Wireless Security

K. Raghunandan and Geoff Smith

Stevens Institute of Technology

September 21, 2013

This material was presented at the IEEE North Jersey Advanced Communications Symposium - Hoboken, NJ - Sep. 21, 2013

Topics

- Cyber Security – hacking community
- Familiarity with IP networks
- What is the security process in IP standards and WLAN
- Aren't all networks IP today?
- Why use cellular – what is its strength?
- Is WiFi same as cellular – differences
- NIST guidelines on network security
- Conclusion

Cyber Security

- Hacking community – their objectives
- Collaboration and Cooperation between them and Homeland security
- What does it take for a hacker to know how cellular security operates?
- Choice:
  - IP network and its security limitations
  - Cellular networks, its strengths and limitations
  - WiFi network, strengths and limitations

This material was presented at the IEEE North Jersey Advanced Communications Symposium - Hoboken, NJ - Sep. 21, 2013

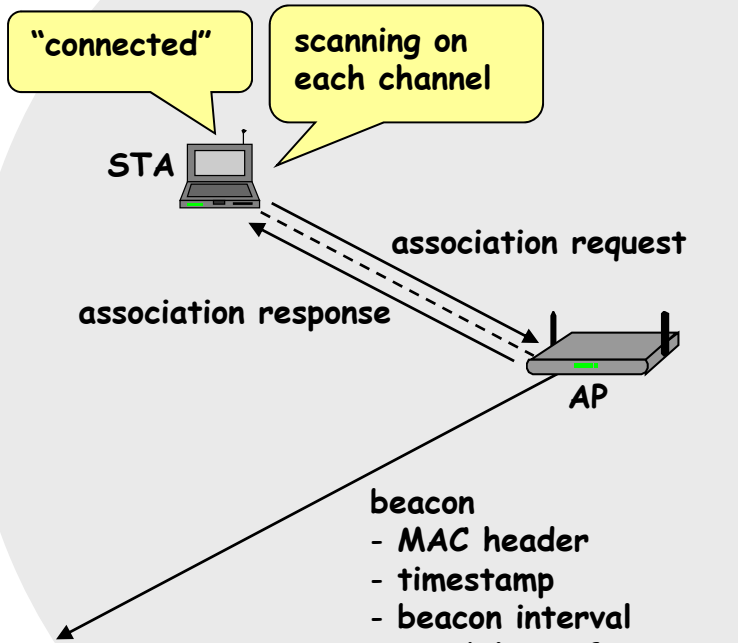
802.11 Standards Defined

802.11 protocol	Release Date	Freq. (GHz)	Bandwidth (MHz)	Data rate per stream Mbit/s	Allowable MIMO streams	Modulation
b	Sep-99	2.4	20	1, 2, 5.5, 11	1	DSSS
a	Sep-99	5	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM
g	Jun-03	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	1	OFDM, DSSS
n	Oct-09	2.4/5	20	7.2, 14.4, 21.7, 28.9, 43.3, 57.8, 65, 72.2	4	OFDM
			40	15, 30, 45, 60, 90, 120, 135, 150		
Ac (DRAFT)	Nov. 2013	5	20	up to 87.6	8	OFDM
			40	up to 200		
			80	up to 433.3		
			160	up to 866.7		

How to increase Capacity

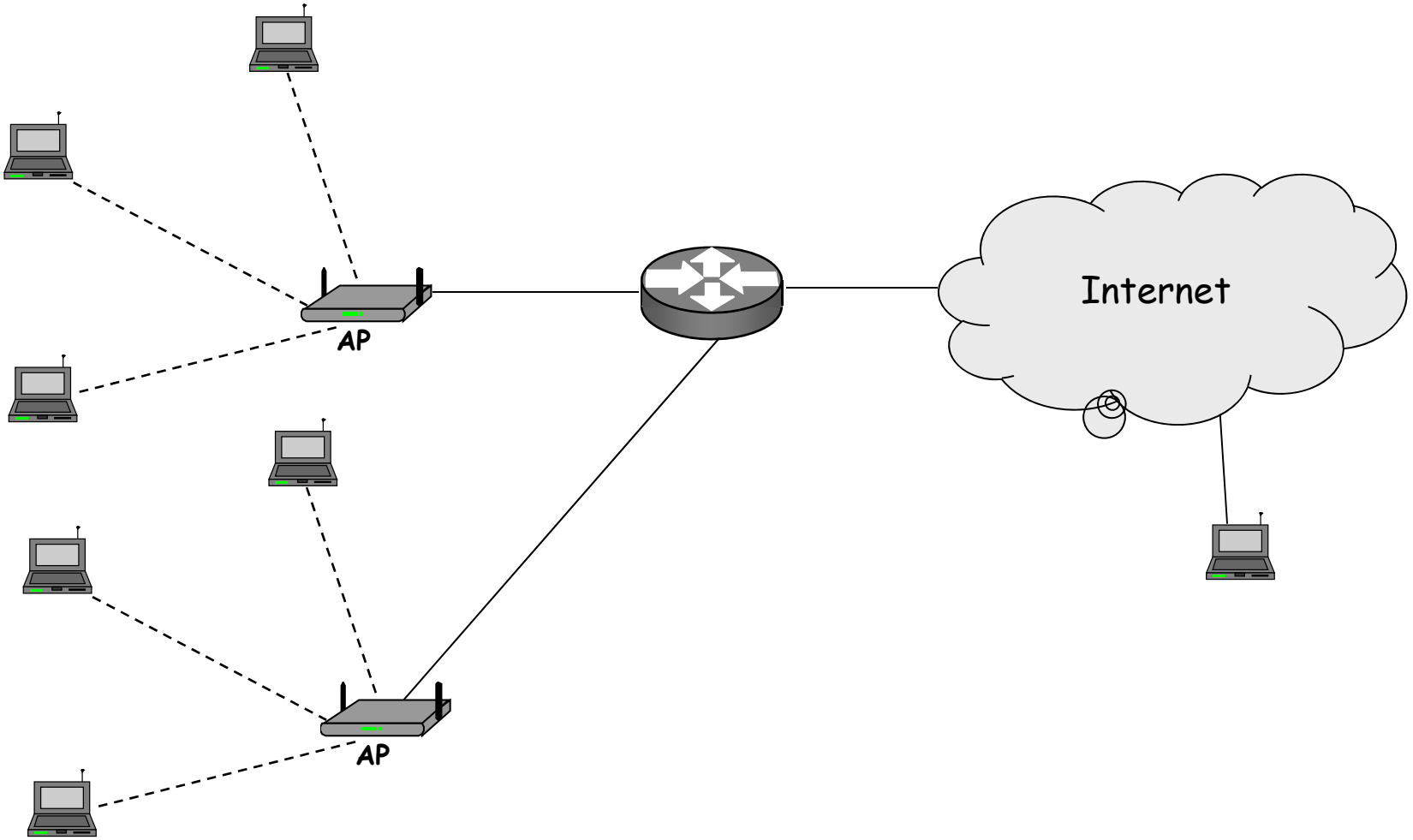
- Channel Size, linear correlation with throughput and is directly correlated to frequency
- MIMO Technology, diminishing returns outdoors in terms of capacity after 2x2
- QAM Modulation, the higher the modulation the lower the TX power
- Coding Gain, to a much smaller extent

