ENHANCING SECURITY AND PRIVACY IN 3GPP E-UTRAN RADIO INTERFACE

Dan Forsberg
Nokia Research Center
Helsinki, Finland

Huang Leping
Nokia Research Center
Tokyo, Japan

Kashima Tsuyoshi
Nokia Research Center
Tokyo, Japan

Seppo Alanärä
Nokia Technology Platforms
Oulu, Finland

ABSTRACT

We focus the security and privacy threats in radio interface between evolved Node B (eNB, "base station") and User Equipment (UE). We identify new threats including several user tracking attacks by various information in MAC and RRC signalling messages, and an active attack with false buffer status reports. Finally, we propose a solution including confidentiality of RRC layer messages, periodic C-RNTI re-allocation on one cell; discontinuous sequence number in RRC message, and one time access token for MAC buffer status report.

1. INTRODUCTION

The 3rd Generation Partnership Project (3GPP), responsible of Global System for Mobile Communications (GSM a.k.a 2G) and Universal Mobile Telecommunications System (UMTS [4],[2] a.k.a 3G) standardization, has started to study Long Term Evolution (LTE) of a Radio Access Network (RAN) and System Architecture Evolution (SAE) of a Core Network (CN) to meet the demand and requirements of next generation mobile networks. LTE/SAE as a successor for 3G UMTS Terrestrial Radio Access Network (UTRAN) is called Evolved-UTRAN (E-UTRAN).

We have identified several differences and new functionalities in the E-UTRAN radio link compared to UTRAN. They are namely: (1) higher user data plane bandwidth, (2) longer User Equipment (UE) active state duration, (3) use of Discontinuous Reception (DRX) in active state, (4) no UE Medium Access Control (MAC) level identity, and (5) X2, the direct interface between evolved NodeBs (eNB).

The rest of this paper is organized as follows. We present the E-UTRAN system and protocol architecture, adversary models and required security features on this system (section 2). Next the threats against E-UTRAN based on the presented adversary model are analysed (section 3). Then we present our threat mitigation solutions (section 4). Finally, we conclude our paper (section 5).

2. SYSTEM ARCHITECTURE AND ADVERSARY MODEL

2.1 System architecture

E-UTRAN consists of eNBs connected to one or multiple control plane Mobility Management Entities (MME) and user plane SAE GWs (see Figure 1). MME and SAE GW reside in the Evolved Packet Core (EPC) network and connect to the eNBs through a many-to-many S1 interface.

E-UTRAN security is important and targeted to be in the same or higher level compared to UTRAN [4]. Security and privacy issues on the radio link (Xu interface) are the main focus of our paper.

Figure 2 shows the protocol architecture of E-UTRAN. In LTE it NAS signalling protection terminates in the Evolved Packet Core (EPC) and RRC and user plane protection in eNB. User plane carries IP data packets (over PDCP), like for HTTP browsing and Voice over IP.

The X2 interface makes E-UTRAN considerably different than UTRAN, which does not have a similar interface. The reason for having X2 is that it allows eNBs to co-ordinate the RAN in a distributed manner, making the centralized UTRAN Radio Network Controller (RNC) unnecessary and thus reducing the number of network elements for LTE. This also results having RRC protocol termination in the eNB instead in the RNC as in UTRAN. Furthermore, in the protocol stacks, the automatic repeat request (ARQ) function of radio link control (RLC) is moved to eNB, and the number of different MAC entities is reduced compared to UTRAN because the time-frequency physical resource is shared between UEs, and there is no dedicated transport channel for data transmission.

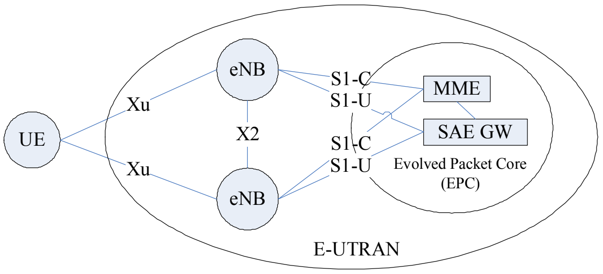

Figure 1: E-UTRAN System Architecture

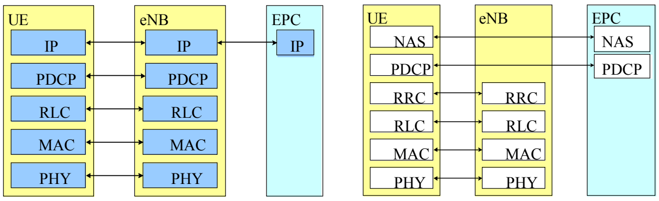

Figure 2: User Plane (left) and Control Plane (right) protocol stacks

We assume that there is no confidentiality or integrity protection at MAC layer, but integrity protection on the RRC layer.

