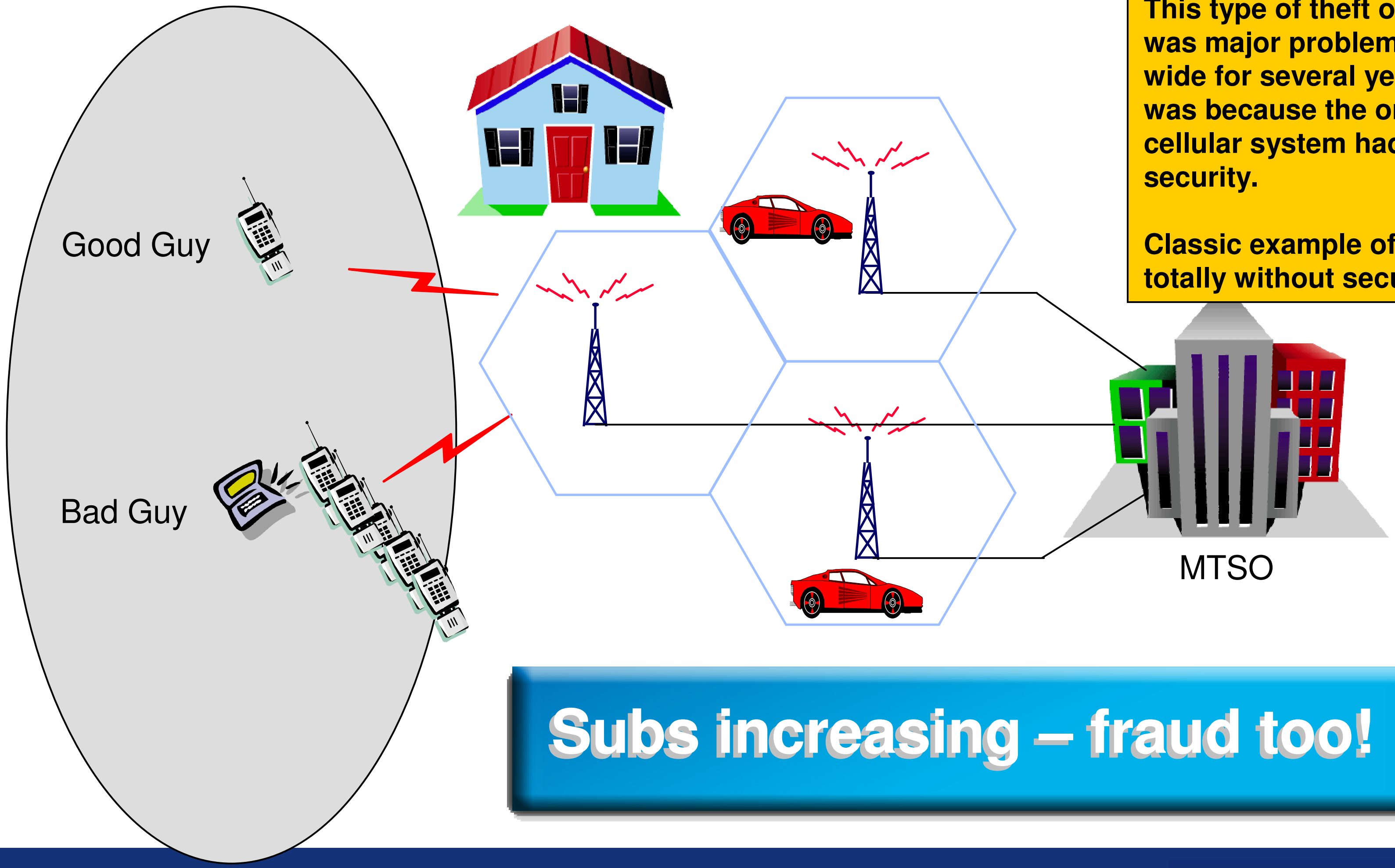
Reprogramming Equipment

“Bad Guys”

Key Motivators

- Anonymity
- Mobility
- Status

Wireless Fraud Was a Major Problem



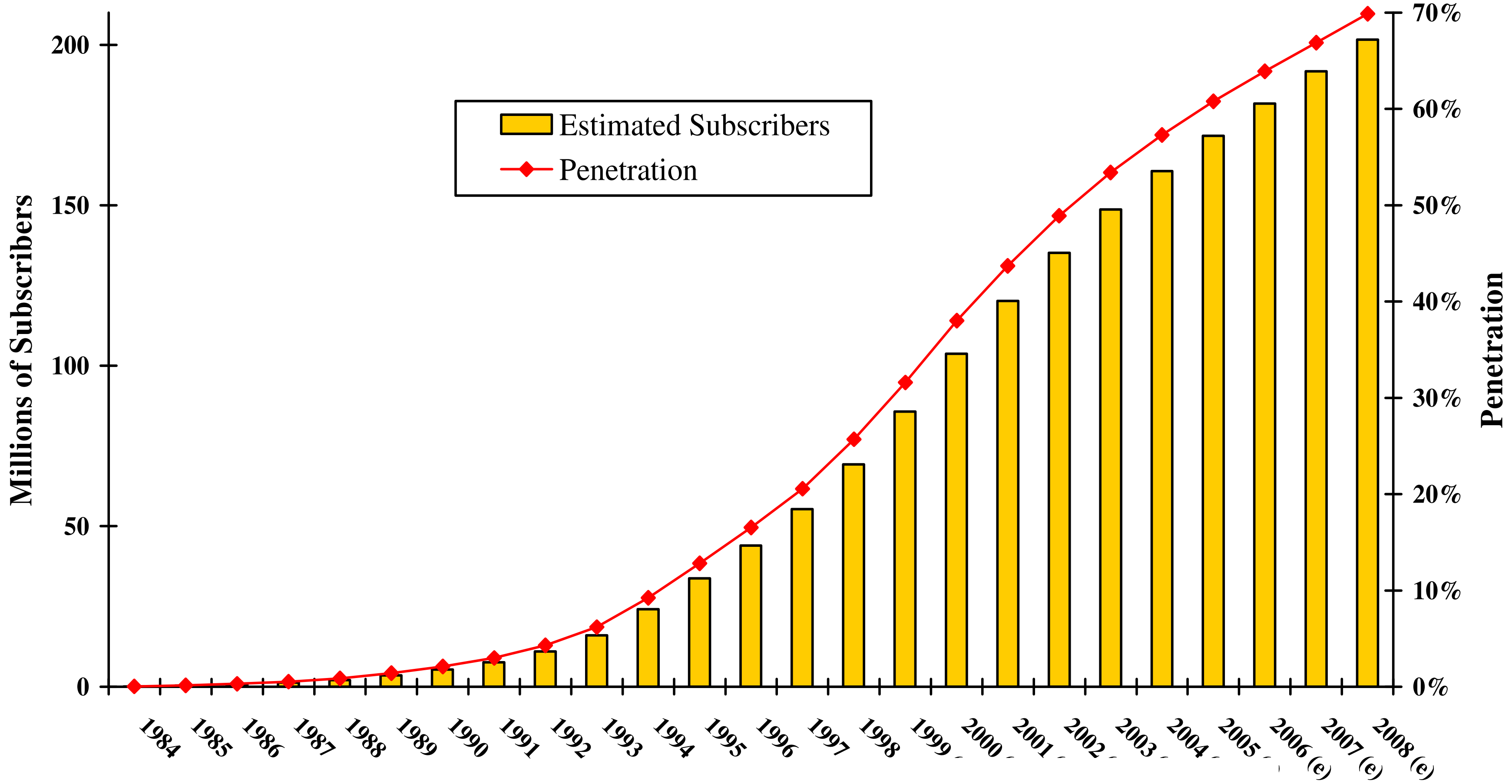
Clone Fraud

This type of theft of service was major problem world-wide for several years. This was because the original cellular system had no security.

Classic example of system totally without security.

Subs increasing – fraud too!

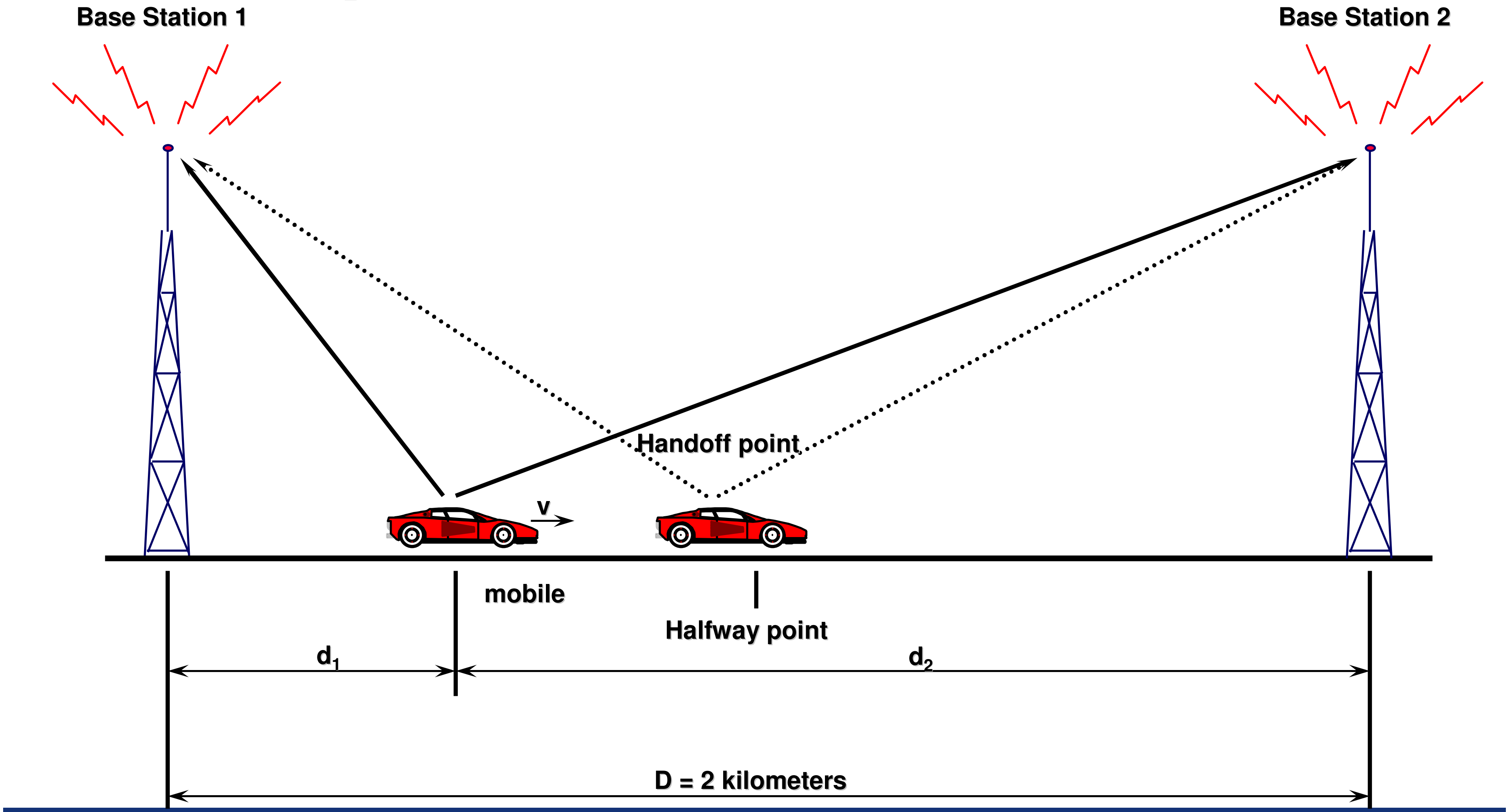
Estimated Cellular Growth in US



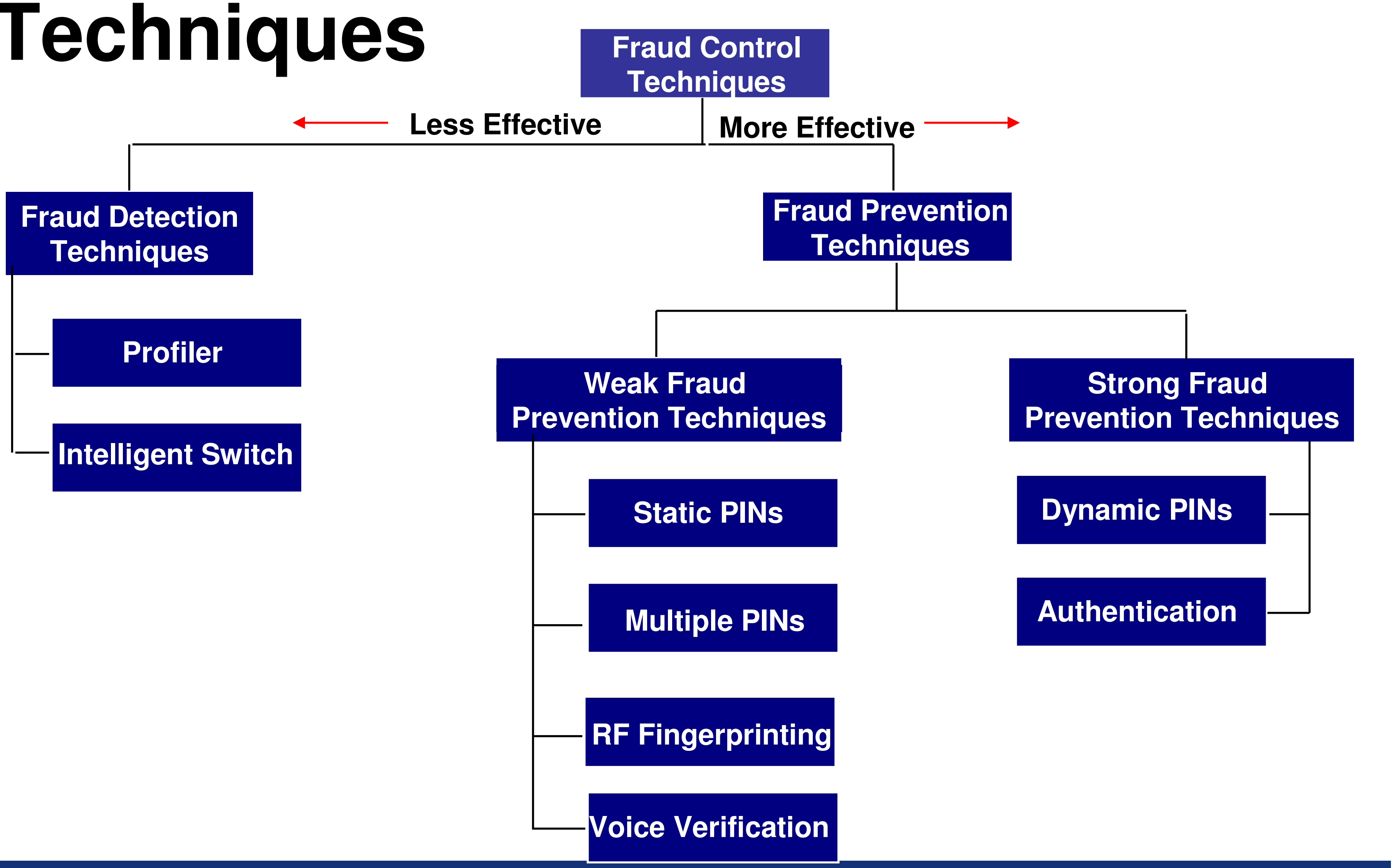
Source: Cellular Telecommunications Industry Association and Donaldson, Lufkin & Jenrette