Introduction to WiFi

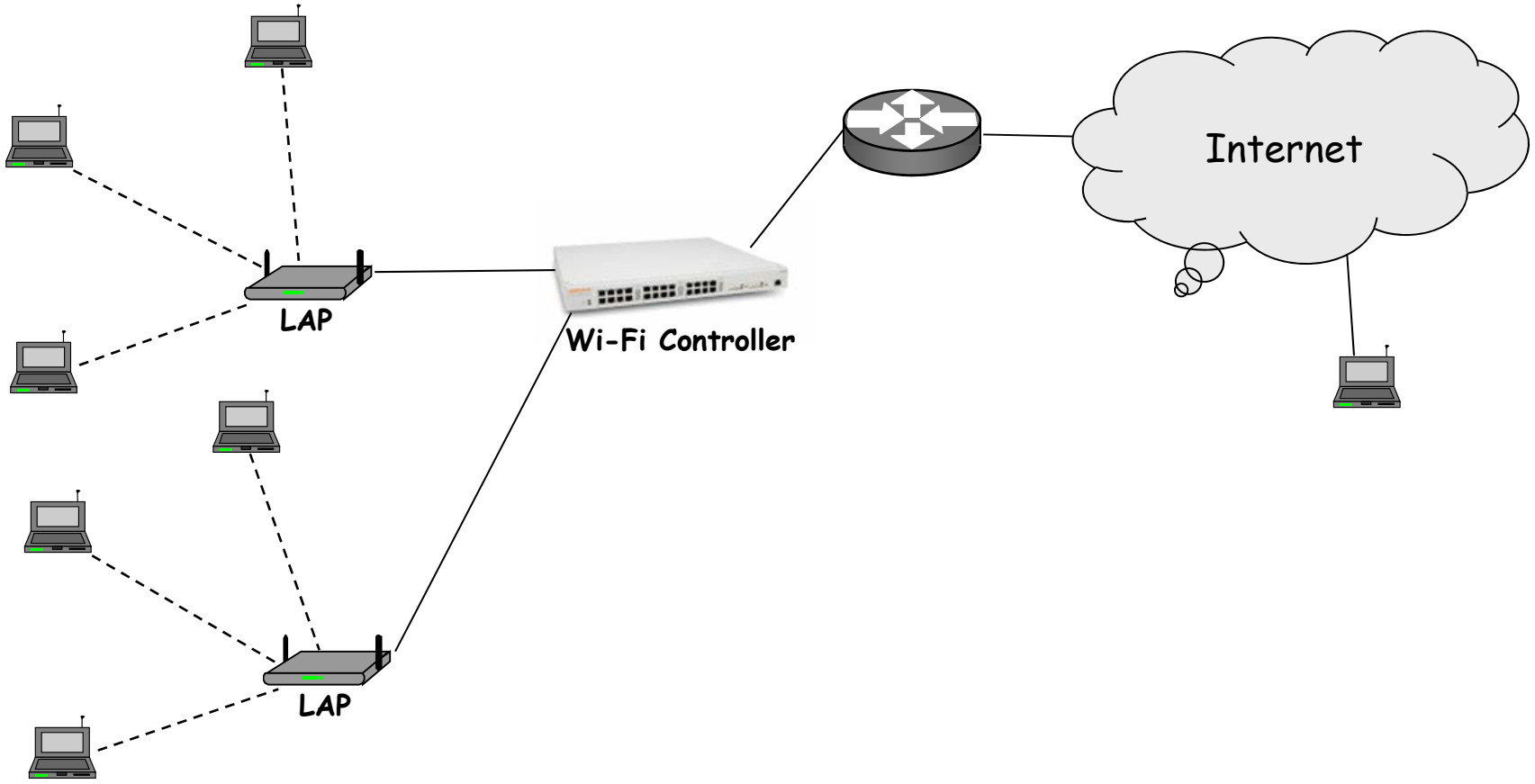


beacon
- MAC header
- timestamp
- beacon interval
- capability info
- SSID (network name)
- supported data rates
- radio parameters
- power slave flags

Introduction to Distributed WiFi Access Point Architecture



Introduction to Controller Based Wi-Fi Access Point

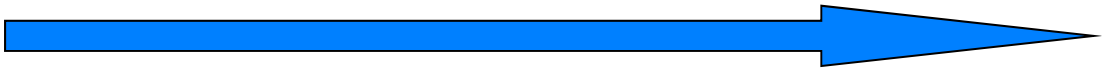


This material was presented at the IEEE North Jersey Advanced Communications Symposium - Hoboken, NJ - Sep. 21, 2013

WLAN Security Standards

	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 or 104bits	104bits perPack	128bits encry.
Key Life	24bit IV	48bit IV	48bit IV
Packet Key	Concatenation	TwoPhaseMix	Not Needed
Data Integrity	CRC32	Michael MIC	CCM
Key Management	None	802.1X/EAP/PSK	802.1X/EAP/PSK

Security Level



WiFi Security Overview

- What is WPA2?
  - Wi-Fi Protected Access 2
  - Introduced September 2004
  - Two Versions
    - Enterprise – Server Authentication 802.1x
    - Personal – AES Pre-Shared Key
  - Full implementation of 802.11i

Bit of History

- 802.11-1997
  - First wireless networking standard
  - Security via WEP
    - Wired Equivalent Privacy
  - WEP shown to have weaknesses in 2001 involving its use of RC4-Stream Cipher
  - Today it can be cracked in several minutes using standard hardware and freeware software.

Bit of History

- 802.11i – WPA
  - Draft implementation
    - WPA implemented a subset of 802.11i specifications.
  - Replaced WEP with WPA-TKIP in 2003
    - Most wireless cards easily upgraded via firmware
    - Most pre-2003 routers could not be upgraded
  - Weakness has been discovered
    - Involved TKIP algorithm use of RC4 cipher.

WPA2 Layer 2 Based Security

- 802.11i – WPA2
  - Full implementation
    - Adopted in September, 2004
  - Replaced WPA with WPA2-AES in 2004
    - Backwards compatible with WPA
  - Uses AES-CCMP
    - Advanced Encryption Standard – Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (Very Strong)
    - Selected by NIST as a US Government standard
  - Provides RSN (Robust Security Network)