1-4244-1144-0/07/$25.00 ©2007 IEEE.

2.2 Security and privacy requirements

Security and privacy requirements for E-UTRAN are based on the respective requirements for UTRAN architecture, grouped in five feature groups [2],[4],[6], including (I) network access security, (II) network domain security, (III) user domain security, (IV) application domain security, and (V) visibility and configuration security. For the analysis of MAC, RLC, and RRC protocol threats, we are only interested on the first group, network access security. Network access security provides following security features on radio access link: (1) User identity confidentiality (privacy); (2) Entity authentication; (3) Confidentiality; (4) Data integrity. Although the security requirement of E-UTRAN does not change too much from UTRAN, E-UTRAN has made a lot of architectural changes and introduced a lot of new features as discussed above. These changes force us to review the current security solutions and to introduce new security ones if new threats are identified.

2.3 Adversary model

In our paper, we consider multiple adversaries with different attack capabilities against the LTE network. Adversaries are classified based on (1) passive or active attacker, and (2) interface/entity they may have access to. All adversaries are able to cover multiple cells with their attacks (coverage). A Passive Radio Link Adversary eavesdrops all packets on the radio link (Xu interface) and decodes the contents if not encrypted. The Active Radio Link Adversary is additionally able to inject authorized and unauthorized packets. Modified UE could for example be used to mount active attacks both against other UEs and eNBs. These are the main adversary models we address on this paper as we want to protect against passive eavesdroppers and active attackers. In addition, we provide the adversary model of an Active Radio Jammer as a reference. When we design security solutions for UTRAN/E-UTRAN, we always compare the consequences with the cost of an attack caused by a radio jamming attack. Radio jamming attacks uses a simple analogous radio transmitter, overrides legit radio signals and confuses UEs and eNBs. This is very easy to implement, but very difficult to prevent in civil communication systems. When we design whether we should integrate a solution for a threat, we always use following criteria: If the cost to launch an attack is equal or higher than radio jamming attack, meanwhile the consequence is on the same level, we will not design a countermeasure to this attack.

3. ANALYSIS OF SECURITY THREATS IN E-UTRAN

We analyze the security and privacy threats based on the system model, adversary models and security requirements discussed above. In this section, we first discuss the information that can be observed in the AS signalling on the radio link. After that, we separately analyze the possible passive and active attacks on this interface.

3.1 Information available to an attacker

Cell Radio Network Temporary Identifier (C-RNTI) provides a unique and temporary UE identification (UEID) at the cell level, and it is assigned by the network via a RRC control signal when a UE is associated with the cell. In order to provide fast and flexible scheduling capability, C-RNTI or some equivalent UEID is transmitted with it's scheduling information in layer 1 (L1) down link (DL) control signal in plain text (i.e. not encrypted). Thus, C-RNTI and related resource allocation and other L1 control information are known to attackers. Layer 1 data frame (Transport Block) is not encrypted in both DL and uplink (UL) directions. Thus, any receiver can detect the control (C-PDU) and data protocol data units (D-PDU) of RLC/MAC/PDCP sub-layers inside them. Information, such as RLC/MAC/PDCP headers and the related control PDUs are readable for attackers. Control signals of automatic repeat request (ARQ) and UL buffer status report for UL scheduling are supposed to be sent as control PDUs. In headers of those messages, logical channel identifier and sequence numbers are supposed to be sent for the purpose of multiplexing, segmentation and ARQ.