Dated material – For illustrative purposes only

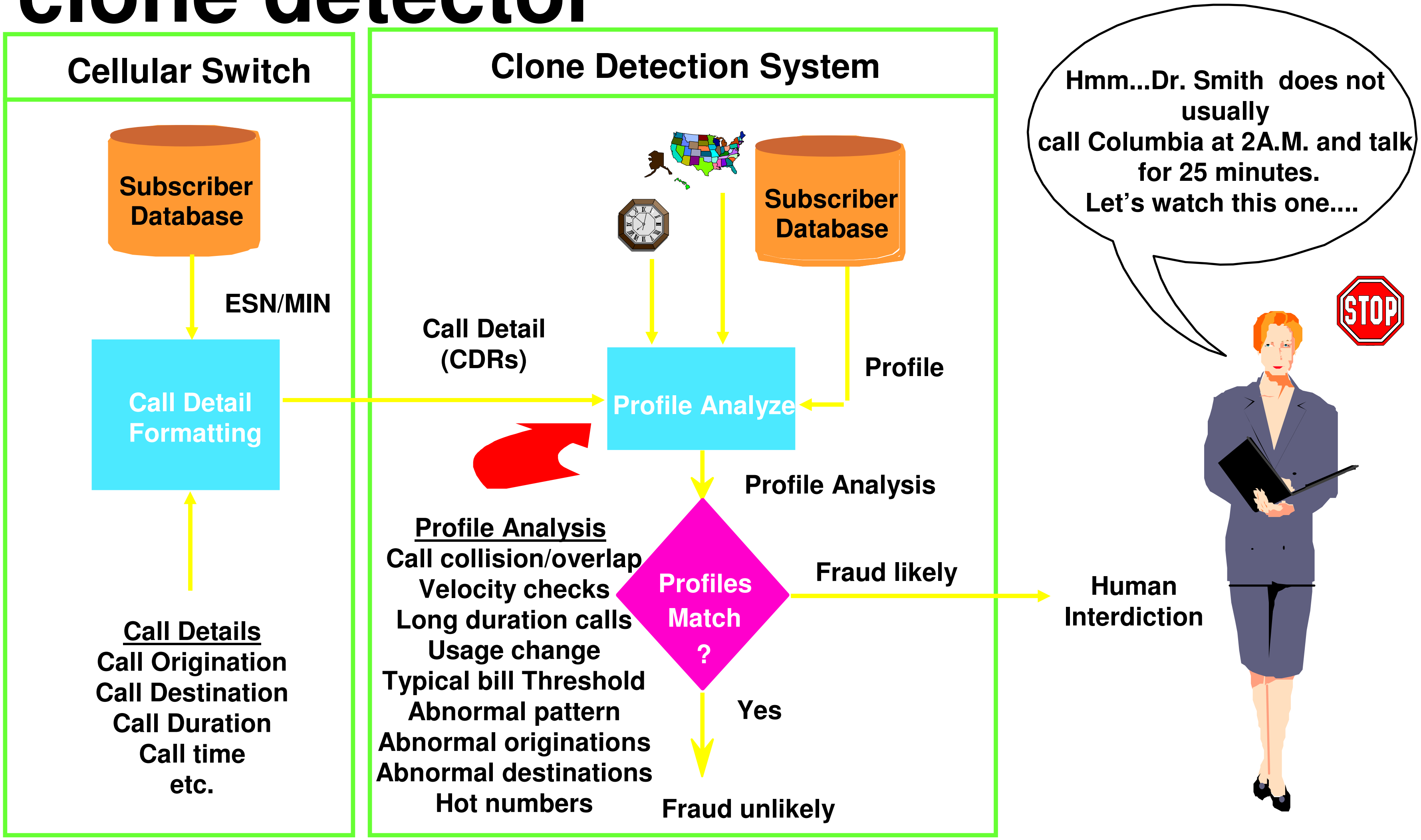
Concept of Handoff



Taxonomy of Fraud Control Techniques



Principle of Profiling System – “clone detector”



Cellular Switch

Subscriber Database

ESN/MIN

Call Detail Formatting

Call Details
Call Origination
Call Destination
Call Duration
Call time
etc.

Clone Detection System

Call Detail (CDRs)

Subscriber Database

Profile

Profile Analyze

Profile Analysis

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 ?

Fraud likely

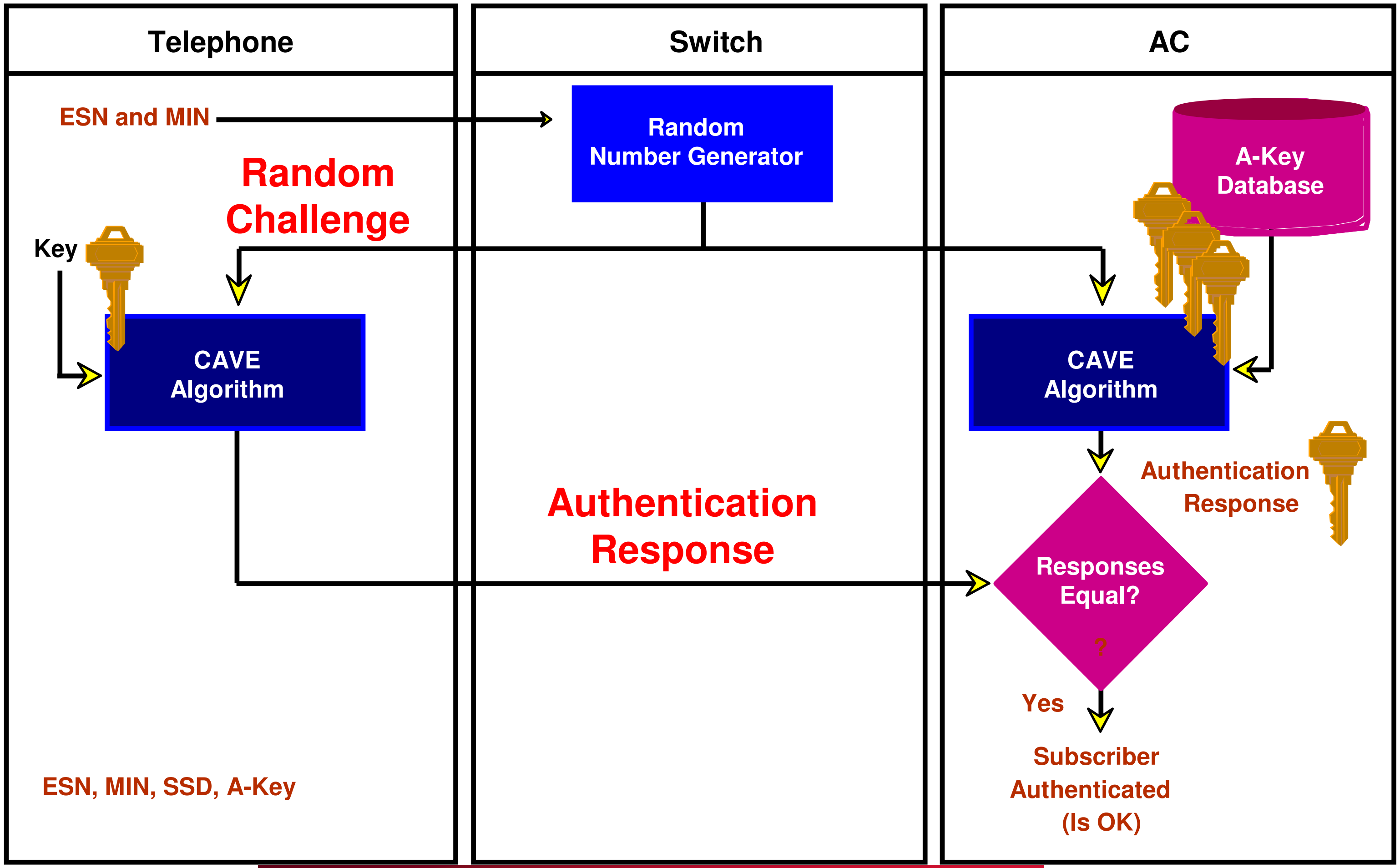
Yes

Fraud unlikely

Human Interdiction

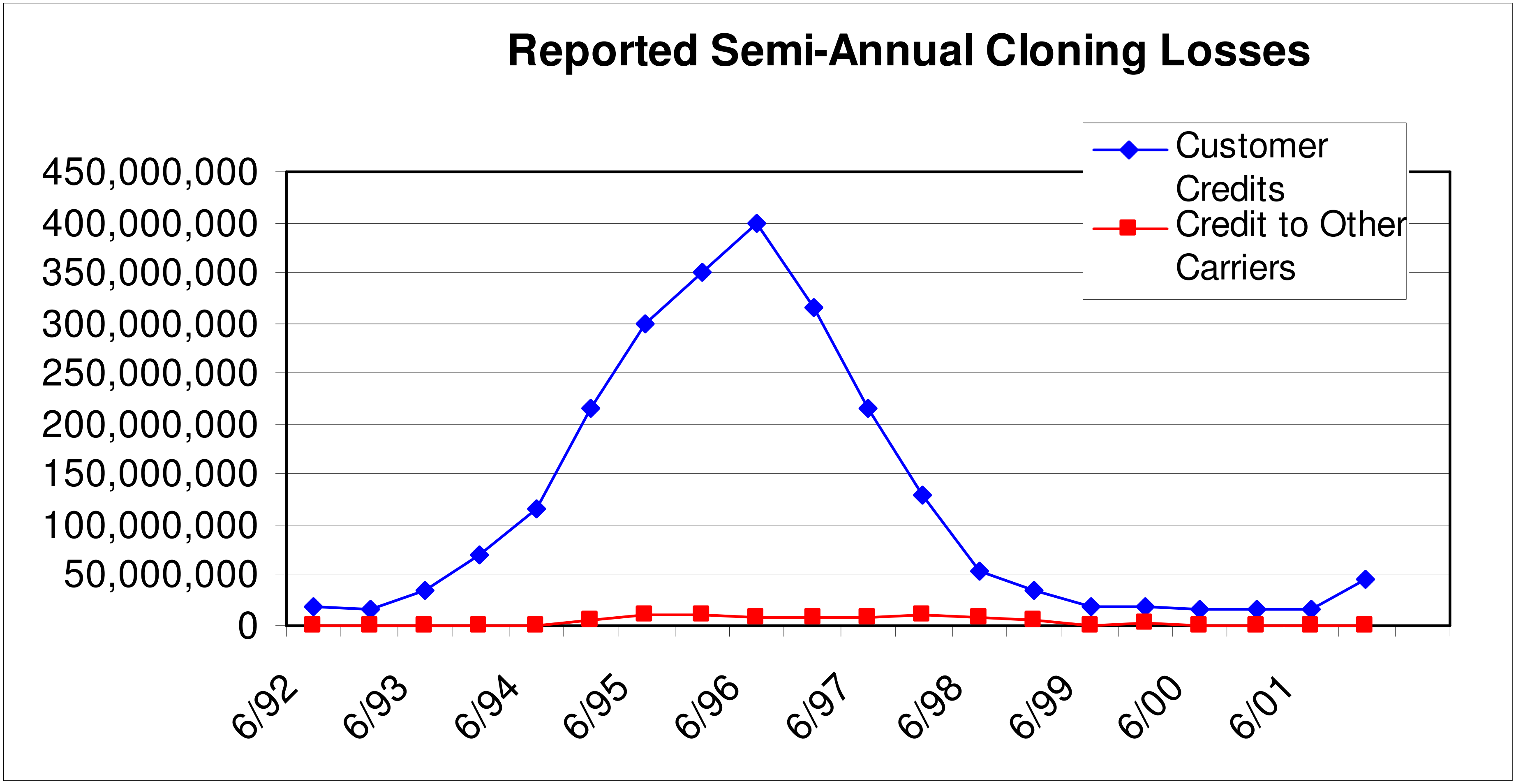
Hmm...Dr. Smith does not usually
call Columbia at 2A.M. and talk for 25 minutes.
Let’s watch this one....