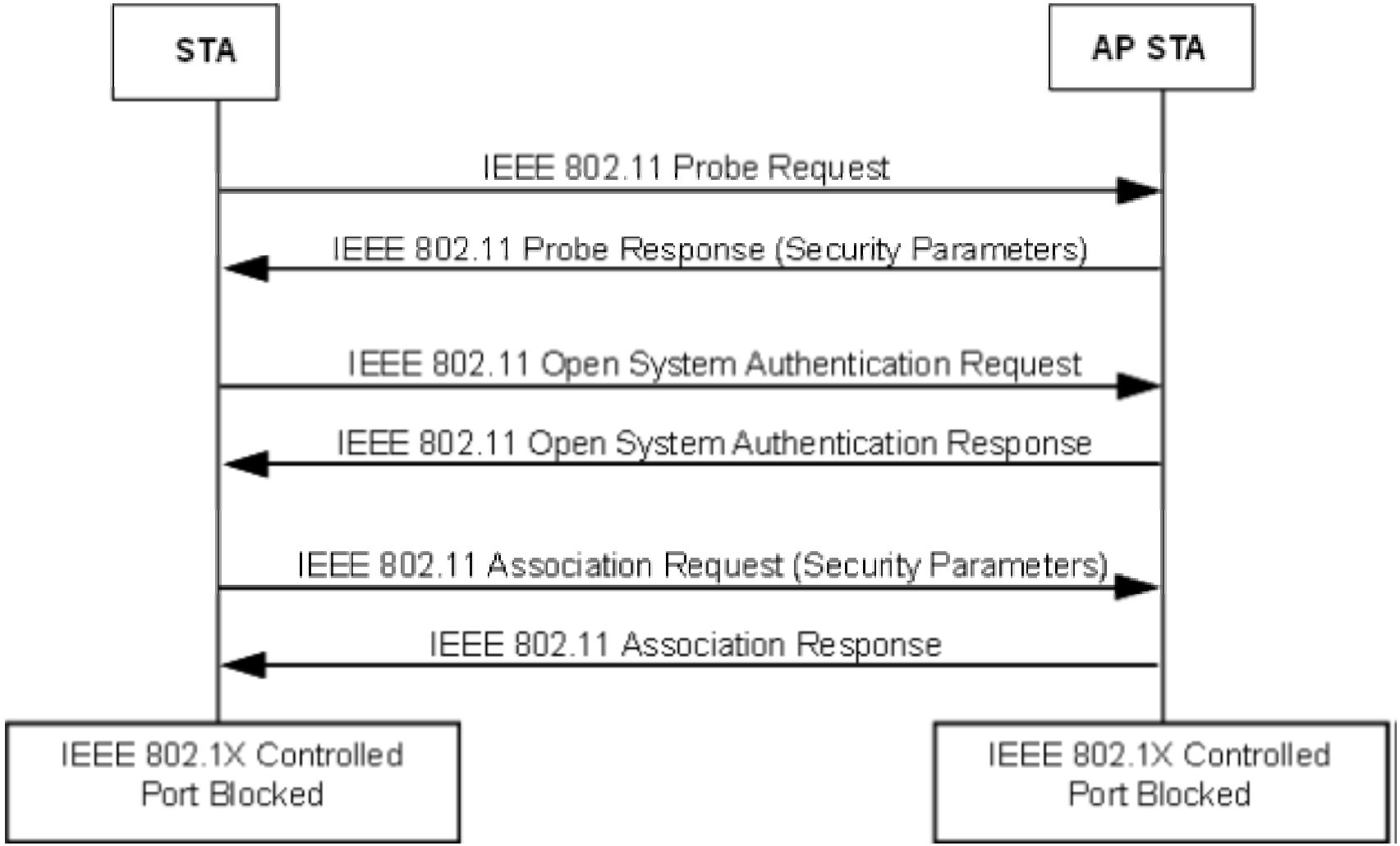
Robust Security Network via 802.1X

- IEEE 802.1X is the standard defined by IEEE for port based network access control.
- Basically a protocol to make sure only legitimate clients can use a network secured by WPA2

Robust Security Network via 802.1X

- Three players are needed to run the 802.1X protocol which uses EAP or Extensive Authentication Protocol
  - A client (STA/Supplicant)
  - A wireless access point (AP STA/Authenticator)
  - An authentication server (AS)

