



InterDigital[®]

Security Analysis of UMTS and Future Converged Devices

**Renuka Racha, Louis Guccione,
Akbar Rahman, Rajat Mukherjee**

Agenda

- Introduction to InterDigital[®]

- Wireless Security
 - UMTS Security
 - MBMS Security
 - WLAN Security
 - Security for 3GPP - WLAN Inter-working

- Summary of Threats to a Converged Device

- Opportunities for Security Enhancements

- Conclusions

Introduction to InterDigital[®]

Introduction to InterDigital[®]

- InterDigital is a developer of advanced wireless technologies and products
 - Pioneered numerous innovative approaches to solve problems in advanced digital wireless communications
 - Leading contributor to the evolution of the major global wireless standards
 - Baseband product solutions and protocol software for 3G multimode terminals and converged devices

- 3G networks provide the necessary capacity and bandwidth to enable new applications and content
 - Such as file downloads, music, video, gaming, and e-commerce
 - Operators will require various levels of security, encryption, authentication, and DRM to be implemented in the devices

- To assure broad commercial adoption of the 3G vision, security must become embedded in all wireless devices

UMTS Security

Security Threats in UMTS

- UMTS improvements address many of the vulnerabilities found in GSM security
 - Mutual authentication of User and Network
 - Message authentication is always on
 - Network is not expected to change the cipher algorithm to “no ciphering”
 - In 3G - mandatory cipher mode command
 - Data authentication
 - Replay inhibition via a sequence number
 - Integrity protection of signaling messages
 - Use of temporary identities to thwart identity catching
 - Use of MS classmark to help thwart ciphering suppression

- UMTS threats
 - **Denial of Service:** Traffic analysis can enable various attacks (by way of, for example, random access probes)
 - **Identity Theft:** An attacker gains unauthorized access to the network. For example an attacker could have stolen the information in the USIM.

MBMS Security

Security Threats in MBMS

- Threats associated with attacks on the radio interface
 - Unauthorized access to MBMS user services and/or data
 - Authorized users have very little incentive to protect the confidentiality of the data required for the service
 - Service keys can be distributed making the traffic keys vulnerable
 - Threat to data integrity
 - Follows from illegal acquisition of MTKs whereby the alteration of the transmission is possible
 - Privacy violation
 - “Content provider is located in 3GPP Network and then linked to the content” (See 3GPP TS 33.246, B.1.5)
 - At this point the user identity can be obtained, either by legal or illegal means, by the content provider: identity theft is a distinct result

WLAN Security

Security Threats in WLAN

- 802.11 wireless systems face numerous threats of which many will be addressed by the 802.11i security standard and an eventual 802.11w standard (that protects “management” frames)

- The three principal threats that will remain are
 - **Traffic Analysis:** On a WLAN an attacker can monitor the radio spectrum and initial unprotected exchanges to determine the location of nodes as well as basic parameters of the network (e.g. SSID). This information could then be used to launch physical or other types of attacks.

 - **Denial of Service:** Due to the CSMA/CA mechanism of WLAN systems (deferring mechanism) by simply generating white noise or 802.11 MAC frames at the same frequency an attacker could create a Denial of Service attack

 - **Identity Theft:** An attacker gains unauthorized access to the network. For example an attacker could have stolen a laptop with digital certificates, or stolen a login password or Pre-Shared Keys, etc.

Summary of Threats to a Converged Device

Overview of 3GPP Security for WLAN Inter-Working

- 3GPP realizes that it is in the best interests of operators and consumers to integrate cellular security mechanisms with mechanisms offered by other interfaces

- Given the increasing popularity of WLAN hotspots, and the trend amongst operators to offer WLAN coverage, 3GPP has taken several steps to integrate WLAN into its architecture

- In addition 3GPP has worked with IETF to develop two protocols that allow a dual-mode (cellular/WLAN) handset to authenticate to the core network of the operator while staying compatible with the authentication procedures of 802.11i. These protocols are
 - EAP-SIM (for WLAN/GSM) and
 - EAP-AKA (for WLAN/UMTS)

Overall Threats to a Converged Device

- If we consider a converged device having just Cellular and WLAN interfaces, the principal threats to such a device would include
 - Traffic Analysis
 - Denial of Service
 - Unauthorized Access of
 - Data stored
 - Credentials used for authentication
 - Network resources