Principle of “Challenge-Response” Cellular Authentication



Reduced fraud dramatically

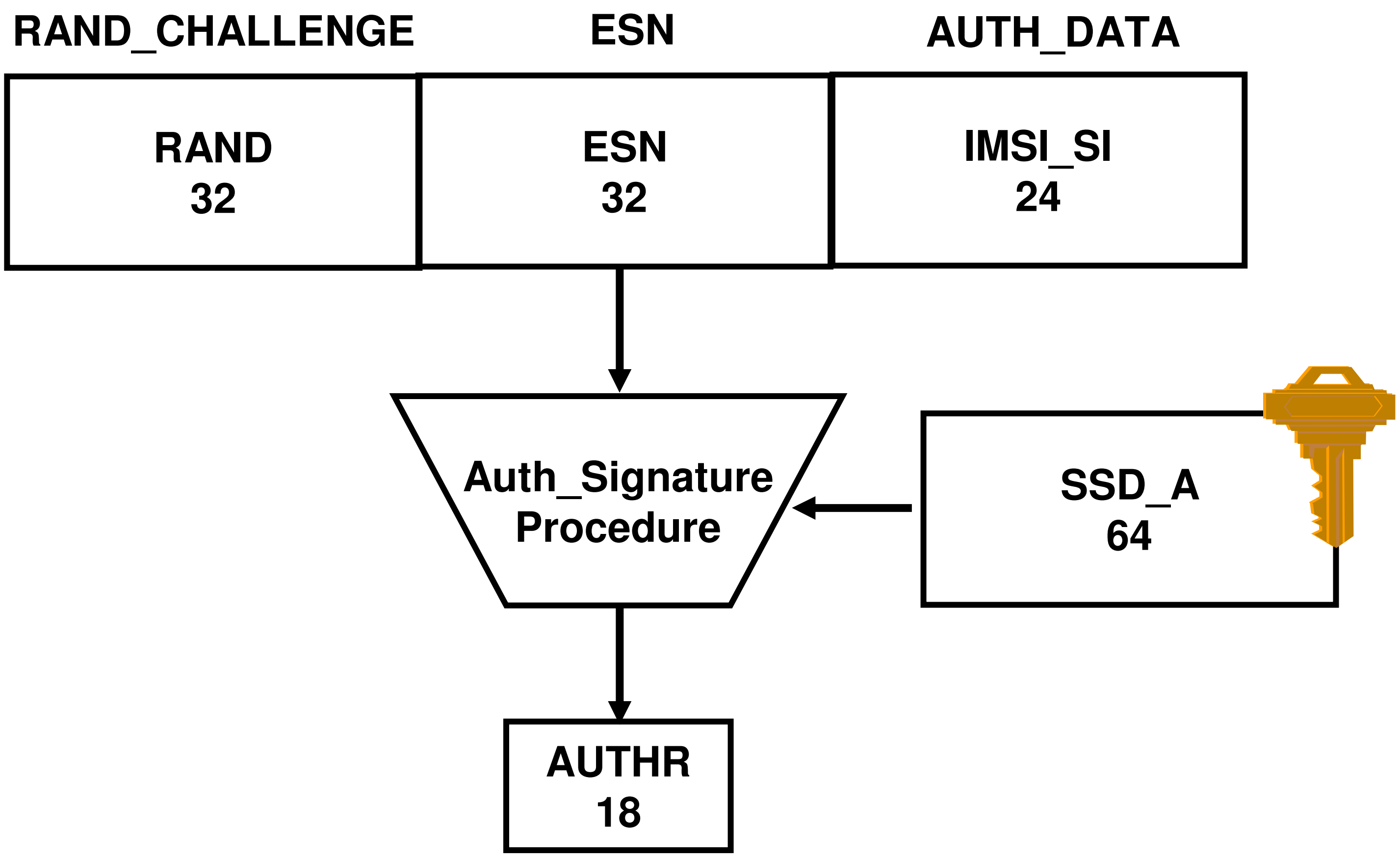
1G / 2G Cellular Theft of Service in US



Source: Cellular Telecommunications Industry Association

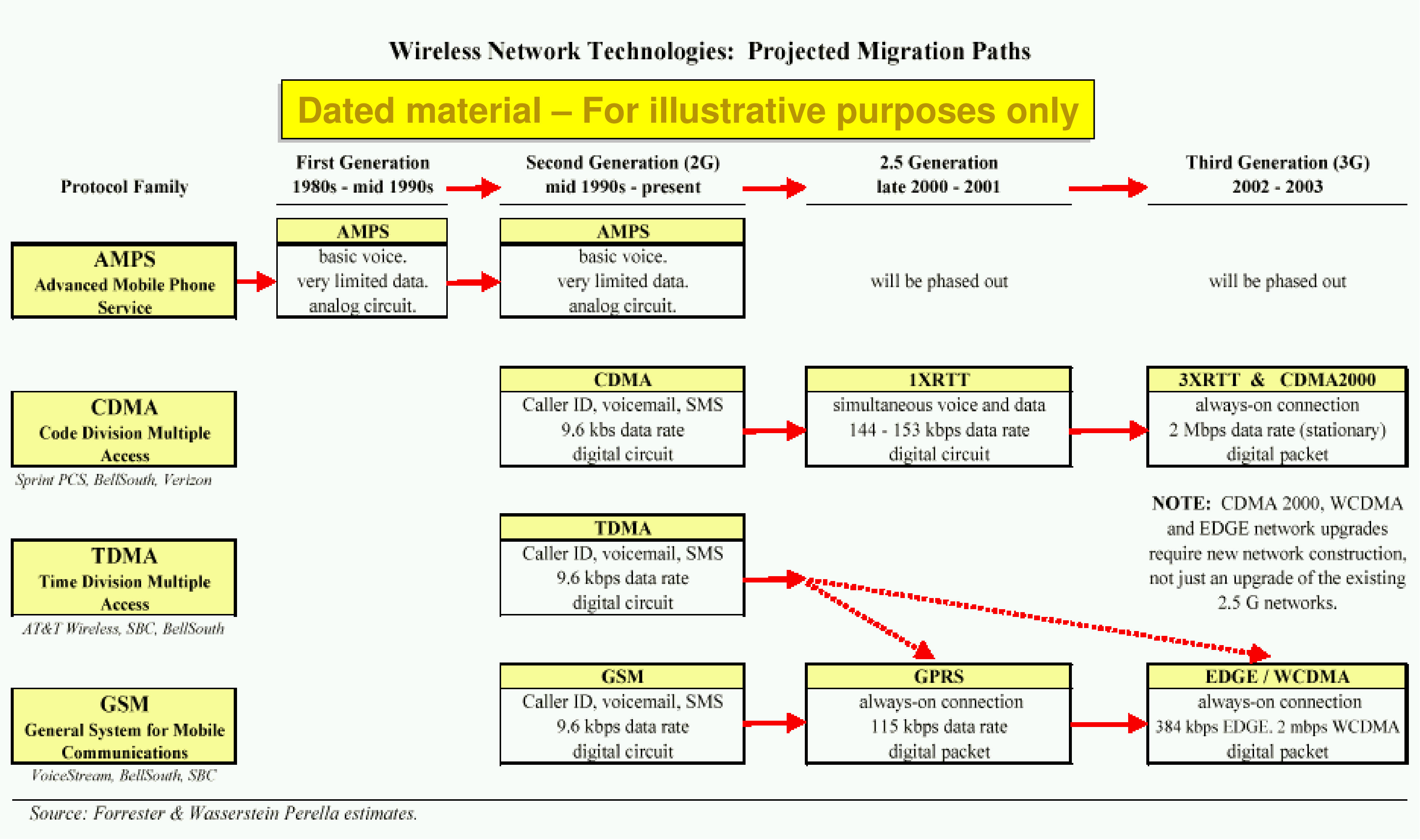
Booz | Allen | Hamilton

Authentication on Mobile Registrations



Use of a proprietary algorithm

Cellular Family Evolution



Wireless Network Technologies: Projected Migration Paths

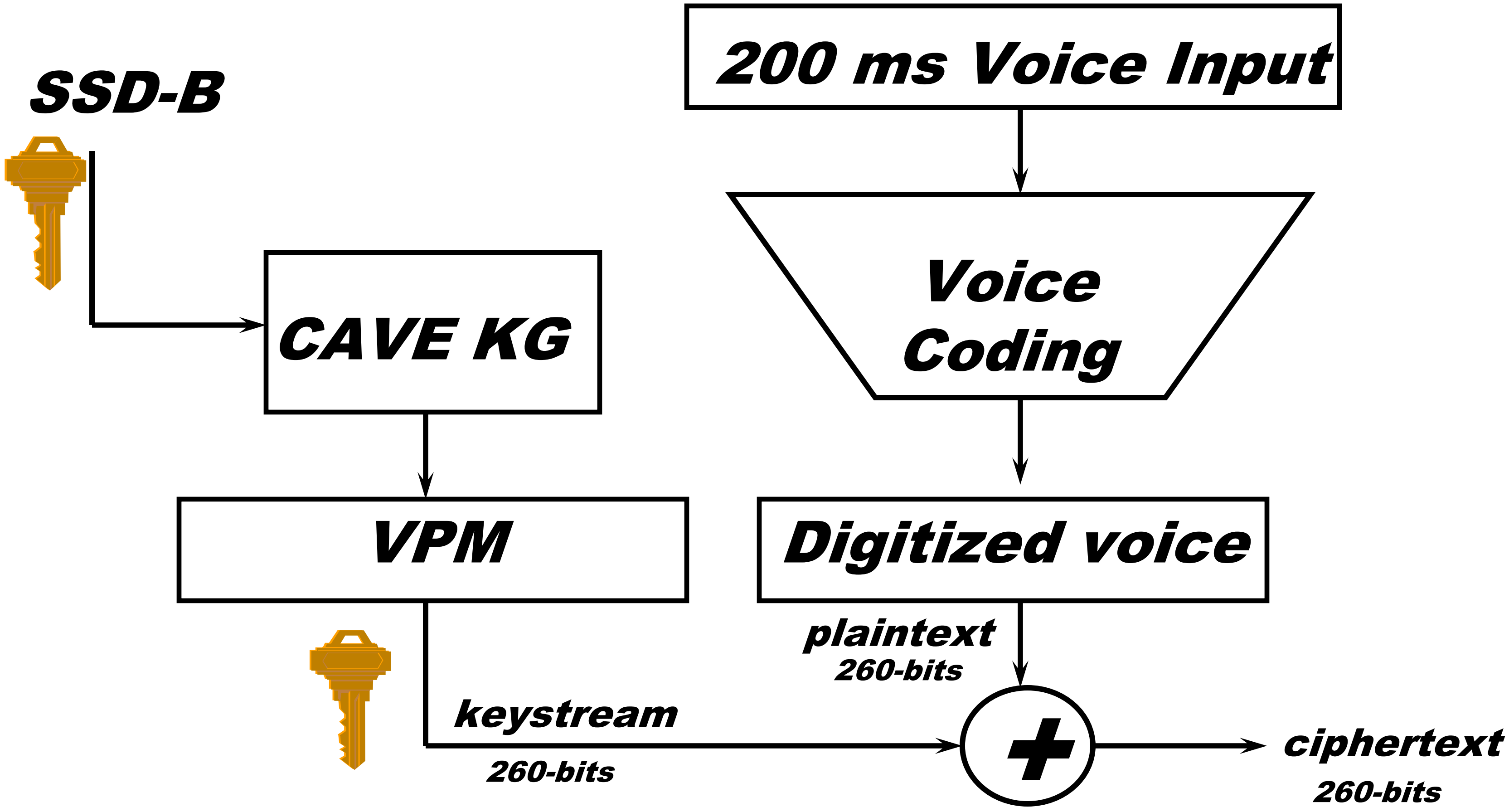
Dated material – For illustrative purposes only

Protocol Family	First Generation 1980s - mid 1990s	Second Generation (2G) mid 1990s - present	2.5 Generation late 2000 - 2001	Third Generation (3G) 2002 - 2003
AMPS **Advanced Mobile Phone Service**	**AMPS** basic voice. very limited data. analog circuit.	**AMPS** basic voice. very limited data. analog circuit.	will be phased out	will be phased out
CDMA **Code Division Multiple Access** *Sprint PCS, BellSouth, Verizon*		**CDMA** Caller ID, voicemail, SMS 9.6 kbs data rate digital circuit	**1XRTT** simultaneous voice and data 144 - 153 kbps data rate digital circuit	**3XRTT & CDMA2000** always-on connection 2 Mbps data rate (stationary) digital packet
TDMA **Time Division Multiple Access** *AT&T Wireless, SBC, BellSouth*		**TDMA** Caller ID, voicemail, SMS 9.6 kbps data rate digital circuit		
GSM **General System for Mobile Communications** *VoiceStream, BellSouth, SBC*		**GSM** Caller ID, voicemail, SMS 9.6 kbps data rate digital circuit	**GPRS** always-on connection 115 kbps data rate digital packet	**EDGE / WCDMA** always-on connection 384 kbps EDGE. 2 mbps WCDMA digital packet

NOTE: CDMA 2000, WCDMA and EDGE network upgrades require new network construction, not just an upgrade of the existing 2.5 G networks.

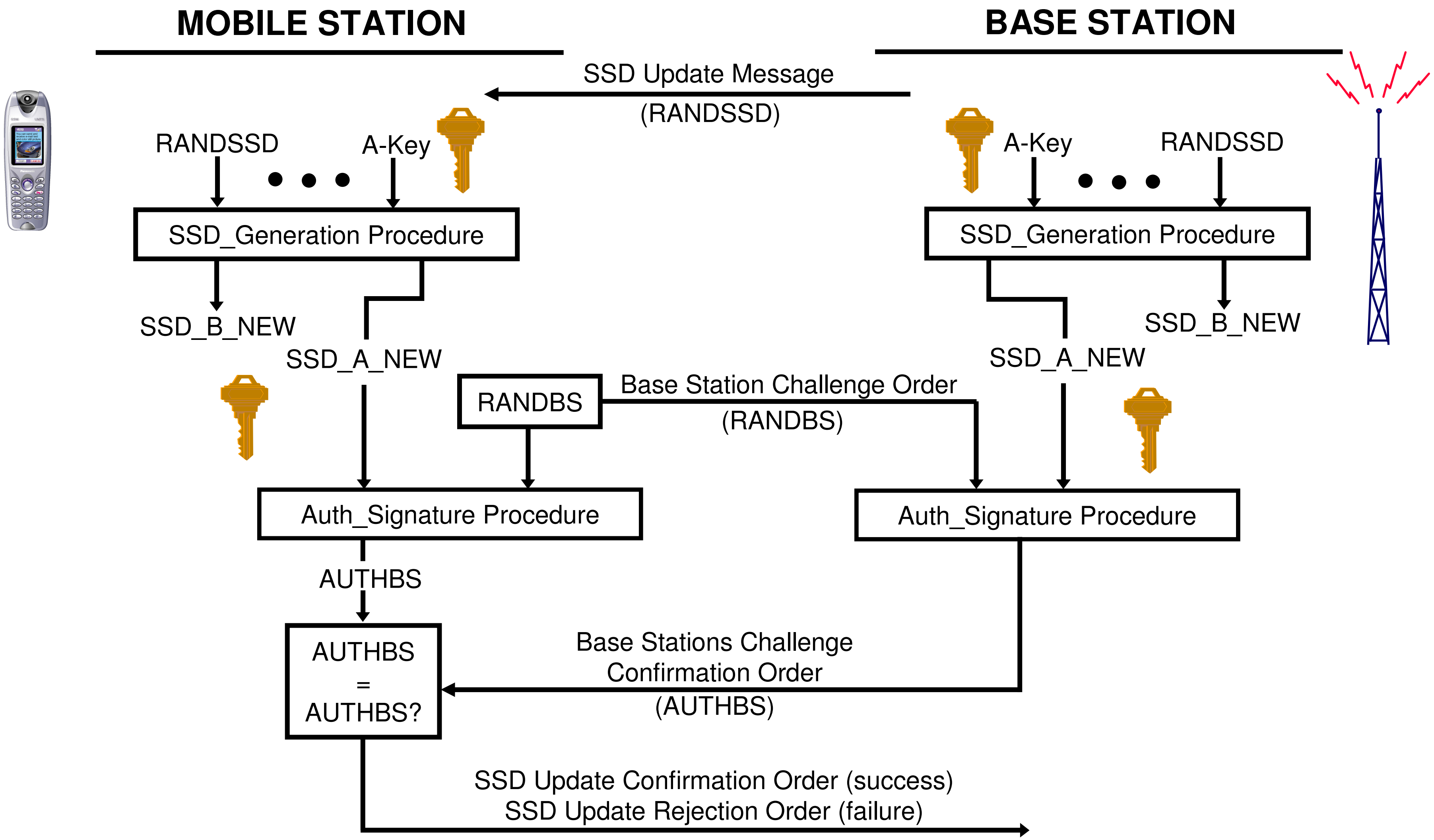
Source: Forrester & Wasserstein Perella estimates.