Robust Security Network via 802.1X



Robust Security Network via 802.1X

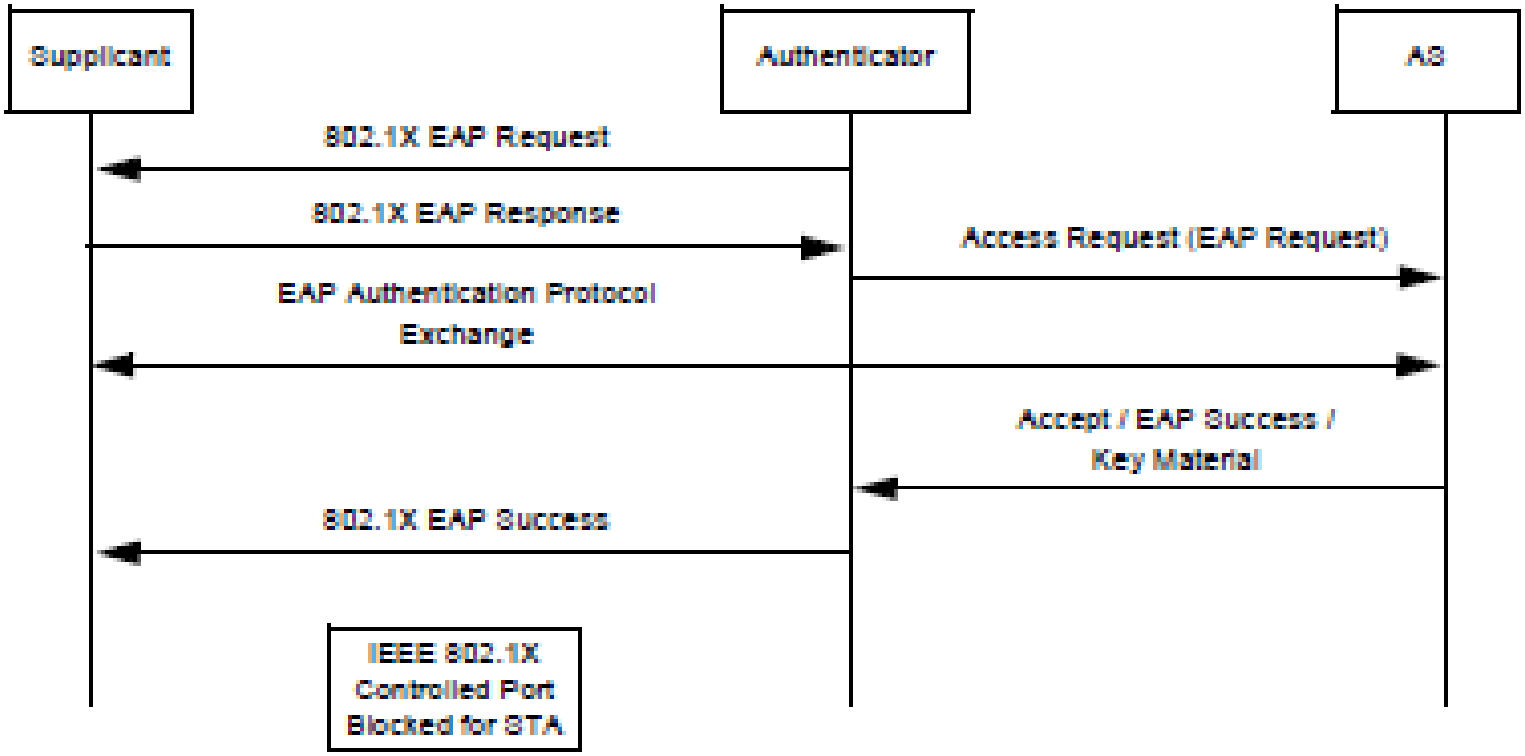


Figure 11b—IEEE 802.1X EAP authentication

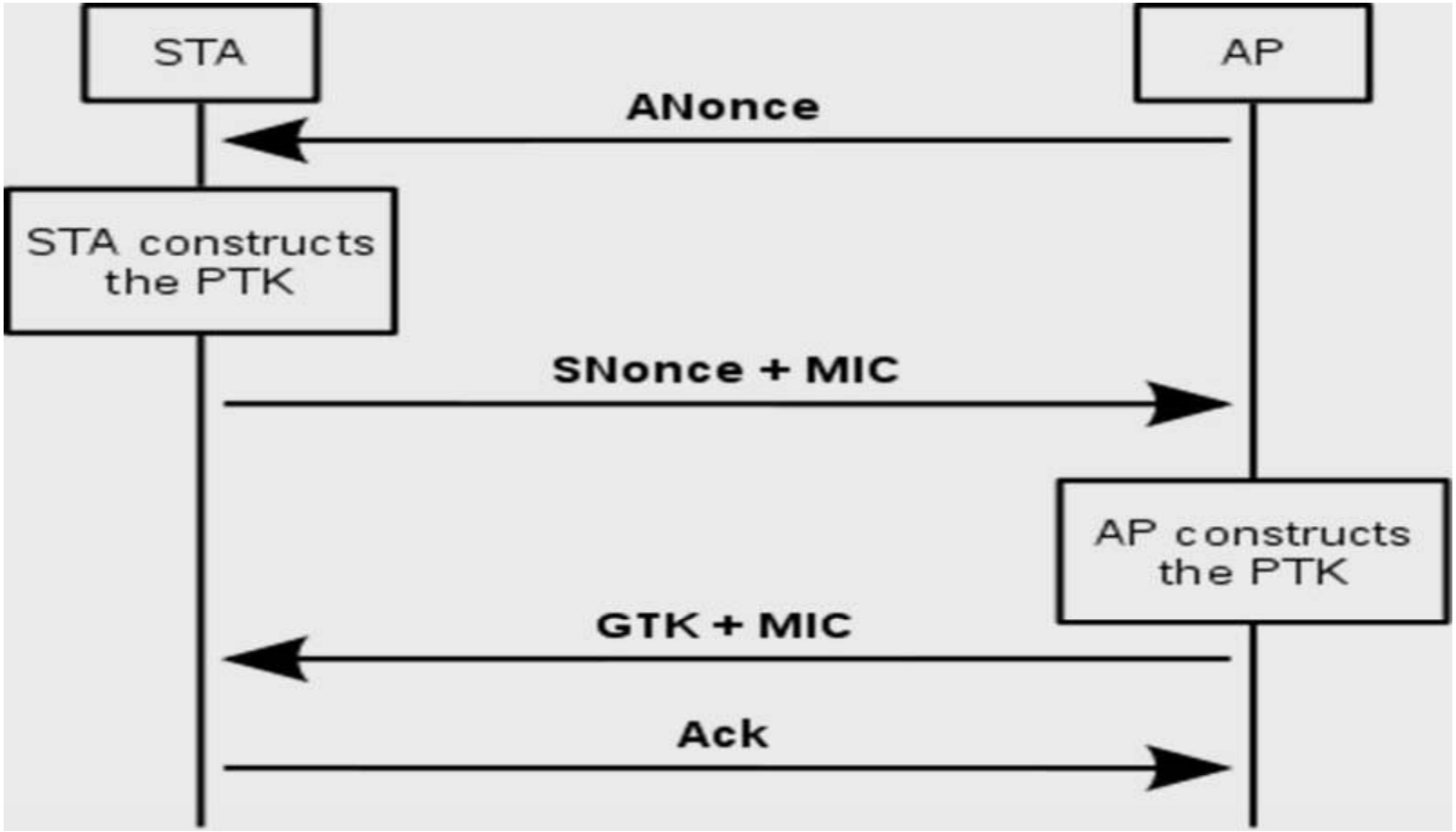
Robust Security Network via 802.1X

- PMK – Pairwise Master Key
  - Sent from the AS to the Authenticator
  - Both the Supplicant and Authenticator now have the same PMK
  - PMK is permanent for the entire session
    - Must generate a Pairwise Transient Key for encryption of data.
      - Done using 4-way handshake

Robust Security Network via 802.1X

- 4-Way Handshake
  - Confirm that the client holds the PMK.
  - Confirm that the PMK is correct and up-to-date.
  - Create pairwise transient key (PTK) from the PMK.
  - Install the pairwise encryption and integrity keys into IEEE 802.11.
  - Transport the group temporal key (GTK) and GTK sequence number from Authenticator to Supplicant and install the GTK and GTK sequence number in the STA and, if not already installed, in the AP.
  - Confirm the cipher suite selection.

Robust Security Network via 802.1X



Robust Security Network via 802.1X

- Nonce
  - A value that shall not be reused with a given key, including over all reinitializations of the system through all time.

Robust Security Network via 802.1X

- PTK (Pairwise Transient Key – 64 bytes)
  - 16 bytes of EAPOL-Key Confirmation Key (KCK)– Used to compute MIC on WPA EAPOL Key message
  - 16 bytes of EAPOL-Key Encryption Key (KEK) - AP uses this key to encrypt additional data sent (in the 'Key Data' field) to the client (for example, the RSN IE or the GTK)
  - 16 bytes of Temporal Key (TK) – Used to encrypt/decrypt Unicast data packets
  - 8 bytes of Michael MIC Authenticator Tx Key – Used to compute MIC on unicast data packets transmitted by the AP
  - 8 bytes of Michael MIC Authenticator Rx Key – Used to compute MIC on unicast data packets transmitted by the station
- Last two only used when TKIP is used.

WPA2-PSK

- Pre-Shared Key Mode
  - Network traffic encrypted using a 256 bit PMK
  - User enters key (Pairwise Master Key)
    - 64 hex digits
    - 8-63 Printable ASCII characters
      - Takes the passphrase, salts it with SSID of AP, then runs it through 4096 iterations of HMAC-SHA-1

WPA2-PSK

- Authentication, Connection, Establishment of PTK and GTK.
  - Similar process as when an AS is present except the PSK is used as the PMK.
  - Creation of PTK and GTK is the same as in Enterprise mode.

Data Encryption via AES-CCMP

- From PC-Mag:
- (AES-Counter Mode CBC-MAC Protocol) The encryption algorithm used in the 802.11i security protocol. It uses the AES block cipher, but restricts the key length to 128 bits. AES-CCMP incorporates two sophisticated cryptographic techniques (counter mode and CBC-MAC) and adapts them to Ethernet frames to provide a robust security protocol between the mobile client and the access point.
- AES itself is a very strong cipher, but counter mode makes it difficult for an eavesdropper to spot patterns, and the CBC-MAC message integrity method ensures that messages have not been tampered with.