- Further, integration of other interfaces (e.g. Bluetooth, WiMAX, Ethernet) would bring with them interface-specific threats that must also be addressed

- **Thus the overall threats to a converged device can be considered to be the sum of individual threats posed by each interface**

Security Features

- **Authentication**
Ensures that the nodes that are communicating are correctly identified
- **Authorization**
Ensures that the access to the service is according to security policy
- **Confidentiality**
Ensures that data (encrypted or sent in the clear) is only read by the appropriate parties
- **Integrity**
Ensures that data is not modified by any party other than the communicating ones
- **Availability**
Ensures that legitimate users are not denied access to resources (e.g. communication link, network resources, etc.) by invalid users
- **Non-repudiation**
Ensures that a party that sent/received data cannot deny having done so

Converged Device Threat Analysis

Threat \ Security Attribute	Authentication	Authorization	Confidentiality	Integrity	Availability	Non Repudiation	Addressed by 3GPP for UMTS	Addressed by 3GPP for MBMS	Addressed by 3GPP IW, 802.11i/w
Traffic Analysis			■				X	X	X
Active Eavesdropping	■	■	■	■	■	■	✓	✓	✓
Passive Eavesdropping			■				✓	X	✓
Man in the Middle (Redirection)	■	■	■	■	■	■	X	X	X
Replay	■	■	■		■	■	✓	✓	✓
Session Hijacking	■	■	■		■	■	✓	✓	✓
Denial of Service	■	■	■		■	■	X	X	X
Impersonation of Network	■	■	■	■	■	■	X	X	X
Identity Theft	■	■	■	■	■	■	X	X	X

■ Represents the security attribute that is compromised in theory by the given threat

- Sound security mechanism
- Mild threat generally difficult to launch
- Vulnerability

Opportunities for Security Enhancements

Opportunities for Security Enhancements Trusted Processing

- Ensure hardware and software perform as designed and mitigate attacks from any unauthorized parties
- Operating systems, platforms, application level functionality and SIM, USIM etc. must interact in a secure and trusted manner
- Trusted authentication assures that the platform configuration and software running on it has not been tampered with, enabling trustworthiness
- Trusted platforms are based on Trusted Platform Modules (TPM), a security component being specified by TCG and functions as the basis of trust within a device

Opportunities for Security Enhancements

Hardware Security

- **Secure Processors**
 - Provide a protected environment for performing security operations
 - A secure environment implemented at the heart of the microprocessor core itself, enables protection of on and off-chip memory and peripherals from software attack. A monitor switches the system between secure and non-secure states
 - When the monitor switches the system to the secure state the processor handles tasks such as authentication, management of ciphering and key management functions and the processing of secure transactions

- **Two factor authentication**
 - Biometrics such as fingerprints, retina scans etc.
 - Secure ID token generators (secure fobs)
 - Smart cards

Opportunities for Security Enhancements

Physical Layer Security

- Properties of the physical medium may be used to protect information exchange
 - Currently, security of communications is jeopardized when the shared secret is compromised
 - In UMTS and WLAN, the authentication and session keys are derived from the shared secret
 - Wireless channel reciprocity provides a unique source of shared data which can be exploited for enhanced security in data communications
 - Techniques that separate authentication and encryption procedures should be investigated

- Other physical layer means offer additional security
 - Wireless channel impulse response signatures can be used in data authentication at the physical layer
 - Several research teams have looked into using this to detect rogue adversarial packets and prevent Denial of Service attacks
 - Various signal dynamics (power, coding type and rate, modulation) and their interaction with the environment can be used to tie accessibility to data based upon receiver/transmitter location characteristics

Conclusions

- With the evolution of personal handheld devices towards open platforms and an always connected world (converged device) the threat of security is more real than ever

- Up to now, some threats on cellular networks have been contained due to the cost of launching the sophisticated attacks
 - These attacks may become easier to launch with the wider availability of equipment
 - Non-cellular radio access technologies can become an avenue for back door attacks

- Operators are increasingly
 - Seeking ways to protect the user and hence their networks from attack
 - Moving to specifying comprehensive device level security requirements

- New developments in security offer a route to providing security which goes beyond just ciphering
 - Wireless networks become more secure
 - Assure the continued roll out of advanced wireless enabled services and applications