IS-54B / IS-136 Voice Privacy – Conceptually



Fixed key XOR makes for bad privacy

SSD Update: Key Update



MOBILE STATION

BASE STATION

SSD Update Message
(RANDSSD)

RANDSSD

A-Key

SSD_Generation Procedure

SSD_B_NEW

SSD_A_NEW

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)

A-Key

RANDSSD

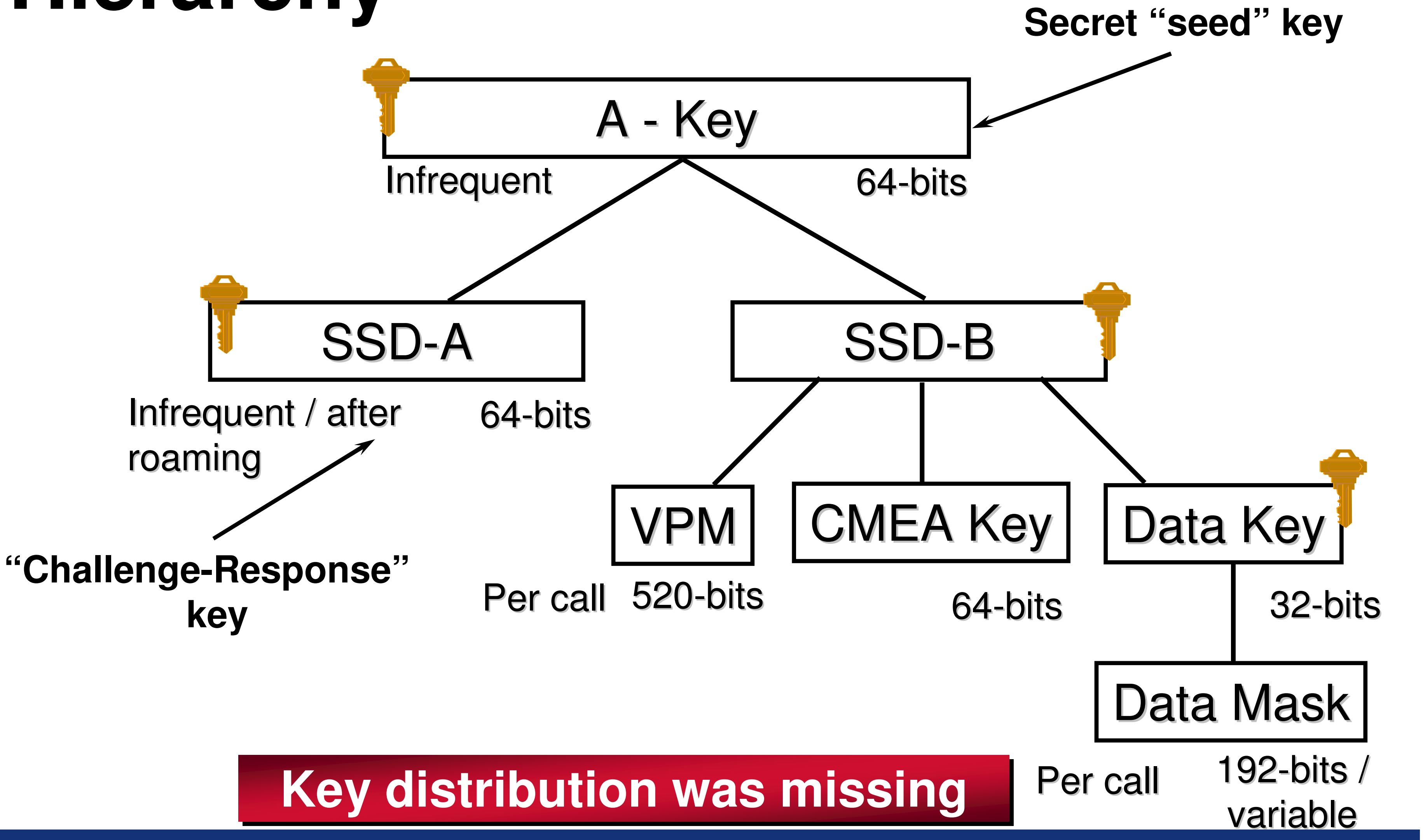
SSD_Generation Procedure

SSD_B_NEW

SSD_A_NEW

Auth_Signature Procedure

2nd Generation Cellular Key Hierarchy



Secret “seed” key

A - Key

Infrequent

64-bits

SSD-A

Infrequent / after roaming

64-bits

“Challenge-Response” key

SSD-B

VPM

Per call

520-bits

CMEA Key

64-bits

Data Key

32-bits

Data Mask

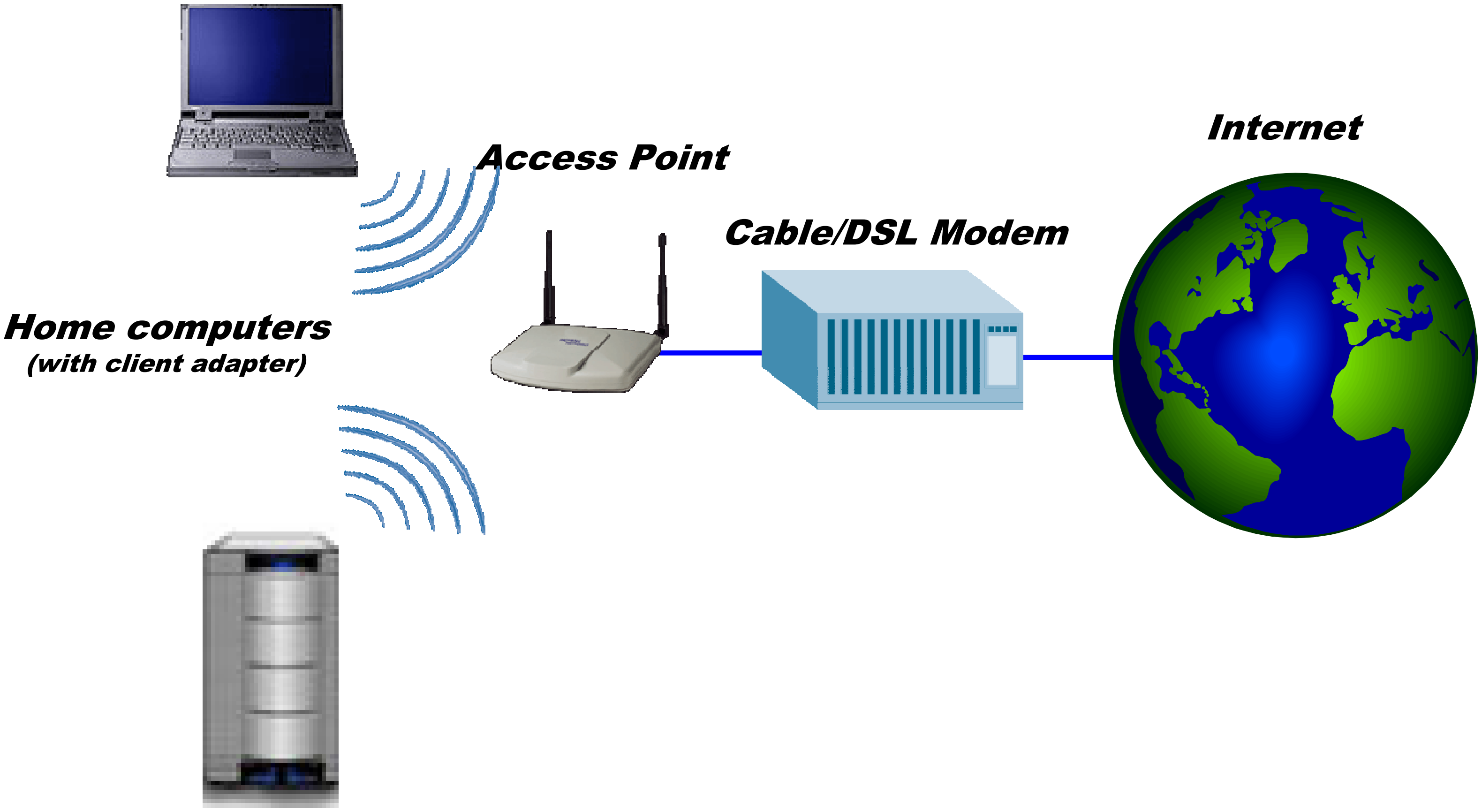
Per call

192-bits / variable

Key distribution was missing

Wi-Fi Security

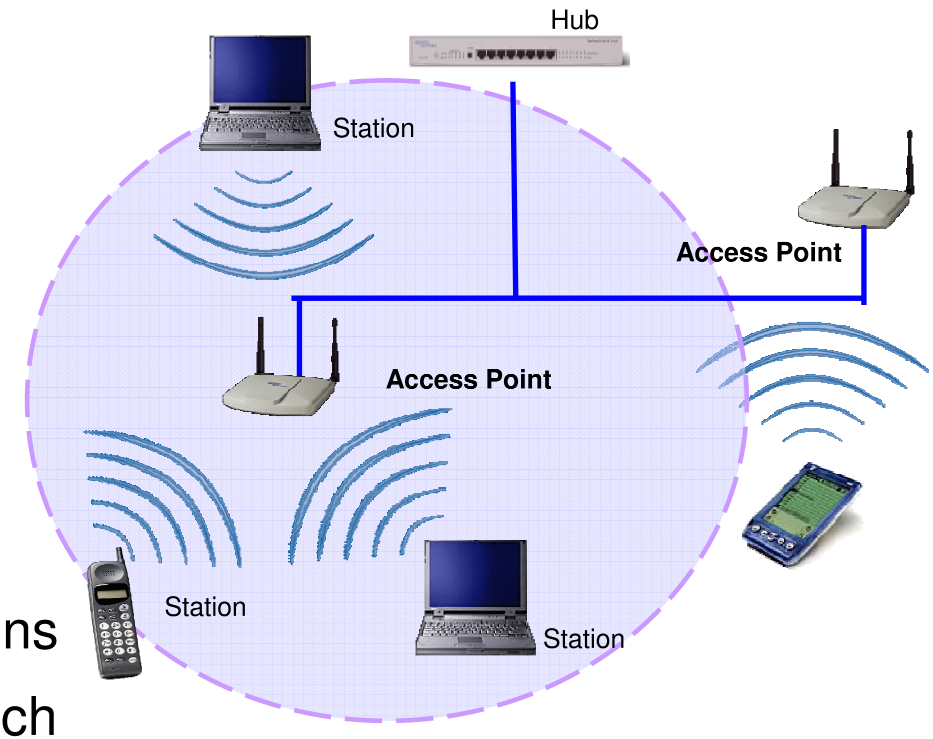
Typical Residential Wi-Fi Deployment



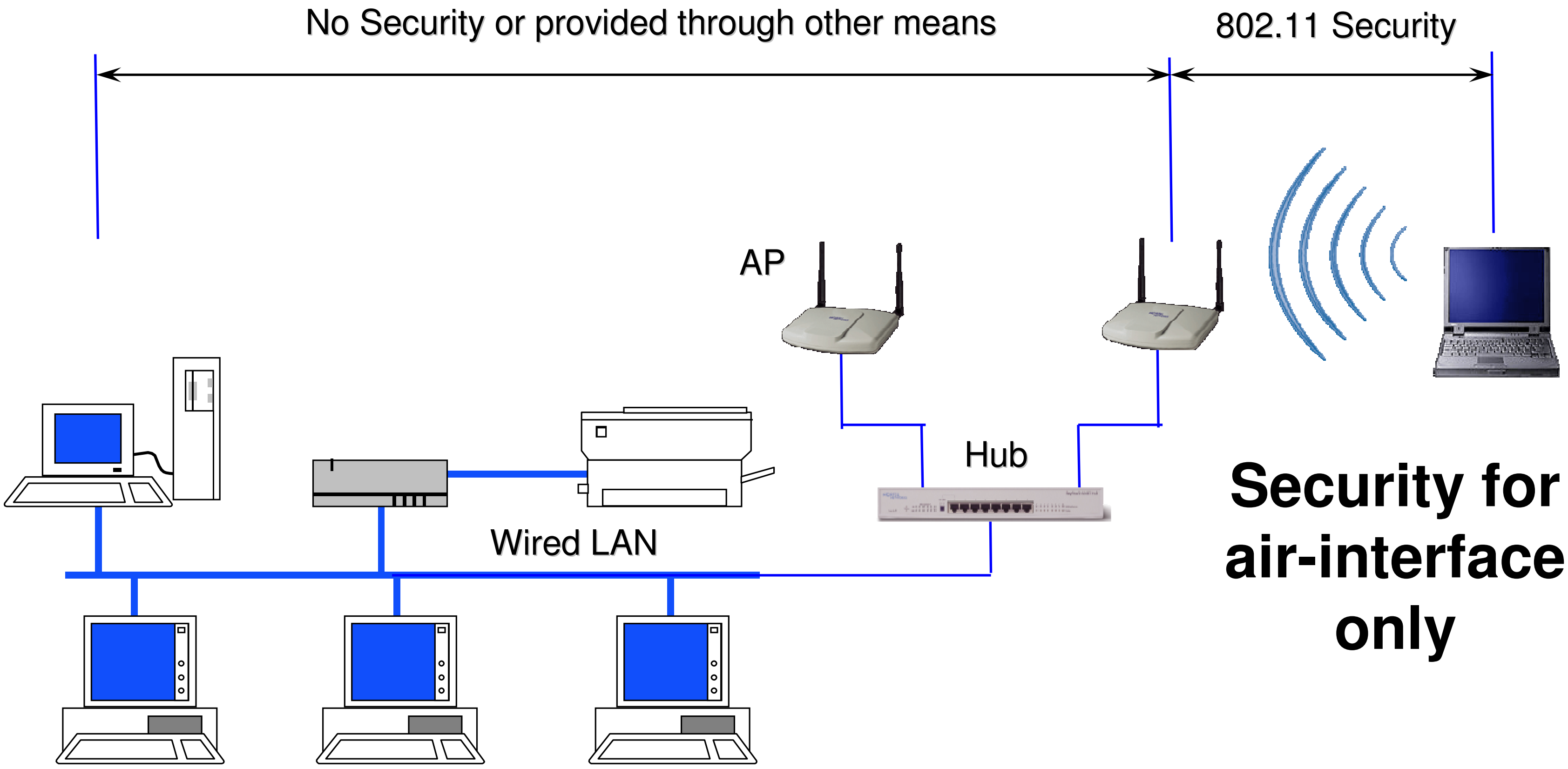
Explosive growth of Wi-Fi

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