Summary on WiFi security

- security has always been considered important for WiFi
- early solution was based on WEP
  - seriously flawed
  - not recommended to use
  - Major flaws were fixed with WPA in 2003 but didn't provide an adequate encryption algorithm
- the new security standard for WiFi is 802.11i/WPA2
  - AES-CCMP encryption algortihm
  - access control model is based on 802.1X (RFC 3748)
  - flexible authentication based on EAP
  - improved key management

15 Minute Break

Are all networks IP today?

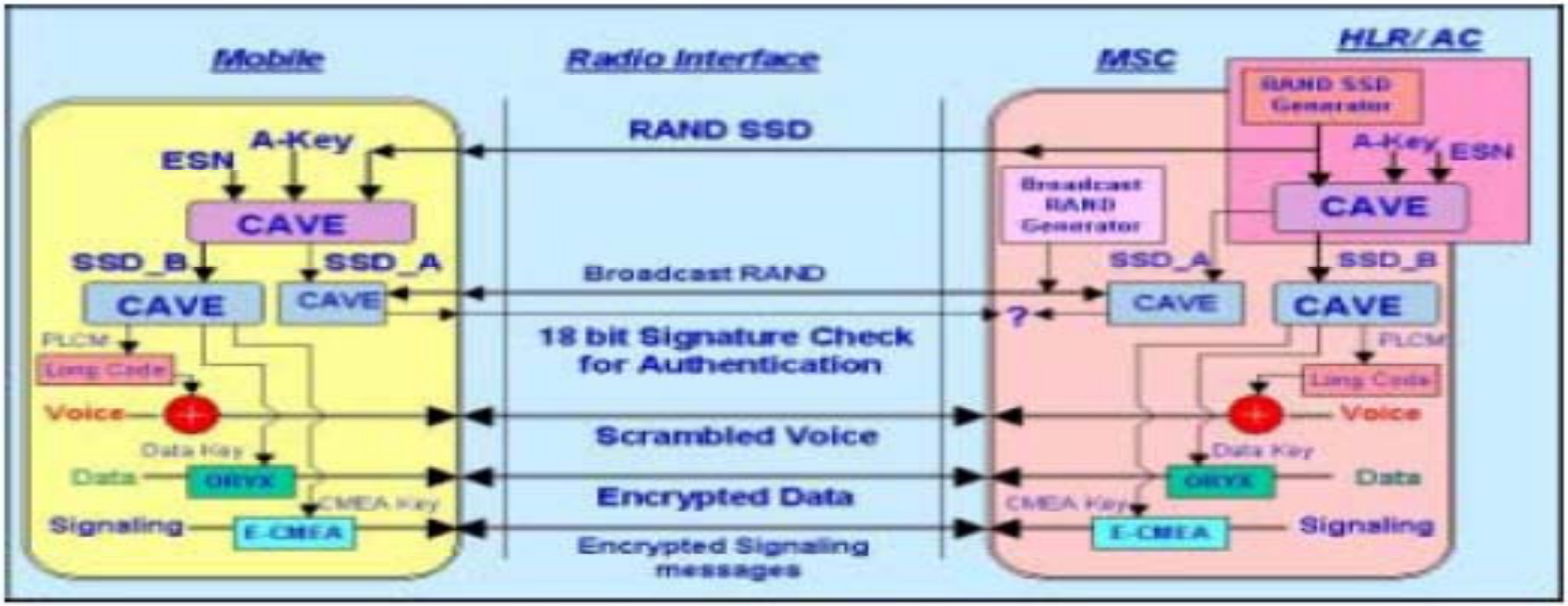
- Most of them are – but many in the process control industry are not
- Many of the existing telecom networks are not IP based either (POTS, ISDN)
- The biggest - none of the cell phones have an IP address
  - How do cell phone get calls / make calls
  - Why not use existing IP security there?
  - When did cellular security begin – Why?

WiFi Vs cellular – different standards bodies (in security)

- WiFi (layers 1, 2 by IEEE 802.11 standards)
  - Security and authentication, handled in Layer- 2 by 802.11i, beyond L-3 by IETF standard)
  - Signals upstream/downstream can be encrypted (but optional) – Also recommended by IETF
- Cellular (entirely handled by 3GPP / ETSI)
  - Security handled at the lower two layers physical (layer-1) and MAC (layer-2)
  - Authentication procedures change with every generation of cellular and start from math (see development process – later)

Why cellular – what is its strength (in security)

- Cellular security origins
  - GSM encryption introduced in 1987 but shown to be insecure in 1994). Later improved upon.
  - CAVE algorithm (1995) – see below*



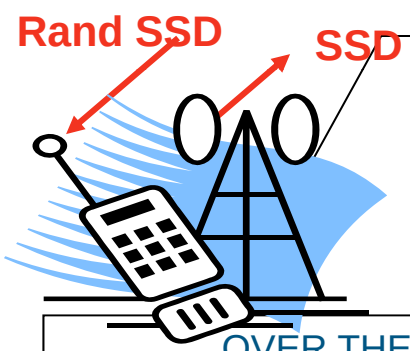
*CDMA 1XRTT security overview - by Qualcomm)

Why use cellular – what is its strength (in security)

– CAVE (Cellular Authentication and Voice Encryption)

Authentication STEP –1
Shared Secret Data (SSD)

Authentication STEP –2
Unique Challenge



(BSC)

Mobility front end (MSC)

Home Location Register (HLR)

OVER THE AIR
Rand SSD – comes from MSC
SSD – Update goes to MSC
MSC verifies
TMSI – **T**em**p**orary **S**ubscriber **I**D
(instead of MIN to avoid detection)

Handset contains:
ESN, MIN,
A-key (write only)
and CAVE algorithm

HLR Knows the handset:
ESN, MIN, A-key (Write only)
MSC generates: Rand SSD
(Random Shared Secret Data)
Asks Handset to generate:
SSD-Update using CAVE
Algorithm.The computation
utilizes handset's own
ESN, MIN and A-Key