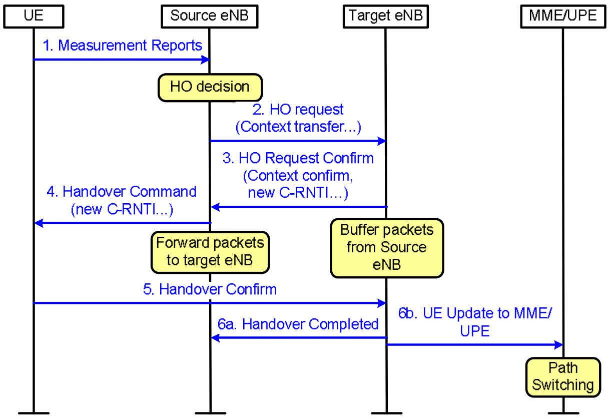

Figure 3: Signaling flow of inter-RAT handover

3.2 Passive Attacks

3.2.1 Tracking based on C-RNTI

As C-RNTI in the L1 control signal is readable, a passive attacker can know whether the UE using the C-RNTI is still in the same cell or not, also can associate the C-RNTI and the corresponding messages if not encrypted. Using the same C-RNTI within one cell provides presence information of the UE for the attacker. If the attacker can map the signalling with services, where the user identity is visible, she/he can map the cell level identity with the user's service level identity.

Figure 3 shows a schematic message sequence chart of the inter E-UTRAN handover. In the handover process, a new C-RNTI is assigned to the UE via the Handover Command message. This means that a passive attacker can link the new C-RNTI in Handover Command message and old C-RNTI in the L1 control signal unless the allocation of C-RNTI itself is confidentiality protected. This allows tracking the UE over multiple cells.

Identifying messages based on small differences in the message lengths is not obvious or most probably not even possible as the messages may be multiplexed with data, control signal, and/or padding. These should be kept in mind, when implementing the system [7].

3.2.2 Tracking based on cell level measurement reports

UE sends cell level measurement reports to the eNBs with the RRC protocol. The measurement report is for example used in handover decision making and possibly with some location based services as it provides information about the signal strength information of UE's surrounding eNBs. A Passive Radio Link Adversary listening to the measurement reports can thus deduce UE's position with higher accuracy than a single cell level identifier. In addition, if E-UTRAN uses an event-driven measurement scheme similar to UTRAN, UE will only send measurement reports when the measurement results satisfy the handover requirements. From the perspective of passive adversary, if it observes an event-driven cell measurement reports with a specific C-RNTI, the adversary knows that it is highly possible that the UE with the observed C-RNTI will be handed over to another eNB after this report.

3.2.3 Tracking based on packet sequence numbers

If the user plane (RLC, PDCP) or control plane (RRC, NAS) packet sequence numbers are continuous before and after a handover, a passive attacker can guess the mapping between the old and new C-RNTIs with a high probability based on the continuity of the packet sequence numbers. The more bits are used for the sequence number on the radio link, the higher the probability. This is particularly true for the E-UTRAN and similar networks with high bandwidth requirements, since the sequence number needs to be longer for the ARQ to work properly. This type of UE tracking is also applicable to the state transitions between idle and active modes if the sequence numbers are kept continuous. A Passive Radio Link Adversary can track the UE based on the continuous packet sequence numbers of packet streams. This attack seems to be especially interesting for E-UTRAN as the UEs will remain in active state long periods of time. It is also expected that UEs will receive more packets from the network in E-UTRAN than for example in UTRAN.

3.3 Active attacks

In E-UTRAN radio link, it is impossible (very difficult) to modify or delete a message from the radio channel. Replaying attack is prevented by sequence numbers in the message headers and as input parameter to the ciphering function. As a result, we mainly analyze the message insertion attacks here. Because RLC/MAC/PDCP UL header information is readable in UL transmission, and the resource allocation of the next transmission timing is also readable in DL L1 control signal, an active attacker can send its data in the allocated resource with proper header setting, such as logical channel ID and sequence number. However, E-UTRAN only provides random access channel for control signalling. Data should be transmitted via a shared channel (SCH). The transmission right on this channel is strictly controlled by the packet scheduler in eNB. Consequently, this type of C-RNTI re-using just collides with the transmission from the correct UE that owns the C-RNTI.

3.3.1 Message insertion attack in UE's long DRX period

In E-UTRAN, UE is allowed to stay in active mode, but turn off its radio transceiver to save power consumption. In such a DRX period, UE keeps its context (e.g. C-RNTI) in eNB. During long DRX period, UE is still allowed to transmit packets in DRX period because UE may have urgent traffic to send after entering DRX period. We believe this mechanism is necessary for a short delay and power efficient E-UTRAN. However, it may create a potential security hole to the system. An adversary can inject C-PDU to the system by using the C-RNTI of a UE in long DRX period. It is only possible to inject C-PDU because user plane PDUs is protected by upper layer security mechanism. But adversary can still benefit from the injection C-PDU into the system, and the cost to launch this attack is lower than radio jamming attack.