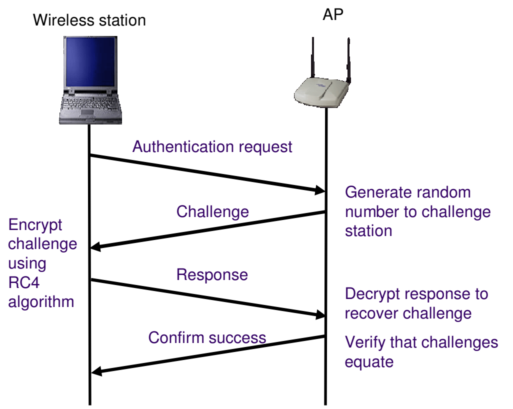
Wi-Fi (IEEE802.11 WLAN) Security

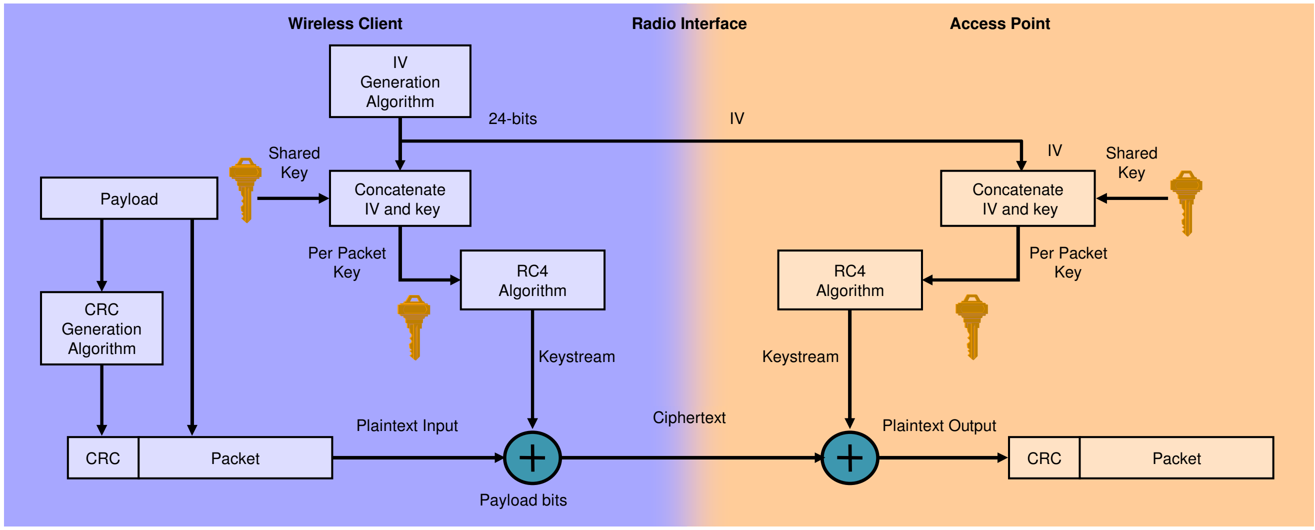


Security for air-interface only

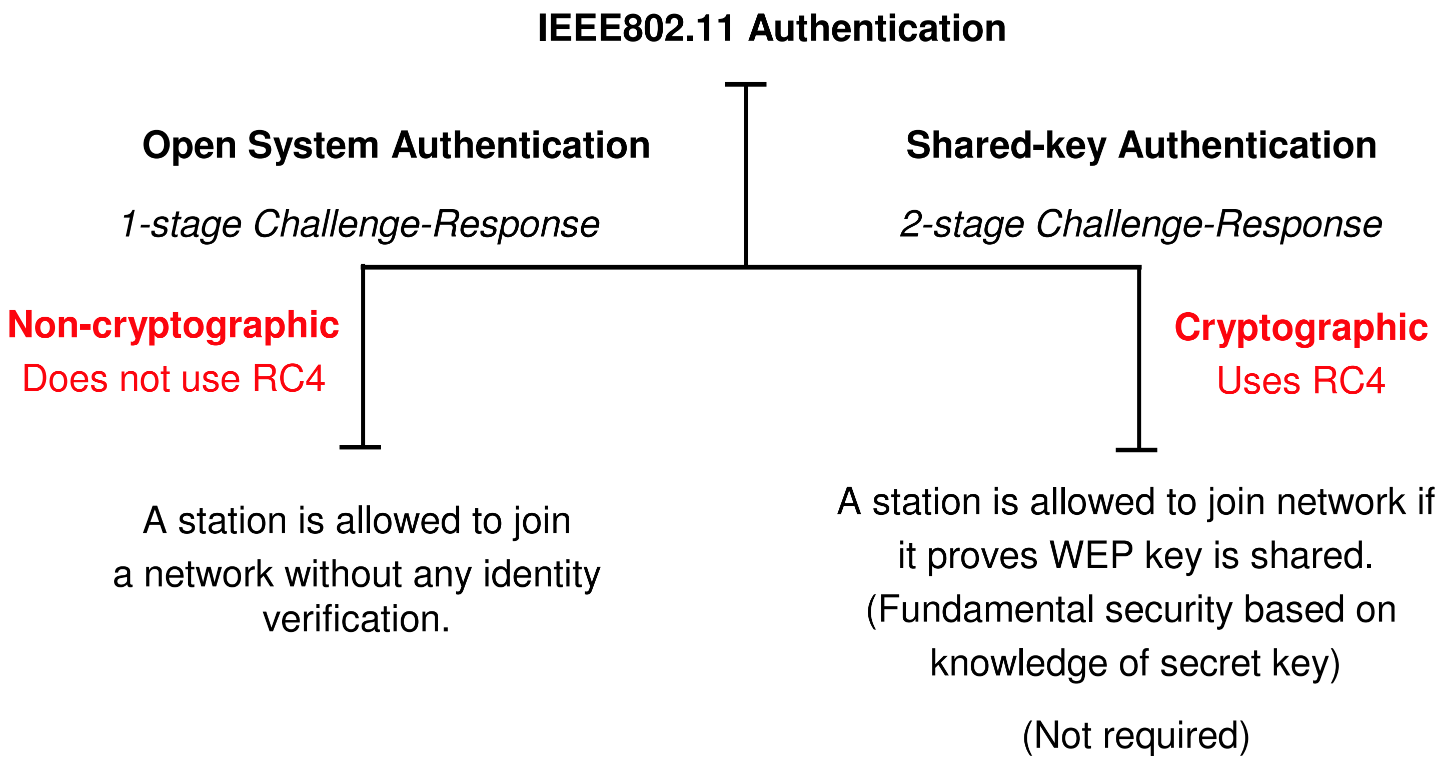
Wired Equivalent Privacy (WEP) / Entity Authentication – Flawed

- 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


Wireless station
AP
Authentication request
Generate random number to challenge station
Challenge
Encrypt challenge using RC4 algorithm
Response
Decrypt response to recover challenge
Confirm success
Verify that challenges equate



IEEE802.11 Entity Authentication is Not Adequate



IEEE802.11 Authentication

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

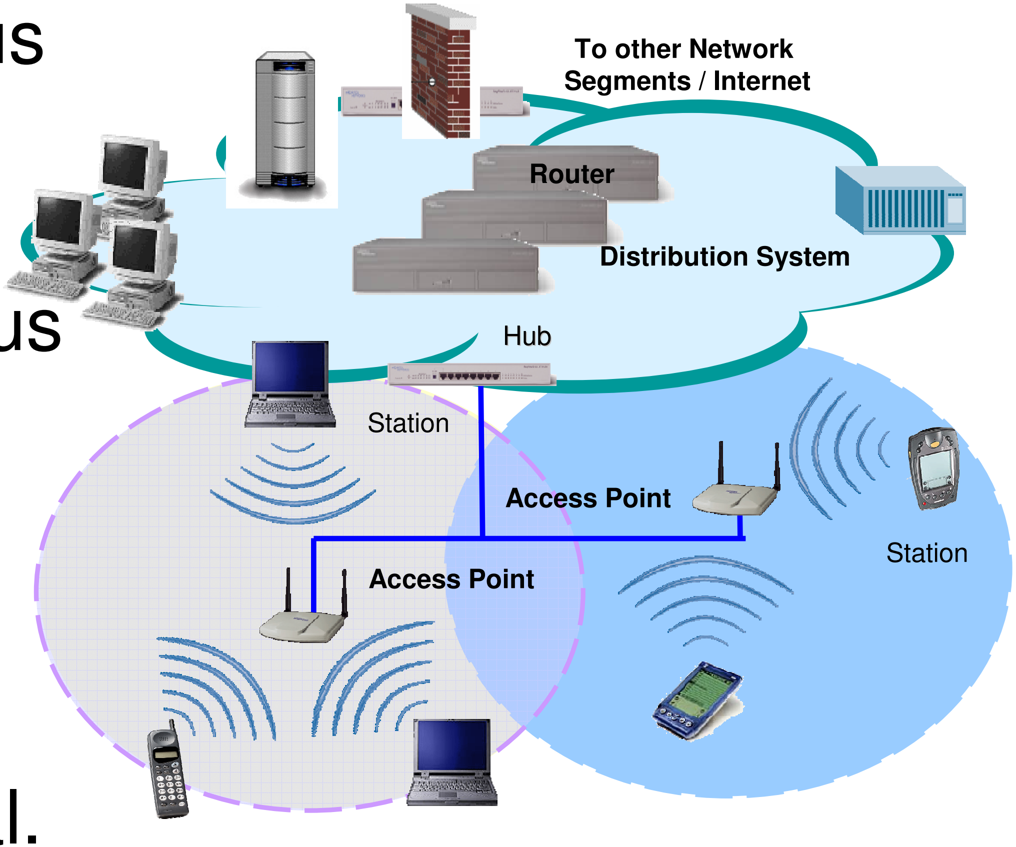
Uses RC4

A station is allowed to join network if it proves WEP key is shared. (Fundamental security based on knowledge of secret key)

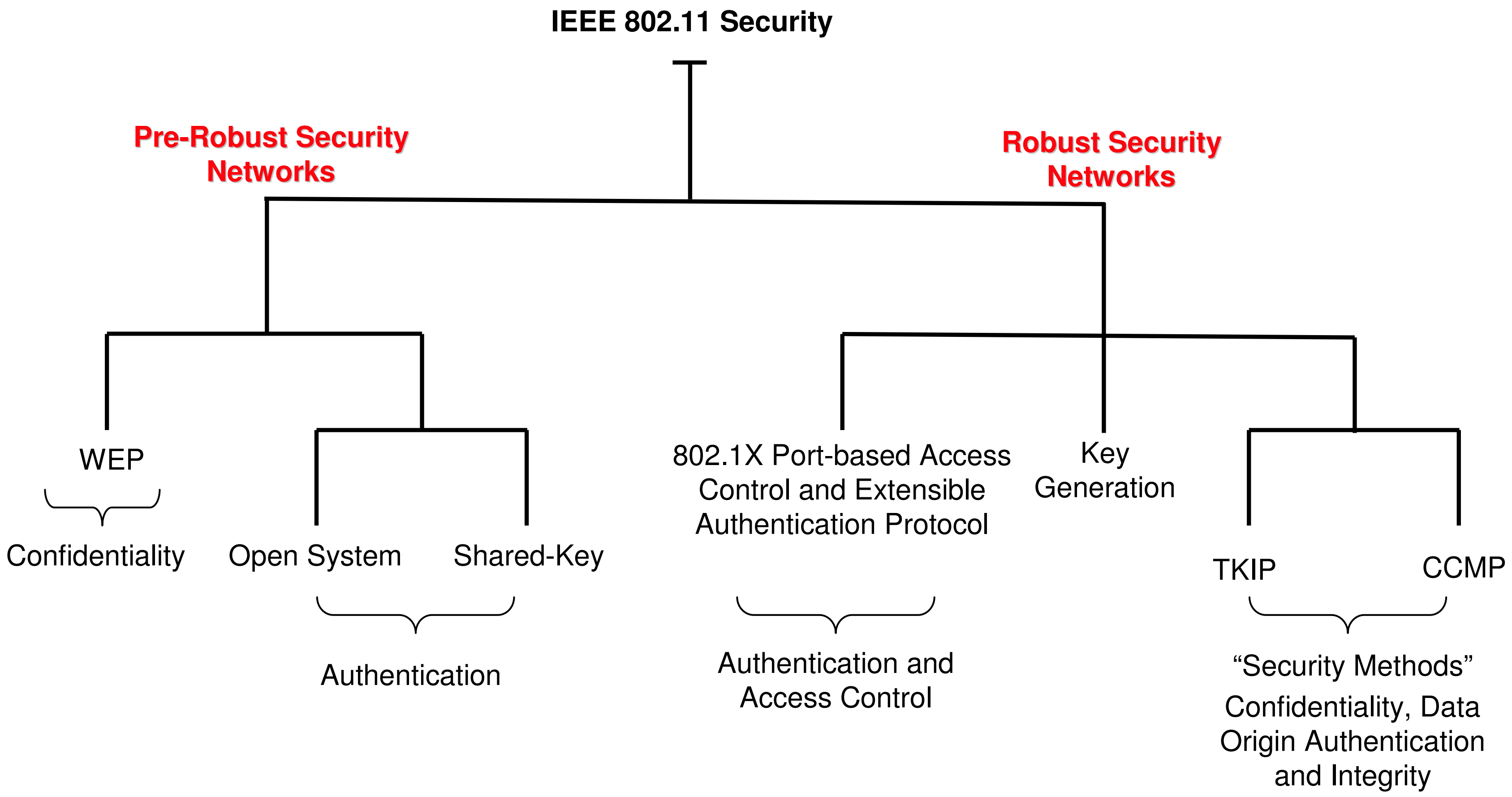
(Not required)

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.