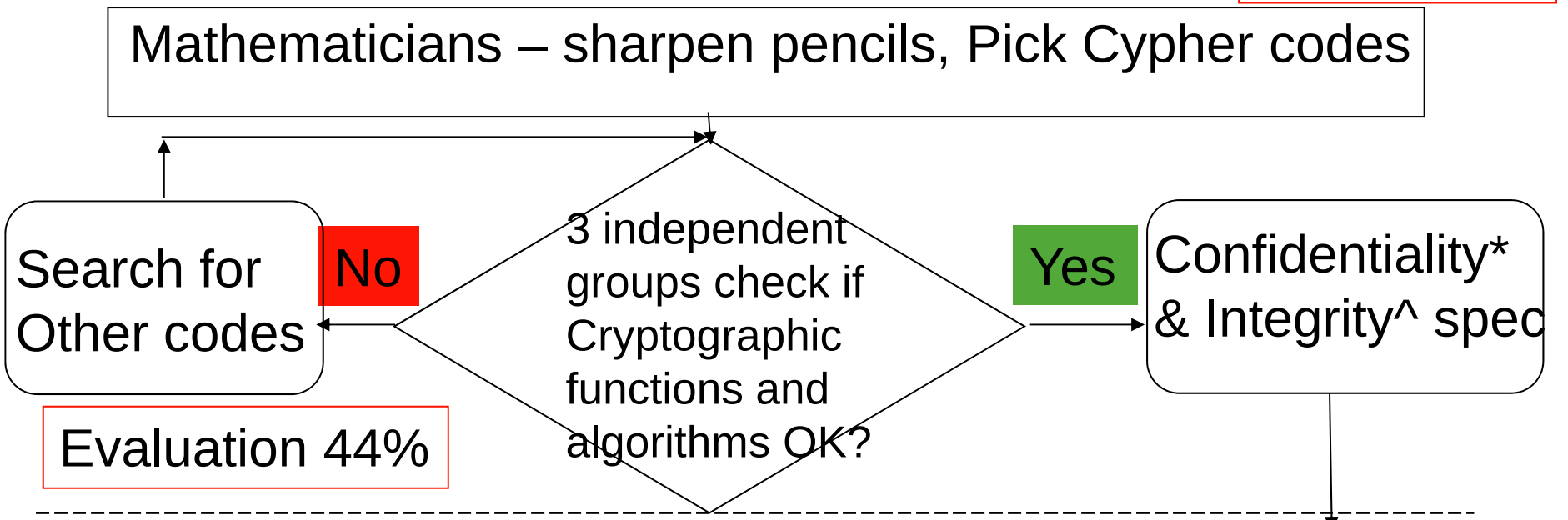
MSC uses SSD
Sent by the handset
and generates a
Unique Challenge (UC)
number. Asks handset to
Compute UC response
Using SSD-U. When
Handset sends UC-R
back to MSC, it is
verified again. After this,
the uplink and down link
are encrypted based on
SSD-U or UC-R

CDMA security - strengths

- CDMA has some inherent security
  - Codes spread signal across the band
  - Soft handoff (decided by handset) makes it difficult to track the mobile
  - Long Code Mask (LCM) provides security at the physical layer
  - CDMA signals are difficult to intercept (needs sophisticated equipment and complex math)
  - Access available only to authenticated mobile units – cannot be duplicated

3GPP Security process – each generation of Cellular

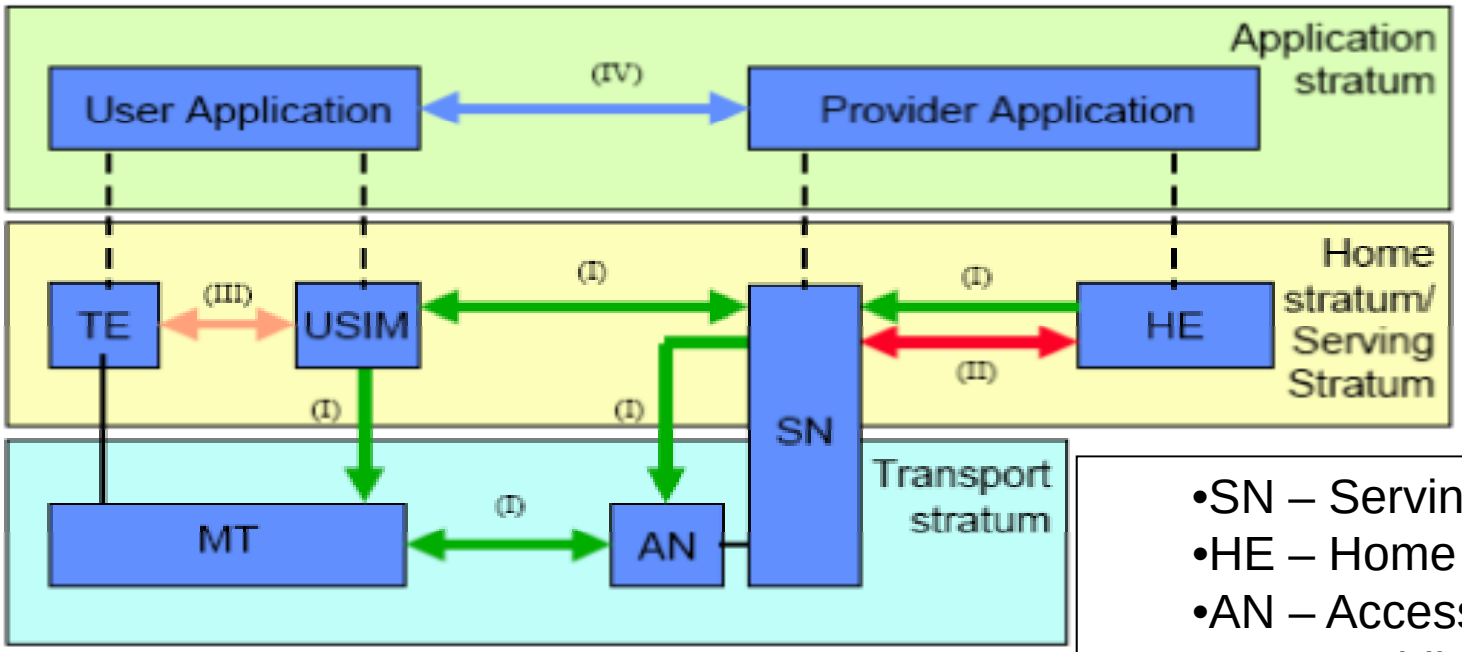
For 3G -Total 550 man days



*Kasumi MAC function F8 – protects confidentiality of user and Signal data streams (UE and RNC)

^Kasumi MAC function F9 – authenticates data Integrity of user equipment and Radio Network Controller data streams

Cellular Security – Overview Architecture



- Network Access Security (I)
- Network domain Security (II)
- User domain Security (III)
- Application domain Security (IV)
- Visibility & Configurability of Security (V)

- SN – Serving Network
- HE – Home Environment
- AN – Access Network
- MT – Mobile Termination
- TE – Terminal Equipment
- USIM – Universal Subscriber Identity Module

Cellular security – in standards*

- Cellular handset Security
  - SIM card – USIM (extension of features)
  - Physical (smart phone – unified checks)
  - Algorithms (authentication, biometrics)
- Network Security
  - Algorithms (Identity, Confidentiality)
  - Authentication process (AUC, RNC, HLR, VLR)
  - Dynamic Mobile Update (128 bit encryption)
  - Roaming authentication
  - SMS, MMS, Navigation and LBS

 * 3GPP – 3rd Generation Partnership Project

Cellular security – in practice

- Cellular handset Security
  - USIM card (PIN, biometrics, transaction ID)
  - Physical Handset (ESN, MIN, IMSI)
  - Algorithms (CAVE, Applications, Contact-less)
- Network Security
  - Algorithms (**Kasumi** Cipher codes)
  - Authentication process (F8 and F9 algorithms for Confidentiality, Integrity – user plane)
  - Dynamic Mobile Update (128 bit encryption)
  - Roaming authentication (layer 1 asymmetric)
  - SMS, MMS, Navigation and LBS

SIM card security – Beginning

* ETSI – European Telecom Standards Institute

The SIM - A Removable Security Module

GSM System Requirement:
To provide the same level of security as the fixed network