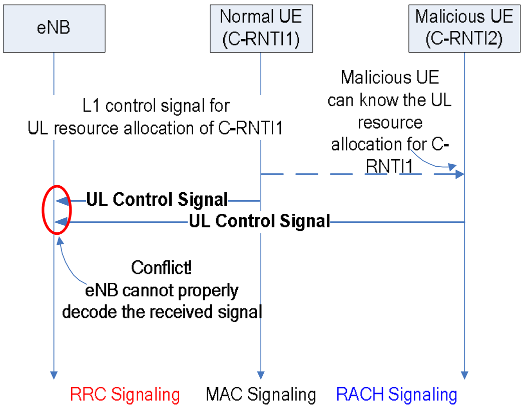
eNB
Normal UE (C-RNTI1)
Malicious UE (C-RNTI2)
L1 control signal for UL resource allocation of C-RNTI1
Malicious UE can know the UL resource allocation for C-RNTI1
UL Control Signal
UL Control Signal
Conflict!
eNB cannot properly decode the received signal
RRC Signaling
MAC Signaling
RACH Signaling

Figure 4: Denial of Service attack

3.3.2 False buffer status report attack

One way to mitigate the message insertion attack would be to request capacity via the UL buffer status report C-PDU. Buffer status report is used as input information for packet scheduling, load balancing, and admission control algorithms. An active attacker can change the behaviour of these algorithms by sending false buffer status reports on behalf of another normal UE. Although the impact of this threat depends on the implementation dependent algorithms, we can illustrate several possible attacks here.

The first attack is to steal bandwidth by changing packet scheduling behaviour. By using other UE's C-RNTI, attacker can send buffer status reports on behalf of other UEs. This can for example make the network believe that the other UEs do not have anything to transmit (i.e. empty buffers). As a result, packet scheduling algorithm in eNB allocates no/less resources to these other UEs, and more resources to the malicious UE (attacker). The second attack is to change the behaviour of load balancing/admission control algorithms in the eNBs. Attacker claims on behalf of real UEs to have more data on the send buffers than what is actually buffered in them. A lot of such fake buffer status reports from various UEs makes the network believe that there is a heavy load on this(these) cell(s). Consequently, new arriving UEs can not be accepted by this cell. These kinds of attacks are hard to detect and will decrease the throughput/capability of the system. The attack may even be considered more harmful than the radio jamming attack, since it requires less energy to execute. In practice, it is difficult for a malicious UE to mount such an attack when the UE is communicating with its serving eNB. As shown in Figure 4, the fake buffer report will collide with a packet from the normal UE. However, as discussed above, it is possible for an adversary to inject a fake buffer status report when UE enters long DRX period. This report will not cause any conflict with the control signal from a normal UE. This attack is illustrated in Figure 5. From this figure, we can observe that when a UE is in long DRX period, the buffer status report will not conflict with packets from the normal UEs.

4. SOLUTIONS FOR THREATS MITIGATION

As discussed in previous section, we observed that UE tracking and false buffer status report are two open security problems on the radio link Xu interface. In this section, we propose solutions to these two threats separately.

4.1 Countermeasure to UE tracking

Frequently transmitting C-RNTI or a field identifying UE without encryption in L1 control signal is inevitable because the flexible scheduling is required to exploit the selectivity of channel frequency response in wide spectral system of E-UTRAN. Thus, we try to propose solutions to this problem based on the assumption that a passive attacker can understand messages and associate them with the C-RNTIs.

