Security risks of pre-IMS AKA access security solutions

Dubravko Priselac
Ericsson Nikola Tesla d.d.
Krapinska 45, 10000, Zagreb, Croatia
dubravko.priselac@ericsson.com

Miljenko Mikuc
University of Zagreb
Faculty of Electrical Engineering and Computing
Unska 3, 10000 Zagreb, Croatia
miljenko.mikuc@fer.hr

Abstract – For IP Multimedia Subsystem (IMS) access security there is only one authentication and access security solution that is known as IMS AKA (as specified in 3GPP TS 33.203). However there exist pre IMS AKA solutions that are designed to either allow usage of non-standard IMS terminals or enable quick IMS deployment. For such pre standard solutions this paper analyzes security risks, viability of illegitimate usage and protection measures. We also present examples of unsecure implementations of security features discovered at IMS softclients.

I. INTRODUCTION

Internet users with narrowband and broadband access experience variations of quality for real time Internet multimedia services (phone or video calls and audio or video streaming). The cause of quality of service (QoS) variation is the fact that Internet service providers provide only best effort Internet access to their users and have no way to impose any quality of service requirement outside of their own network.

Solving the quality of service problem for Internet Protocol (IP) multimedia services was one of the main drivers for creation of IP Multimedia Subsystem (IMS). IMS enforces QoS by monitoring user traffic according to user negotiated QoS parameters. Another driver was the need for quick service introduction for IP multimedia services. That requirement was fulfilled by borrowing Intelligent Network (IN) idea of centralized service control.

At the beginning IMS was envisioned as a merge between Internet services and mobile networks, i.e. a system where mobile user accesses Internet services with guaranteed quality of service and inter-operator roaming. In later design phases IMS embraces wireless local area network (WLAN) and fixed access types as well.

Security in mobile networks has evolved from analog mobile Nordic Mobile Telephony (NMT) network with no proper authentication and no encryption, over digital Global System for Mobile communications (GSM) network with encryption but only partial authentication to Universal Mobile Telecommunications System (UMTS) networks with encryption and mutual authentication. The main security feature of GSM/UMTS networks is user transparency. Users are not required to either know or input long security keys in order to authenticate themselves to network. All security features including the secret key reside on a smart card that is inserted into user terminal.

IMS has wisely adopted UMTS strong and user transparent authentication mechanism that will sweep out password based human dependent authentication methods from IMS visioned Internet world.

From security point of view it sounded too good to be true. Well, it was until some obscure ideas like legacy terminals and quick deployment got into IMS focus…

II. IMS SECURITY

IMS may be exposed to attack by different types of attackers. First type are script kiddies, curious but inexperienced crackers who lack the ability to write sophisticated hacking programs on their own and who have fun initiating simple attacks for published security problems and their exploits. Unlike the script kiddies the second type are well-educated attackers and their frauds are driven towards financial goals. Third type also possesses good knowledge and economical motivation but their activities are not frauds but industrial espionage. IMS operator employees are potentially dangerous attackers since they have excellent knowledge of the system.

There are different security threats to IMS system:

- Unauthorized access to services.
- Disturbing or misusing network services (leading to denial of service or reduced availability).
- Unauthorized access to sensitive data (violation of confidentiality).
- Unauthorized manipulation of sensitive data (violation of integrity)

Protection of IMS system is achieved by implementation of different security services: authentication, authorization, integrity, confidentiality and availability.

IMS Security consists of following security areas:

- *Access Security* covering end-user access to the IP Multimedia System and its services.
- *Network Domain Security* covering perimeter protection and the protection of communication towards co-operating external networks (operators) and between geographically dispersed sites. It also covers node protection and security audit logging.
- *Operation and Maintenance (O&M) Security* covering access control for management operations and the protection of O&M, provisioning and charging interfaces.
- *Security Management* covering the management of security functions and attributes.

There are five different security associations and different needs for security protection of IMS and they are numbered 1, 2, 3, 4 and 5 in figure 1 where:

1. Provides mutual authentication between the user equipment (UE) and the IMS Core Network Subsystem (IM CN SS). The Home Subscriber Server (HSS) is responsible for generating keys and challenges while the authentication is carried

out by the Serving Call Session Control Function (S-CSCF).