IEEE802.11i Amendment – Enter Robust Security Networks



IEEE 802.11 Security

Pre-Robust Security Networks

Robust Security Networks

WEP

Confidentiality

Open System

Shared-Key

Authentication

802.1X Port-based Access Control and Extensible Authentication Protocol

Key Generation

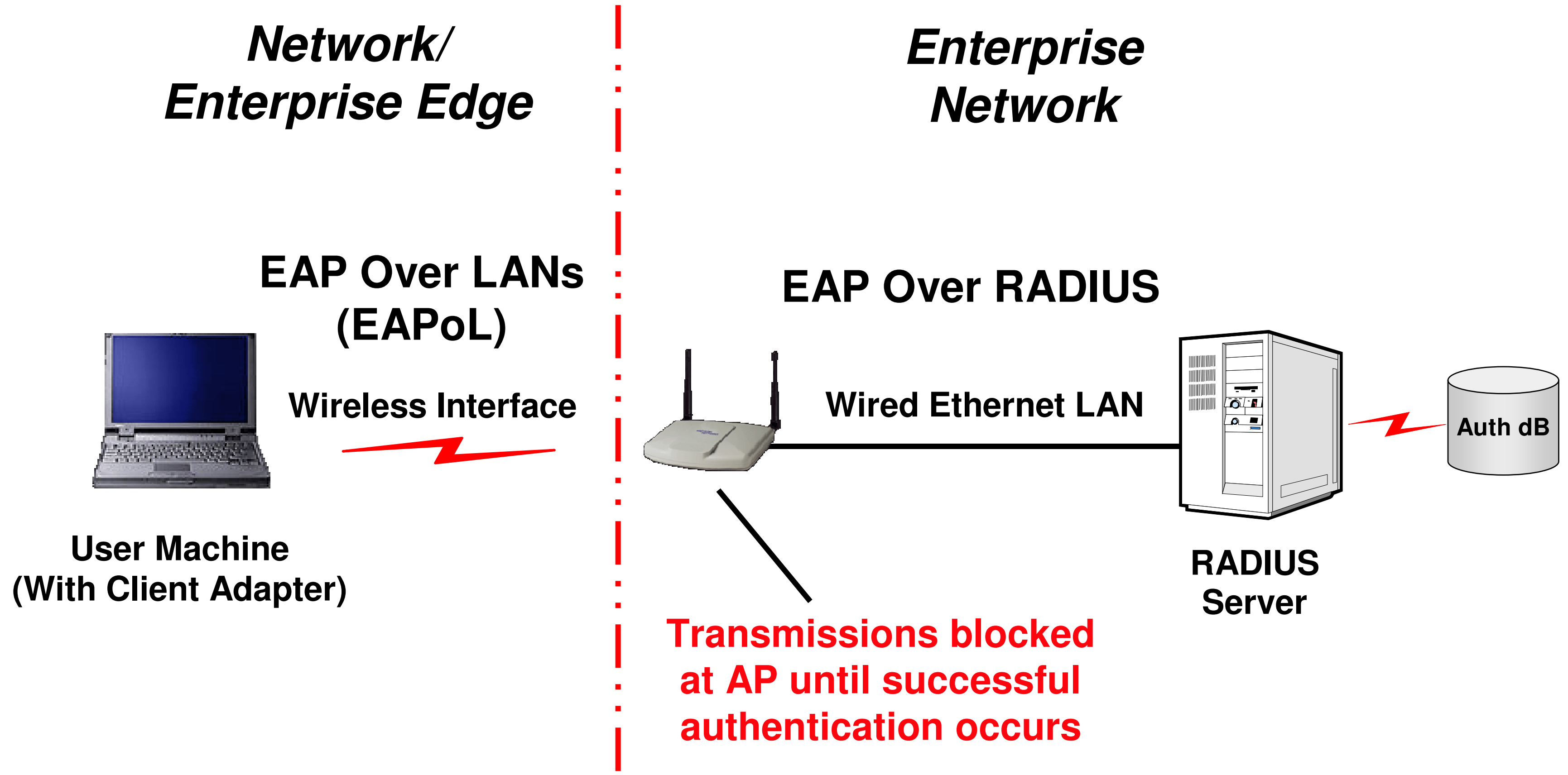
Authentication and Access Control

TKIP

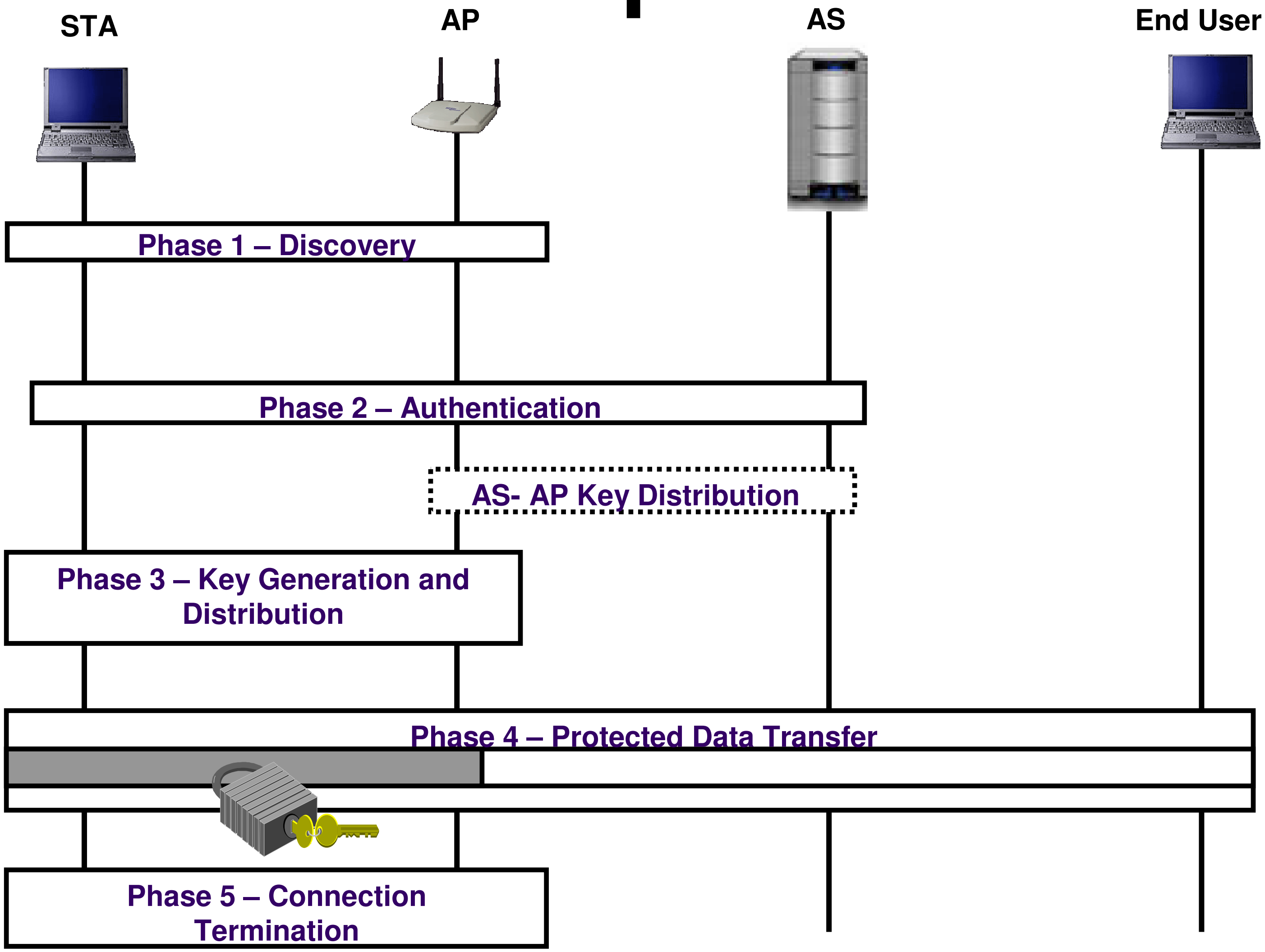
CCMP

"Security Methods" Confidentiality, Data Origin Authentication and Integrity

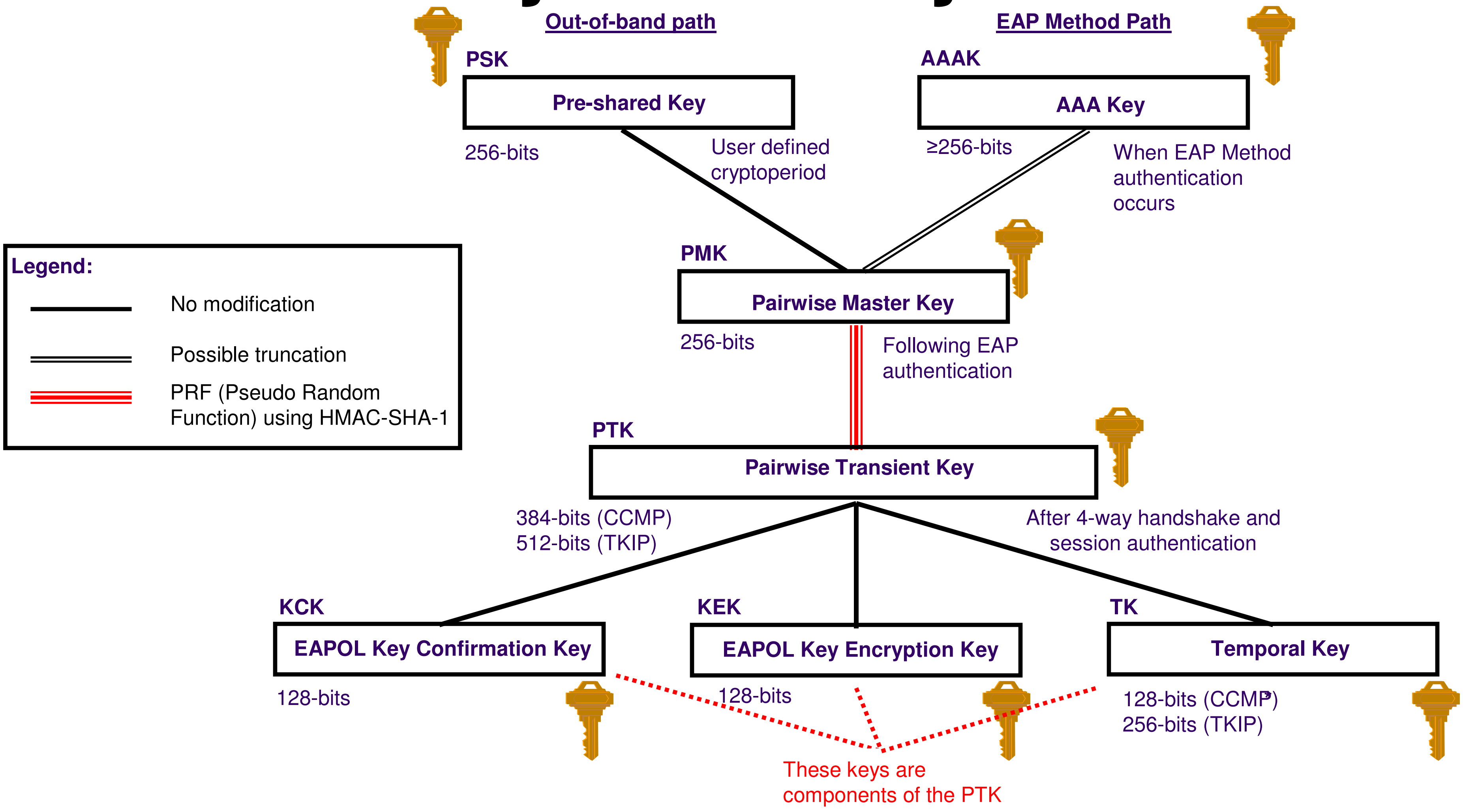
IEEE802.1X Port-Based Access Control


Network/ Enterprise Edge
Enterprise Network
EAP Over LANs (EAPoL)
EAP Over RADIUS
Wireless Interface
Wired Ethernet LAN
Auth dB
User Machine (With Client Adapter)
RADIUS Server
Transmissions blocked at AP until successful authentication occurs

RSN Phases of Operation


STA
AP
AS
End User
Phase 1 – Discovery
Phase 2 – Authentication
AS- AP Key Distribution
Phase 3 – Key Generation and Distribution
Phase 4 – Protected Data Transfer
Phase 5 – Connection Termination

Pairwise Key Hierarchy



Out-of-band path

EAP Method Path

PSK

Pre-shared Key

256-bits

User defined cryptoperiod

AAAK

AAA Key

≥256-bits

When EAP Method authentication occurs

Legend:

No modification

Possible truncation

PRF (Pseudo Random Function) using HMAC-SHA-1

PMK

Pairwise Master Key

256-bits

Following EAP authentication

PTK

Pairwise Transient Key

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

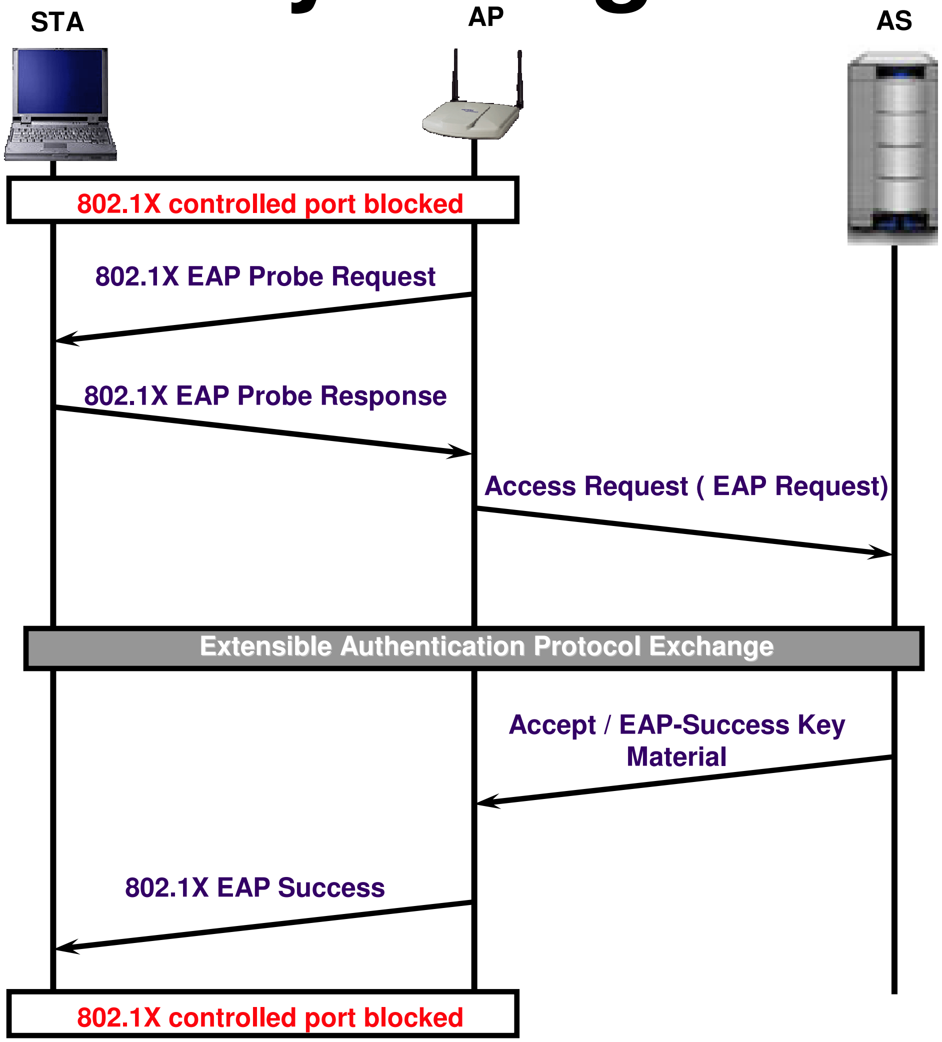
TK

Temporal Key

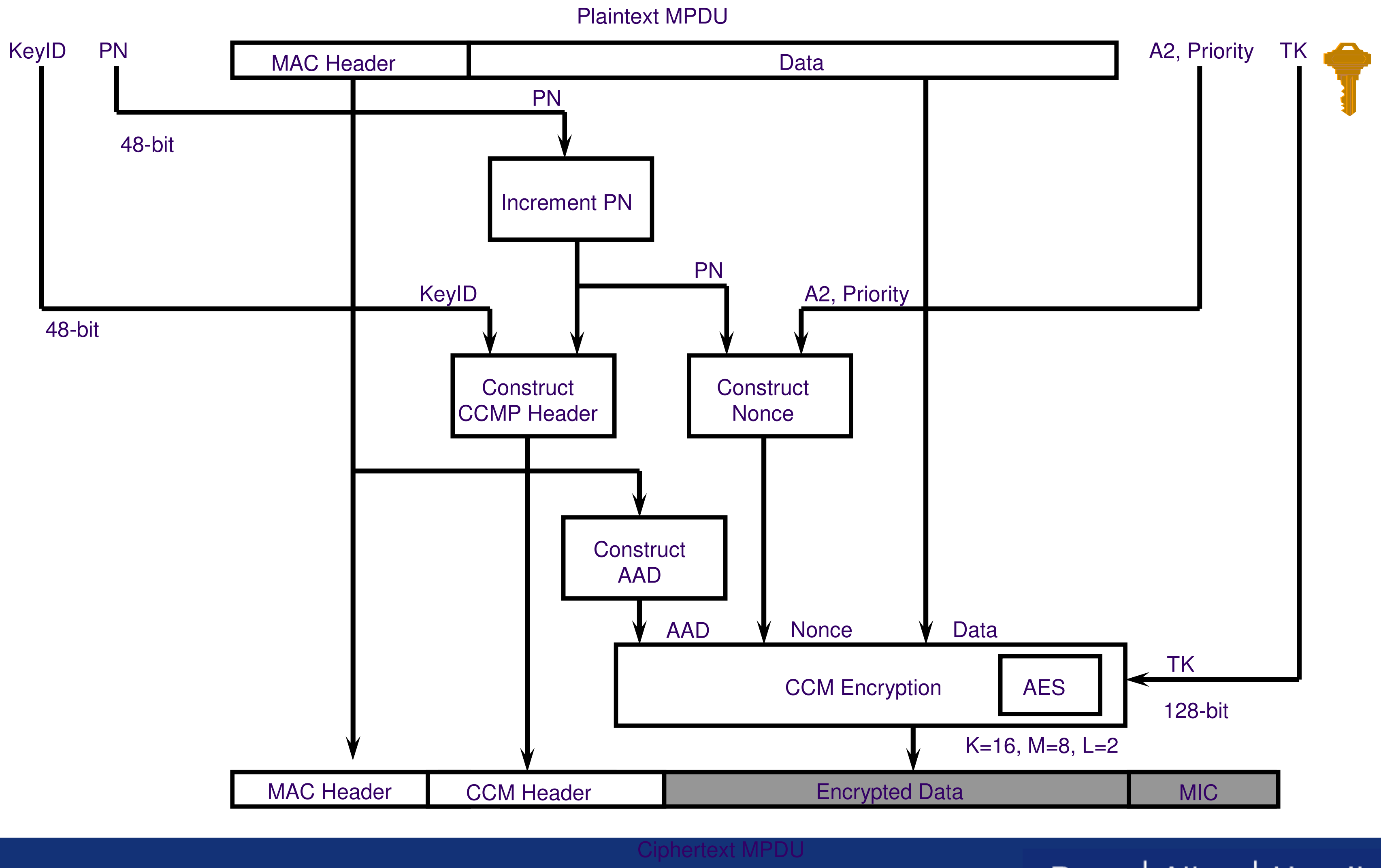
128-bits (CCMP)
256-bits (TKIP)

These keys are components of the PTK

IEEE802.1X Flows – Management Frame Security being developed


STA
AP
AS
802.1X controlled port blocked
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)



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)

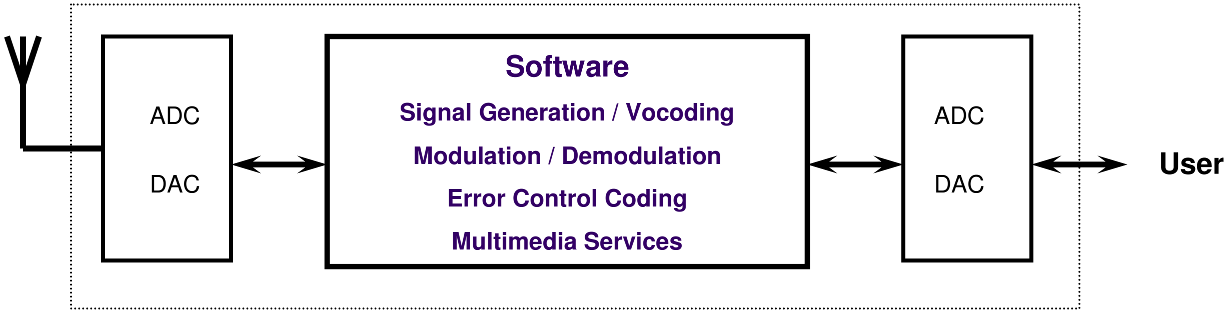
Some Lessons-learned for Wireless – 4

- *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

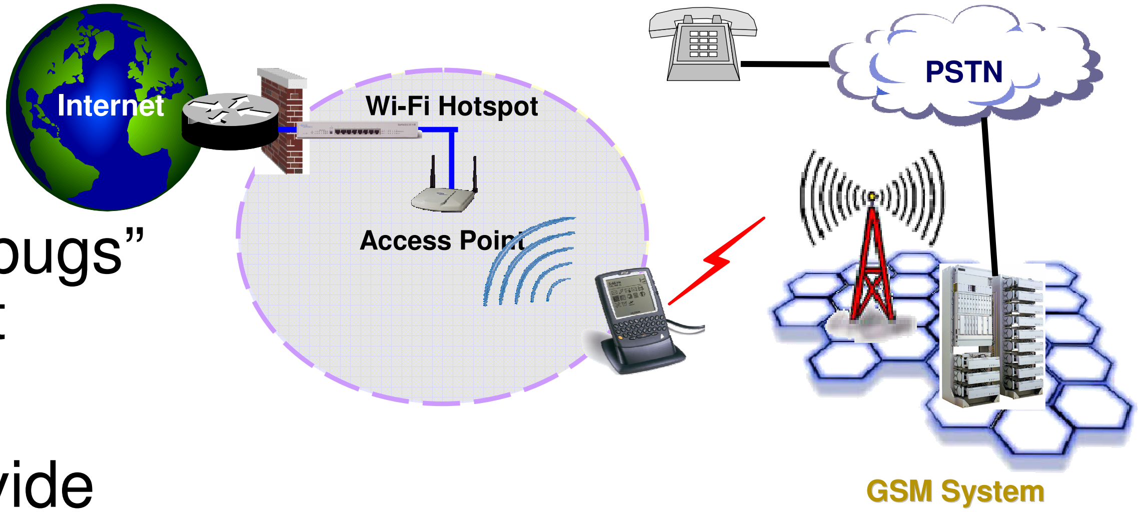
"… to build flexible radio systems, multiservice, multistandard, reconfigurable and reprogrammable by software."



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.

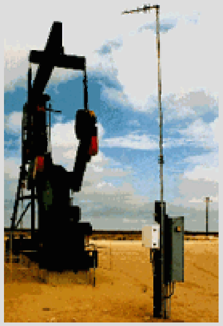
Benefits of SDR

- 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



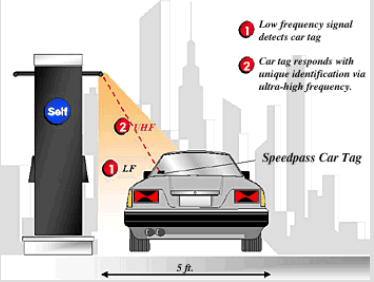
SDR as Mobility will serve critical needs…

Supervisory Control and Data Acquisition (SCADA)



Remote telemetry for utilities and energy systems

Point of Sale / Asset Tracking


1 Low frequency signal detects car tag
2 Car tag responds with unique identification via ultra-high frequency.
Self
2 UHF
1 LF
Speedpass Car Tag
5 ft.