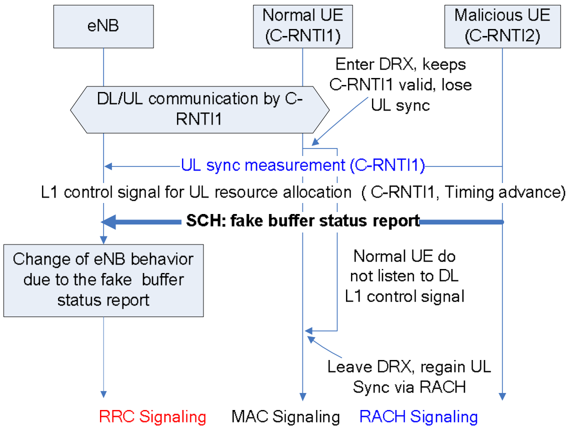
eNB
Normal UE (C-RNTI1)
Malicious UE (C-RNTI2)
Enter DRX, keeps C-RNTI1 valid, lose UL sync
DL/UL communication by C-RNTI1
UL sync measurement (C-RNTI1)
L1 control signal for UL resource allocation (C-RNTI1, Timing advance)
SCH: fake buffer status report
Change of eNB behavior due to the fake buffer status report
Normal UE do not listen to DL L1 control signal
Leave DRX, regain UL Sync via RACH
RRC Signaling
MAC Signaling
RACH Signaling

Figure 5: Successful packet injection attack

4.1.1 Ciphering RRC messages

To mitigate threats other than tracking based on the sequence numbers, we propose to cipher RRC messages. Whether to cipher all RRC messages or a part of RRC messages listed below depends on other issues such as system complexity etc.

a) Ciphering RRC messages, such as Handover Command and Handover Confirm, prevents a passive attacker from understanding associating the RRC messages to a C-RNTI, and mapping them together during handovers

b) Ciphering RRC measurement report messages, prevents an attacker from understanding the measurement report and tracking UEs accurately.

In general, ciphering all RRC messages prevents other types of attacks based on plain text RRC messages that we have not even detected or analysed. Ciphering all RRC messages is also similar to what UTRAN does.

4.1.2 Periodic C-RNTI re-allocation on one cell

In case the UE stays long times in a single cell it may be beneficial to securely re-allocate the C-RNTI to make it more difficult for an attacker to get information about a single UE presence on the cell. This also makes it more difficult for an attacker to detect if new UEs arrive to the cell or if they are just UEs refreshing the C-RNTI.

4.1.3 Discontinuous sequence numbers

Sequence numbers, if they exist, are used at least for ciphering and deciphering in PDCP, RRC, and NAS, and for re-transmission in RLC. In addition, they may be used for re-ordering if necessary. Thus, although an RRC message can be ciphered to prevent UE tracking, the sequence number needs to be transmitted without encryption because it is used as an input parameter for the ciphering function. To mitigate UE tracking based on sequence numbers, we propose that the sequence numbers over the radio are discontinuous in handovers and possibly also in idle-to-active mode transitions.

The sequence number must be continuous for the ciphering function during a key lifetime, as it is required that the sequence number as an input variable for the ciphering function must be unique for both UL and DL packets with the same ciphering/integrity protection key. Thus, one possible solution is to use a random offset to make the user and control plane sequence numbers discontinuing on the radio link. For example, these random offsets are selected by the target eNB and carried along with the new C-RNTI to the UE via source eNB in the encrypted RRC Handover Command message.

Another solution is to use fresh keys for each eNB, which then allows setting the sequence number to any random value and thus makes it discontinuous.

4.2 Countermeasures to active attacks

As discussed in previous section, we identified that an Active Radio Link Adversary can utilize false buffer status reports to change the behaviour of packet schedulers, admission control and load balancing algorithms on the eNBs. As a solution to this problem, we propose to include a one-time access token within the MAC level buffer status report message. UE needs to present this token to the eNB to get the access right. As per definition the one-time-access-token is different for each buffer status report sent during a DRX period. There are several ways to update the one-time-access-tokens in eNB and UE.

a) A new one-time-access-token is sent in the encrypted RRC control message from eNB to the UE. This however requires RRC protocol involvement for each buffer status report, which is not considered to be feasible.

b) UE receives a nonce at initialization phase via a secure channel (ciphered RRC or NAS) and uses a one-way hash function to generate one-way chain of access tokens [7]. One access token is used per buffer measurement report.

c) UE and eNB can use a shared RRC key(s), a pre-defined increasing sequence number, and other known parameters to calculate a series of numbers as access tokens with a one-way hash function.

The size of the token may become an issue when optimizing the communication. In this case the output from the one-way hash function can be truncated to a certain number of bits (like 8...32 bits)

Figure 6 illustrates the one time access token solution. eNB first provides information for creating the access token via RRC messages. When a UE has some urgent traffic to send in DRX period, it first transmits an UL synchronization message to ask for DL/UL resources. After receiving UL synchronization message, eNB allocates some DL/UL resources for that UE. UE then sends buffer status reports with a one-time access token. This prevents an Active Radio Link Adversary from sending false buffer status messages on behalf of the legit UEs.