- **The SIM: Providing the security**
  - issuer specific algorithm for cipher key generation
  - security management specified by issuer
  - issuer specific authentication algorithm
- **The SIM: Providing universal plastic roaming**
  - keeping your identity when changing terminal or technology
- **The SIM: Freeing the mobile of the burden of the subscription**
  - terminal does not contain any subscription data
  - creating a global terminal market
  - bigger choice for the customer through more competition

Multi application platform –

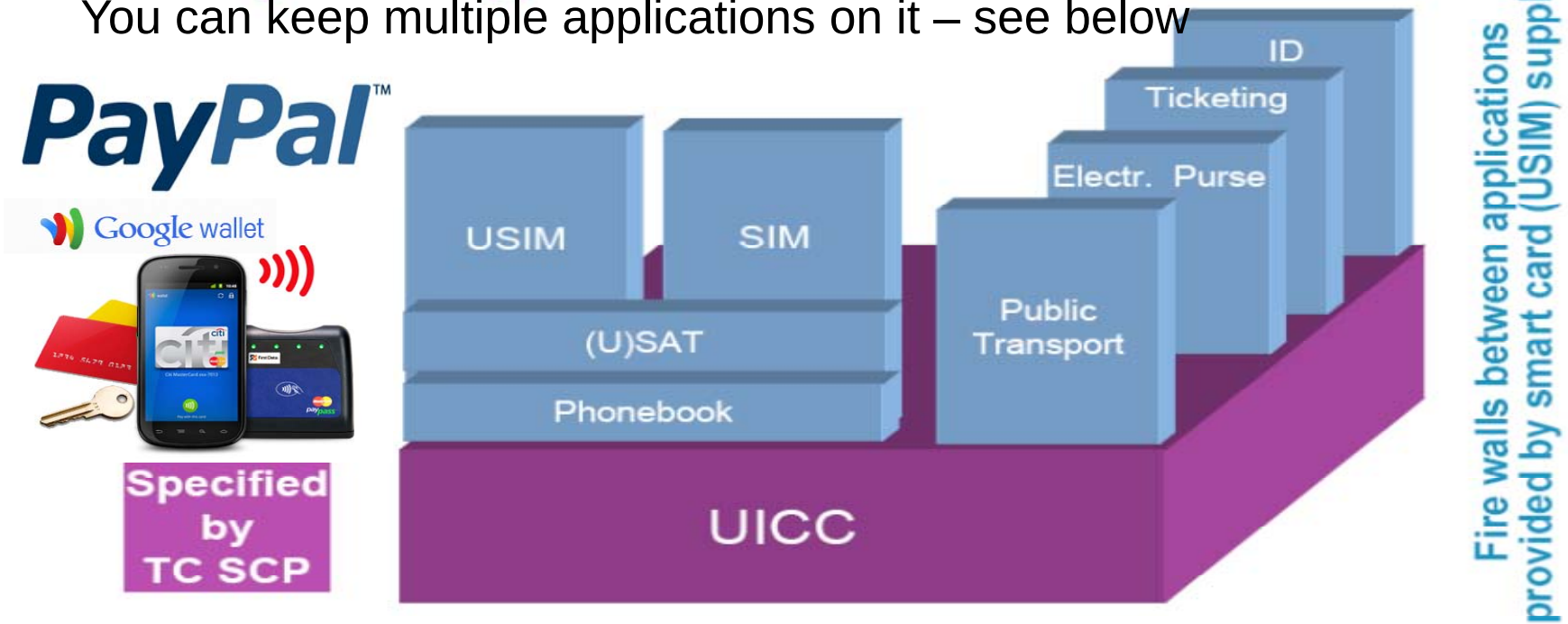
The UICC – Universal IC Card

the Multi-application Platform

It is a New generation USIM Card that works with any 3G or 4G service

The UICC specifies generic (application independent) functions and features with a clear separation of lower layers and applications

You can keep multiple applications on it – see below



* TC SCP – Technical Committee Smart Card Platform

Flexible Platform – UICC

The UICC

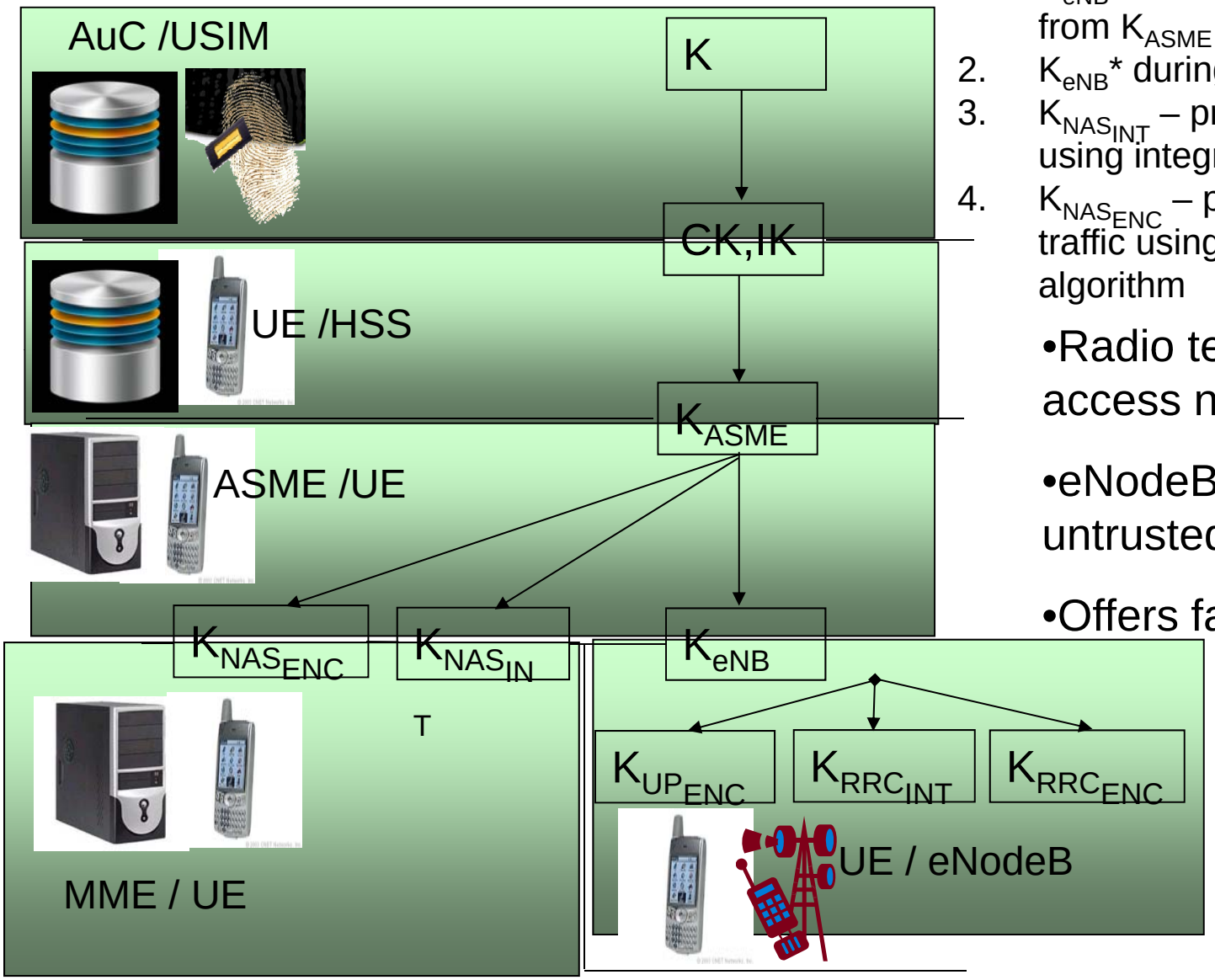
* ETSI – European Telecom Standards Institute