Mobile commerce, inventory, border enforcement

Remote Sensing

Urban search and rescue, geology, environmental science, and civil engineering

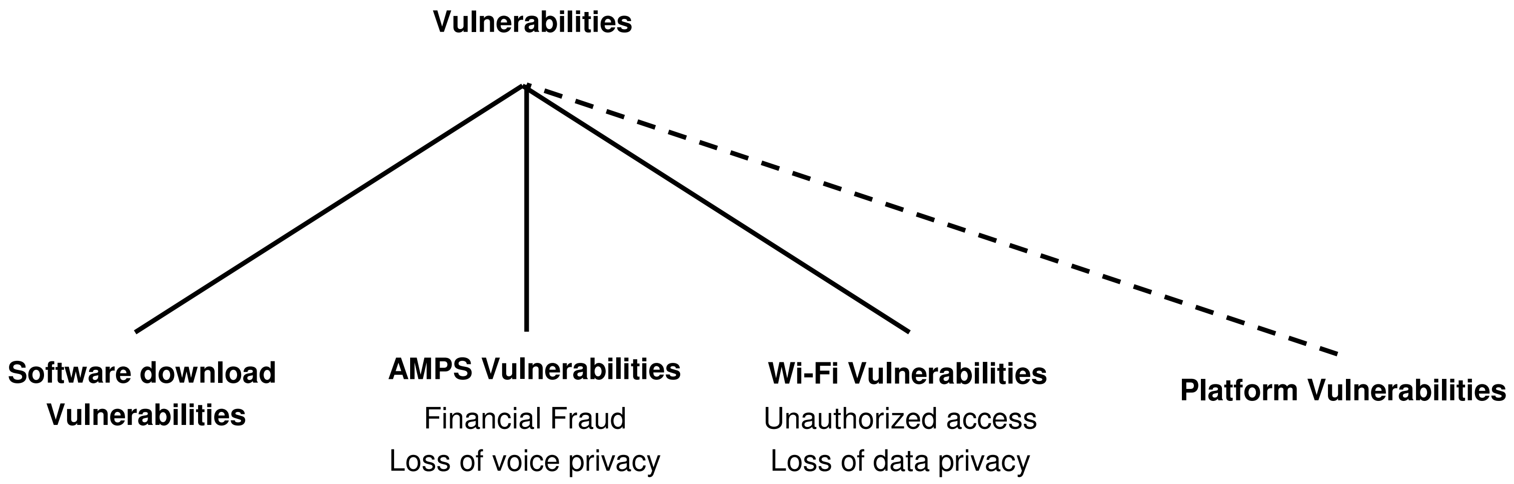
Informatics / Geolocation

Navigation, location-aware services, surveying, aviation, direction-finding

Booz | Allen | Hamilton

Public Safety will be a beneficiary

Vulnerabilities in SDR: Related to Embedded Interfaces



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

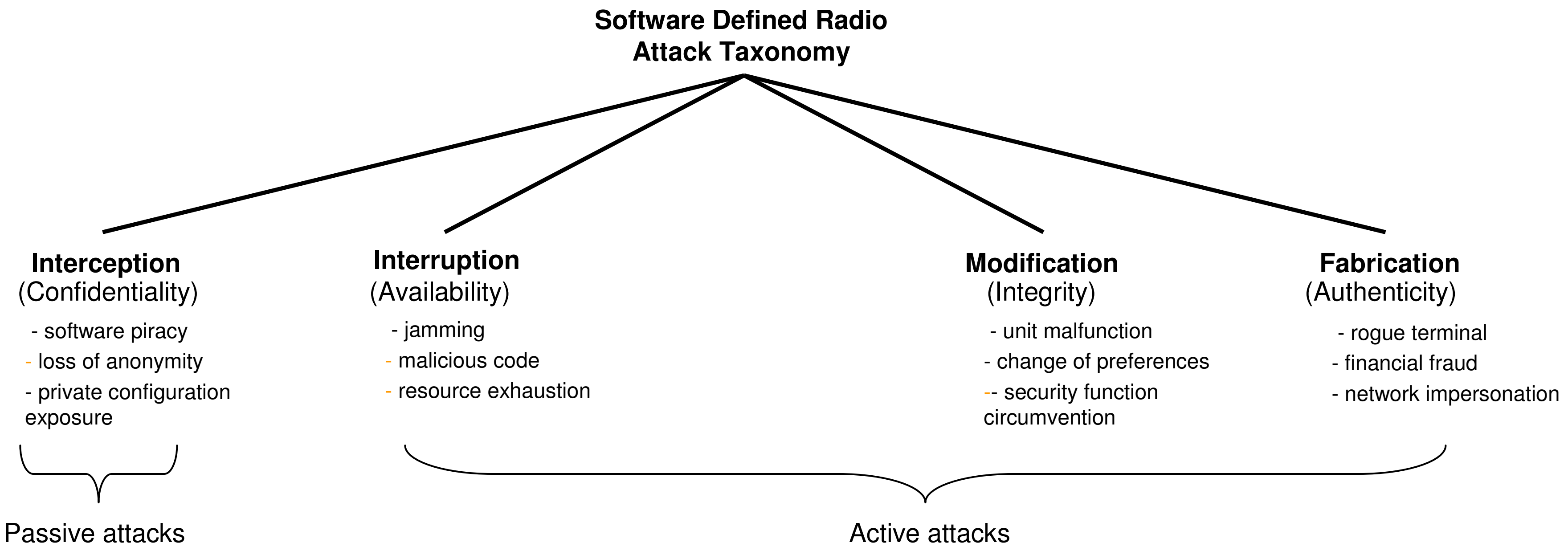
Wireless Technology Alternatives

- 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



Software Defined Radio Attack Taxonomy

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

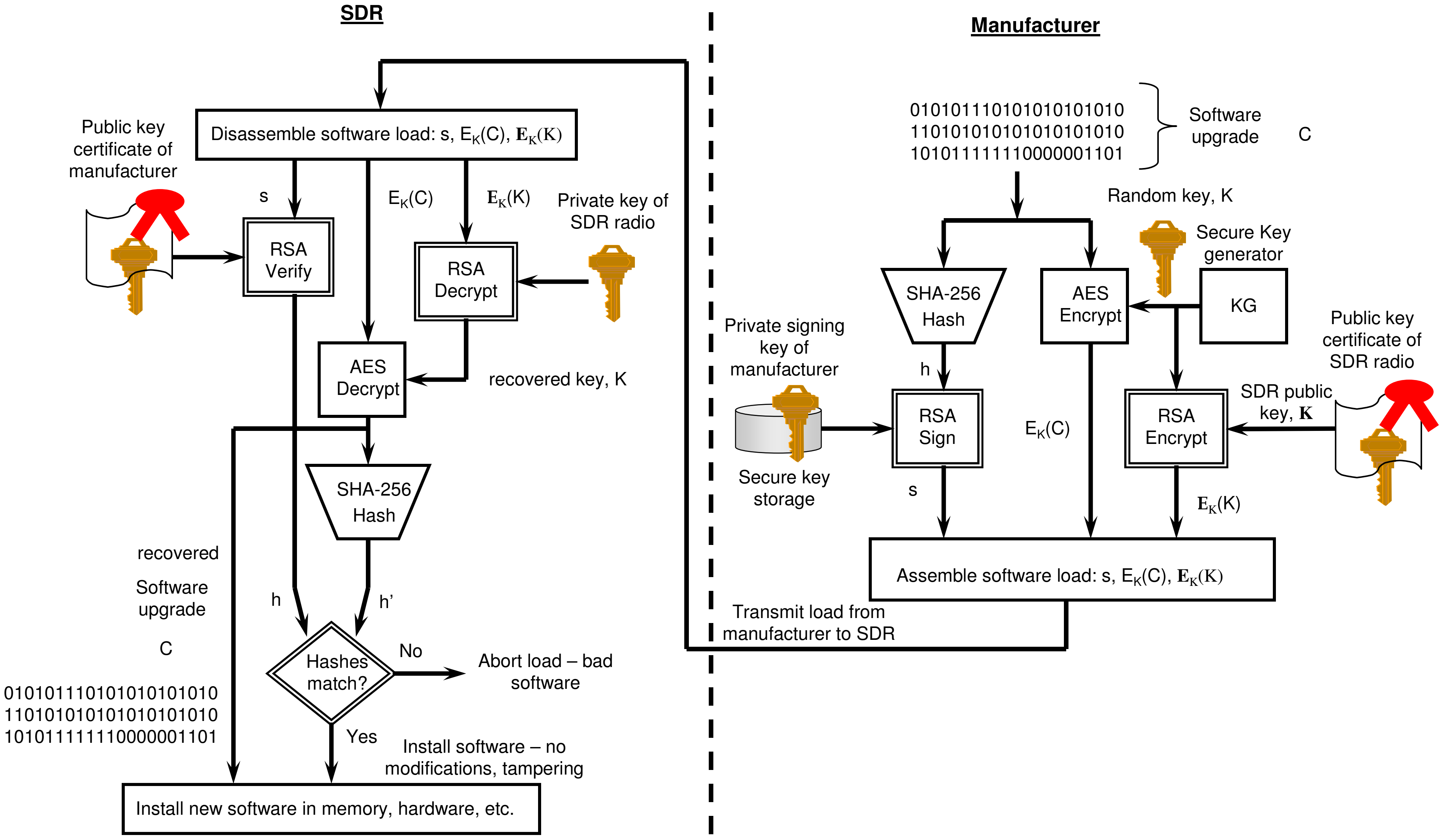
Passive attacks

Active attacks

What are the required services for the SDR / CR environment?

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

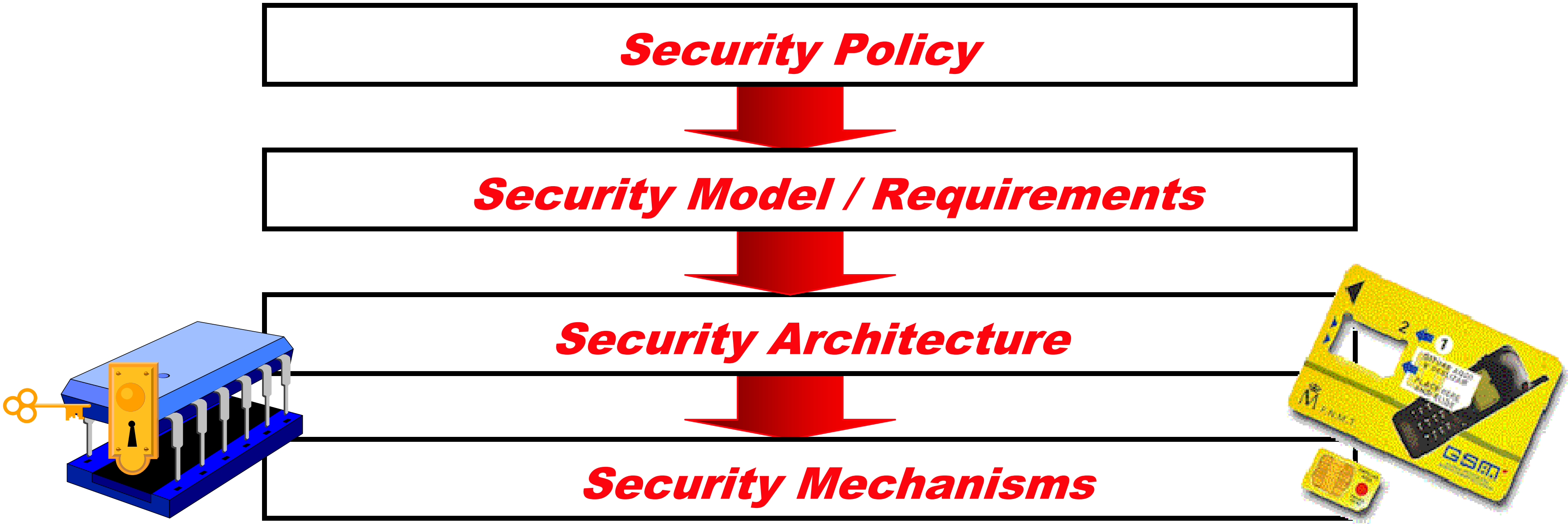
PKC Software Download


SDR
Manufacturer
Disassemble software load: s, $E_K(C)$, $\mathbf{E}_K(K)$
Public key certificate of manufacturer
s
$E_K(C)$
$E_K(K)$
Private key of SDR radio
RSA Verify
RSA Decrypt
AES Decrypt
recovered key, K
SHA-256 Hash
recovered Software upgrade
C
01010111010101010101010
11010101010101010101010
10101111111110000001101
h
h'
Hashes match?
No
Abort load – bad software
Yes
Install software – no modifications, tampering
Install new software in memory, hardware, etc.
01010111010101010101010
11010101010101010101010
10101111111110000001101
Software upgrade
C
Random key, K
Secure Key generator
SHA-256 Hash
AES Encrypt
KG
Private signing key of manufacturer
h
RSA Sign
$E_K(C)$
RSA Encrypt
Public key certificate of SDR radio
SDR public key, $\mathbf{K}$
Secure key storage
s
$E_K(K)$
Assemble software load: s, $E_K(C)$, $\mathbf{E}_K(K)$
Transmit load from manufacturer to SDR

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

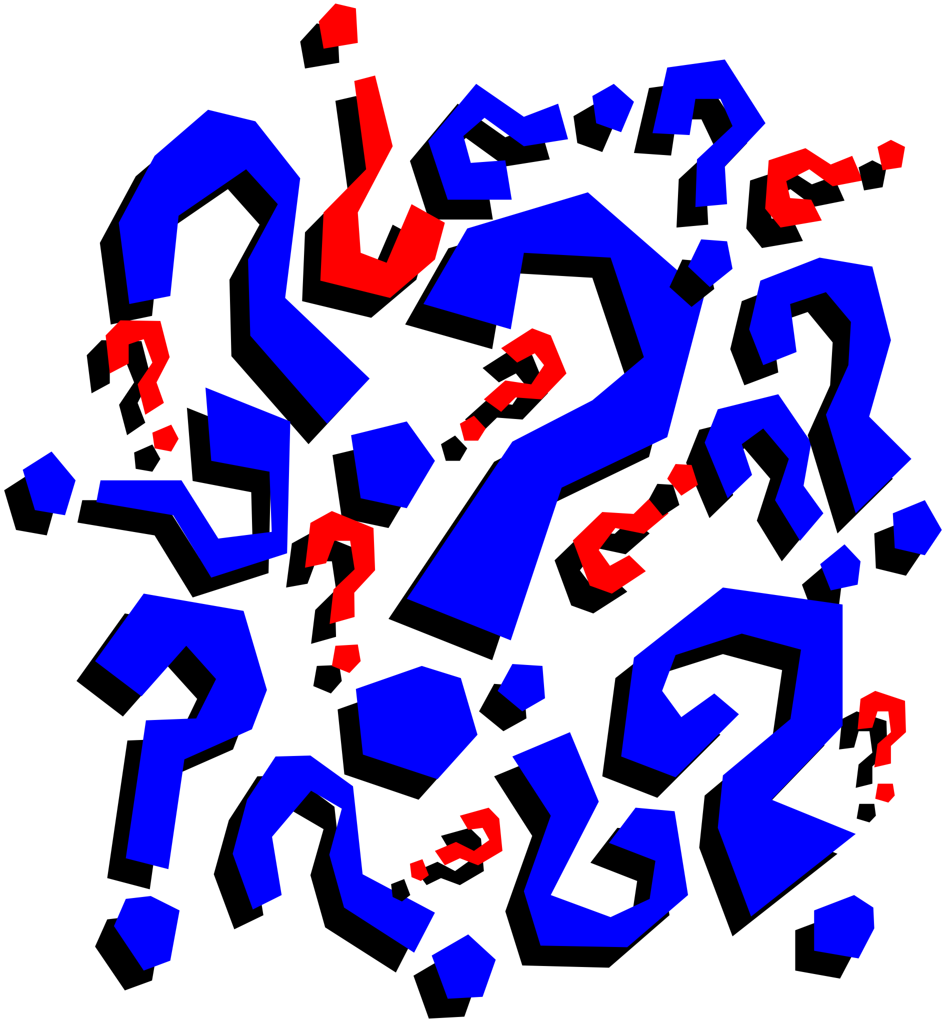
Security Mechanisms

Passwords	Firewalls	Encryption	Audit Trails
Tokens/Smart Cards	Filters/Guards	Digital Signatures	MLS/Secure OSs
Biometrics	Intrusion Detection	Key Man'ment/PKI	Virus Detection

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.

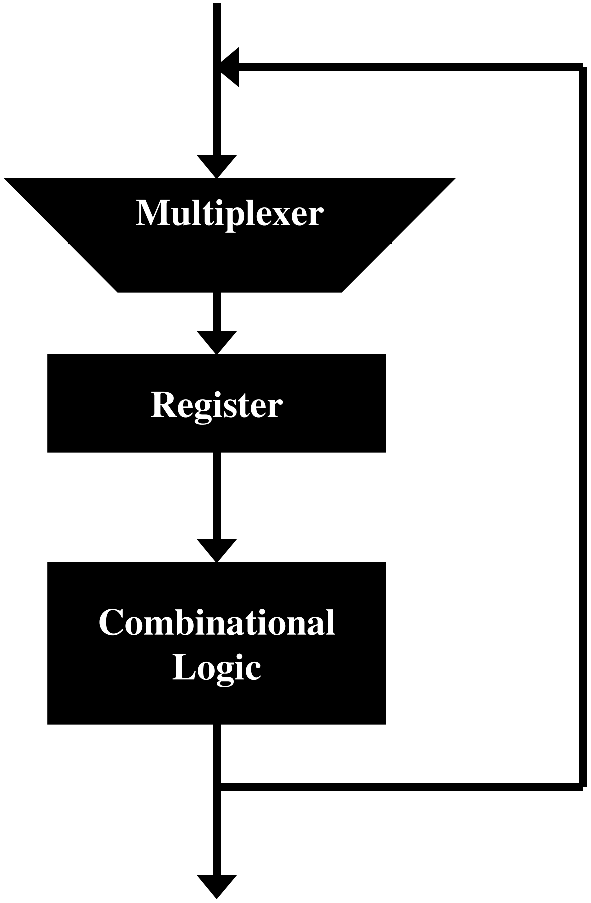
http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

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

	WiFi	1st Generation Cellular
Time Period	2002	1992
State of industry	Exploding	Exploding
State of security	Poor	Poor
Buzzwords	War-driving and war-chalking	Counterfeiting / cloning
Tools of choice	Netstumbler and Airsnort	Curtis ESN reader and Timson software
Detectability	Difficult.	Difficult a priori. Easy after the customer complains
Triage solution	Patched WEP, VPNs	PINs, clone detectors, RF fingerprinting
"Hot" solution to the problem	Switch-based security devices	RF fingerprinting

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

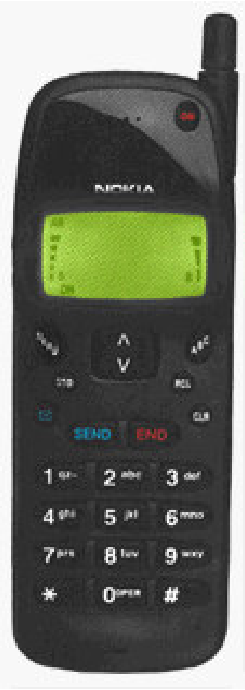
- *Confidentiality* – ensures that only authorized individuals and parties can access information in a computer system or communications network. This access includes copying, displaying, printing, and other forms of disclosure.
- *Integrity* – ensures that only authorized individuals and parties can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