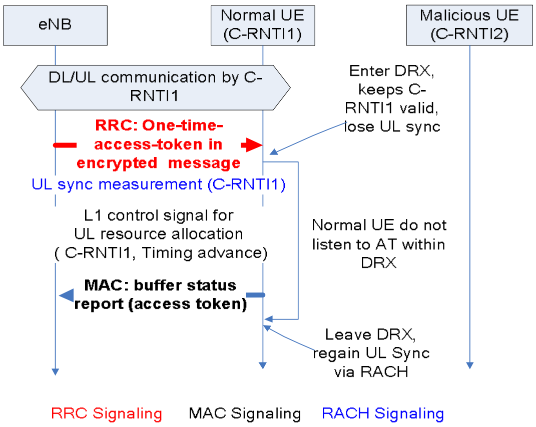
eNB
Normal UE (C-RNTI1)
Malicious UE (C-RNTI2)
DL/UL communication by C-RNTI1
Enter DRX, keeps C-RNTI1 valid, lose UL sync
RRC: One-time-access-token in encrypted message
UL sync measurement (C-RNTI1)
L1 control signal for UL resource allocation (C-RNTI1, Timing advance)
Normal UE do not listen to AT within DRX
MAC: buffer status report (access token)
Leave DRX, regain UL Sync via RACH
RRC Signaling
MAC Signaling
RACH Signaling

Figure 6: A one-time access token

5. CONCLUSION

In this paper we have analyzed the security and privacy threats on the LTE radio link Xu interface. The objective of our analysis is to design a protocol stack that satisfies four security and privacy requirements as in UTRAN: (1) User identity confidentiality (privacy); (2) Entity authentication; (3) Confidentiality; (4) Data integrity. When designing countermeasure to those threats, we carefully considered both the performance degradation caused by additional security functions and seriousness of the newly identified threats.

In RRC layer, we identified several new threats including user tracking attacks by various information in RRC signalling, and active attack by false buffer status report. Considering the seriousness of those attacks, we conclude that is it necessary to include confidentiality and integrity protection in RRC layer messages. On the other hand, in MAC/RLC/PHY we identified threats towards users' identity confidentiality (privacy) and data integrity, which are not mitigated with the RRC layer confidentiality and integrity protection. The threats include false MAC level buffer status reports and tracking by C-RNTI. We avoid using any cryptographic functions in MAC/PHY layer because of performance consideration. Instead, we proposed two non-cryptographic solutions to address these threats' namely discontinuous packet sequence number by random offset and one-time access token for authenticated buffer status reports on the MAC layer.

We believe that the threats and countermeasures we have described are not E-UTRAN specific only, but are applicable for other radio access technologies as well. Alone these threats are not severe, but together they pose a risk to the system. We believe that our described countermeasures are cost efficient and easy to implement and thus applicable for E-UTRAN.

ACKNOWLEDGMENT

We would like to thank Sebire Benoist and Dajiang Zhang for providing good comments for us.

REFERENCES

[1] H. Kaaranen, A. Ahtiainen, L. Laitinen, S. Naghian, V. Niemi, "*UTRAN Networks, Architecture, Mobility, and Services*", 2001 John Wiley & Sons, ltd, ISBN 0471 48654 X.

[2] V. Niemi, K. Nyberg, "*UMTS Security*", 2003 John Wiley & Sons. Ltd, ISBN 0-470-85314-X

[3] 3GPP TR 25.913: "Requirements for Evolved UTRA (E-UTRA) and Evolved UTRAN (E-UTRAN)"

[4] 3GPP TS 33.102: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; 3G Security Architecture"

[5] 3GPP "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Rationale and track of security decisions in Long Term Evolved RAN/3GPP System Architecture Evolution", work-in-progress

[6] 3GPP TS 33.120: "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Security principles and objectives"

[7] Andrea Bittau, Mark Handley, Joshua Lackey, "The Final Nail in WEP's Coffin", *Proceedings of the 2006 IEEE Symposium on Security and Privacy (S&P'06)* - Volume 00, Pages: 386 – 400, 2006.