3GPP TSG SA3 Ad-hoc Meeting **S3z030012**
3 - 4 September 2003
Antwerp, Belgium

Agenda item: 6.2

Source: Samsung

Title: (U)SIM clone and MBMS security

Document for: Discussion

1. Introduction

Current broadcast/multicast service content provider shall prefer to provide the similar content to the mobile users using the new MBMS bearer in the future. And the (U)SIM clone scenario, which is similar to the decoder clone scenario existing in current satellite pay-TV system, shall likely occur in the future MBMS commercial application. In this document, this (U)SIM clone scenario is analyzed and it is concluded that frequent MBMS key updating may reduce the harm caused by this (U)SIM clone. And SA3 is proposed to take this into consideration when evaluating various MBMS user authentication/authorization and MBMS key management/distribution approaches .

2. Discussion

Users services that use MBMS bearer are currently being standardized within the work item "MBMS Teleservice", which was approved during previous SA#21 plenary meeting. Also, the MBMS bearer is also available to support services other than the MBMS Teleservice. Considering that the service content providers who provide the broadcast/multicast services to users using existing bearers (e.g. satellite pay-TV) nowadays shall likely prefer to provide the similar service contents to the mobile users using the future MBMS bearer, it can be predicted that service similar to the satellite Pay-TV service shall likely be introduced in "MBMS Teleservice".

As we know, one major security threat to current satellite Pay-TV service is the decoder clone. Most satellite Pay-TV industry insiders suggest about 10 per cent above the industry's 1.5 million paying subscribers are illegally tapping into pay-TV content. Such users legally buy a satellite dish and decoder, which is loaded with an illegally programmed smart card that gives access to all services. Once the satellite signal has been decoded with the illegal smart card, all channels, including pay-per-view events and adult and premium channels, become available. The similar decoder clone problem may also exist in the future MBMS system.

2.1 (U)SIM clone

Until now, several different mechanisms [1][2] have been reported to be feasible to be used to crack the SIM encryption, thus allowing that the creation of a cloned phone can be done even in only a few minutes in current GSM system. It can even be imaginable that future U(U)SIM smart card for 3G can also be possible to be cracked and cloned if the hacker can contact the U(U)SIM for enough long time, as computer runs faster and faster. Also, Considering the backward compatibility, some legacy SIM cards in current system can be also used for accessing some 3G services, e.g. MBMS. For example, some people may be reluctant to migrate or renew their own SIM cards for MBMS services because they have to re-enter their phonebooks. These legacy SIM cards shall face more threats to be possibly cloned.

In current GSM network, it was reported that each of these cloned SIM cards can pass the network authentication successfully and can be used normally as the original legal one. The only effect to these SIM cards (cloned cards and original legal card) is that only one of them can be used at the same time. Usually it is the UE who owns the cloned or original SIM card but powers on latterly. The VLR/HLR shall only store this latest position of the UEs(SIMs) reported.

In current GSM network and future GERAN/UTRAN network, charging is quite related to subscriber certification. Once the (U)SIM and the network has already passed the mutual authentication each other, the (U)SIM card owner shall have to pay for whatever this (U)SIM is involved in. Usually, most CS/PS domain services shall request the UE reside in RRC Connected state for voice call and/or data transmission/reception, no matter whether this UE is equipped with one legal (U)SIM card or cloned SIM card. That is, the UE who owns the cloned (U)SIM card can also be charged for the voice call it makes and/or data it receives/transmits. Thus, this (U)SIM clone scenario may do not harm much to the network operator if charging for the service subscribed by the original legal (U)SIM is only based on time/duration/volume. But this (U)SIM clone scenario shall harm the network operator greatly if flat-rate charging is adopted for the service subscribed by the original legal (U)SIM.

As for the legal and original (U)SIM owner, the situation shall be quite opposite. If charging for the service subscribed by the original legal (U)SIM owner is relevant to time/duration/volume, this original legal (U)SIM owner has to afford extra payment caused by the cloned ones. While flat-rate charging is adopted for the service subscribed by the original legal (U)SIM owner, one predefined charging shall be accounted for this original legal (U)SIM owner no matter how long the call or service lasts and/or how many bits of the content the user actually receives during a agreed time interval. In other words, this (U)SIM clone scenario may do not harm much to the original legal (U)SIM owner within this agreed time interval when the flat rate charging mode is adopted.

Certainly, the network operator can disable all these (U)SIM cards (both the cloned cards and the original card) and instruct the user to change to a new (U)SIM card if it is reported stolen or possibly cloned. Also, the network may find some suspicious (U)SIM cards and further check their validations with the original users.

2.2 (U)SIM clone for MBMS security

For MBMS, it is widely accepted that a SIM or USIM shall be present in the UE to receive MBMS multicast services. This (U)SIM is used to uniquely authenticate and authorize one particular user whether he is allowed to access one particular MBMS service or not.

As we know, in order to use radio and network resources efficiently, the network shall be able to select ptp or ptm transmission mode depending on the number of users for one specific service. Currently within RAN2/3, it is agreed that UEs, in no matter RRC IDLE state or in RRC Connected state, shall be able to receive the MBMS traffic data when ptm transmission mode is used. The nature of ptm transmission (e.g. user occasionally listens in to a ptm transmission) makes it difficult for the network to charge for the exact amount of content that the user has consumed; the network may simply have no way to find out this. Thus, this makes it possible the flat rate charging mode shall be used for at least certain kinds of MBMS services. This flat rate charging mode is widely accepted within SA3 indeed as one possible charging modes for MBMS.

Thus, this makes it possible that the original (U)SIM owner can turn to be malicious; this hacker may try to clone his own (U)SIM card, which shall give this hacker enough long time for operation, and sell them on low prices. One by one, UEs equipped with one cloned (U)SIM card can power on, pass the network authentication to obtain the traffic encryption key and then reside quietly in RRC IDLE state for MBMS data reception. And this malicious original (U)SIM card owner may never report or admit that his (U)SIM card is stolen/cloned even when the network owns some suspicion and check this with him.

However, since illegal UEs equipped with cloned (U)SIM cards can only pass the network authentication one by one, it is quite obvious that there shall exist some delay from the time when the first illegal one passes the authentication to the time when the last illegal one passes the authentication. MBMS traffic encryption keys should only be distributed to the users who can pass the network authentication, so this delay means that these illegal UEs may obtain different versions of the traffic encryption keys, if these traffic encryption keys can vary adequately fast. Thus, although each illegal UE may be able to get the correct version of the traffic encryption keys at the time when it passed the network authentication, some of these illegal UEs have to only use the expired version of the traffic encryption keys for some time before they pass the network authentication next time. In this means, frequent MBMS key updating can reduce the harm caused by this (U)SIM clone scenario.

3. Conclusion

Based on these analyses above, it seems that the possible (U)SIM clone scenarios existing in the future UTRAN/GERAN network systems shall be one great threat to the MBMS actual commercial application, and frequent MBMS key updating may be able to reduce the harm caused by the (U)SIM clone to some extent. So, we propos that SA3 should take this into consideration when evaluating various MBMS user authentication/authorization and MBMS key management/distribution approaches.

4. Reference

[1] “Partitioning Attacks: Or how to rapidly clone some GSM cards”, Josyula R Rao, IEEE Symposium on Security and Privacy, May 12-15. 2002

[2] “GSM Crack Belittled: SIM Code Copying Not Unique”, Edward Warner, Wireless week, April 20, 1998