- The UICC provides a standardised security platform on which specific applications can be realised using today's interface to the outside world
  - Logical channels allow to run applications in parallel
  - Applications may share standardised security functions
  - Applications may have their own security functions and attributes (algorithms, (file) access conditions, …)

  As long as an application uses only the functionality specified in the platform it will run on any terminal supporting all the platform
- A new high speed Megabit interface is about to be standardised and will allow to use the smart card for DRM, stream ciphering (Pay TV) and as a mass storage device
- A contactless interface will create a wealth of new opportunities (Such as paying at a store or entry to trains etc)

LTE – Security key hierarchy

3GPP TS 33.310



1. K_{eNB}-derived by UE and MME from K_{ASME}
2. K_{eNB}* during handoff
3. $K_{NAS_{INT}}$ – protects NAS traffic using integrity algorithm
4. $K_{NAS_{ENC}}$ – protects NAS traffic using Encryption algorithm

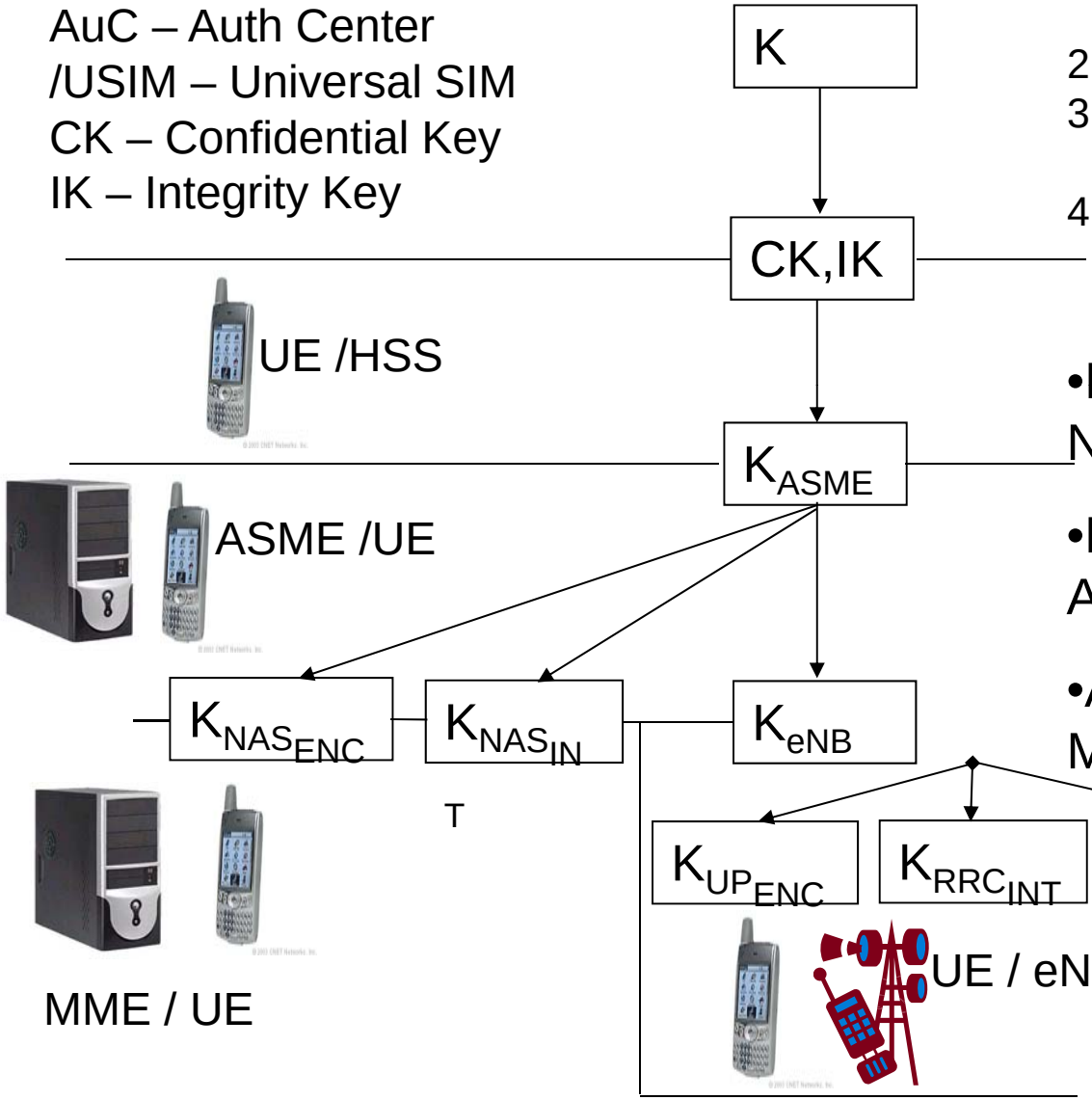
- Radio terminates in access network
- eNodeB can be in untrusted locations
- Offers faster handoff

Keeps security breaches local

LTE – Public key infrastructure

3GPP TS 33.220

AuC – Auth Center
/USIM – Universal SIM
CK – Confidential Key
IK – Integrity Key



1. K_{eNB}-derived by UE and MME from K_{ASME}
2. K_{eNB}* during handoff
3. $K_{NAS_{INT}}$ – protects NAS traffic using integrity algorithm
4. $K_{NAS_{ENC}}$ – protects NAS traffic using Encryption algorithm

- K_{eNB}-Key for enhanced Node B
- K_{NAS} – Key Network Access Segment
- ASME – Access Security Management Entity

NIST guideline - network security

Use 128 bit encryption

- 3GPP Implementation choices
- Two sets: 128-EEA1/EIA1 & 128-EEA2/EIA2
  - AES and SNOW 3G chosen as basis
  - Different from each other as possible
  - Cracking one would not affect the other
- Third set EEA3/EIA3 under consideration (under public evaluation)

"LTE Security" by *Dan Forsberg*, *Gunther Horn*, *Wolf-Dietrich Moeller*, *Valtteri Niemi* ISBN: 978-0-470-66103-1

Conclusion

- Choice:
  - IP network and its security limitations
  - Cellular networks, its strengths and limitations
  - WiFi network, strengths and limitations
  - Why these two differ – because of standards as network design approach
- Separation of layers - LTE
  - Deliberate attempt to keep security aspects by segments