2. Provides a secure link and a security association between the UE and the Proxy CSCF (P-CSCF) with authentication of data origin.
3. Provides security within the network domain internally for the Cx-interface.
4. Provides security between different networks for Session Initiation Protocol (SIP) capable nodes. This security association is applicable when the roaming UE is in a visited network.
5. Provides security within the network internally between SIP capable nodes. This security association is applicable when the UE is located in his own home network.

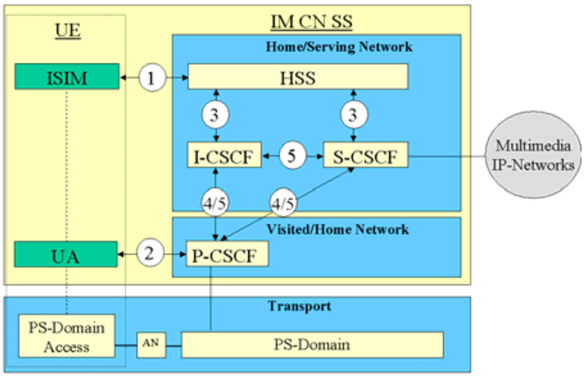

Figure 1: The IMS security architecture

III. IMS ACCESS SECURITY – IMS AKA

Access security addresses the security between the UE and the IMS network.

Following security features are included in IMS access security:

- Authentication of the subscriber and the network, allowing the network and the user to authenticate each other. (see security association number 1 in figure 1)
- Confidentiality and Integrity protection of the IMS signaling. (see security association number 2 in figure 1)
- Policy control system, which allows the network to control the traffic to and from the UE.

Standardized IMS access security solution is specified in 3GPP TS 33.203 and also referred to as IMS AKA. It is basically UMTS AKA protocol used in 3G mobile networks that is integrated into HTTP Digest protocol.

IMS users must be authenticated and authorized in order to use IMS services. Authentication and authorization functions and other user information reside on a smart card that is inserted in the UE. The smart card is known as Universal Integrated Circuit Card (UICC). UICC can hold different applications: Subscriber Identity Module (SIM), UMTS Subscriber Identity Module (USIM) or IP Multimedia Services Identity Module (ISIM). Access to IMS is allowed only with an USIM or ISIM application. A secret long-term key is pre-shared between the ISIM and the HSS. The key is used for symmetric cryptography by Authentication and Key Agreement (AKA) mechanism. Instead of the secret key the UE and the IMS network exchange challenge and response values that are generated from the key. Result of AKA is not only mutual authentication but also negotiation of confidentiality and integrity keys for IP security (IPsec) tunnels. IPSec tunnels (see security association number 2 in figure 1) are formed between the UE and the IMS for all subsequent exchange of control SIP messages thus only unprotected control messages are error messages and initial register messages.

From user prospective IMS AKA does not require any user action and therefore it is not prone to human glitches.

Media protection (encryption or integrity protection) is currently not defined for IMS and thus it relies on the protection provided by the access network.

IV. PRE-IMS AKA SOLUTIONS

A Number of pre IMS AKA security solutions have been defined despite the existence of the standard authentication and access security solution. 3rd Generation Partnership Project (3GPP) standards are structured as Releases. IMS is introduced in 3GPP Release 5 but that initial release covers only 3G mobile access to IMS services. WLAN and fixed line are supported in later releases.

As standard solution requires that IMS terminals implement IPv6 and IPSec protocols as well as UICC with ISIM or USIM, different pre IMS AKA solutions have been defined to cover legacy terminals or just to enable early deployment of IMS services.

Different standardization bodies have chosen different pre IMS AKA solutions:

- Early IMS – used by 3GPP mobile access
- Digest authentication – used by Telecoms & Internet converged Services & Protocols for Advanced Networks (TISPAN) and PacketCable
- Network Attachment Sub-System (NASS) - IMS bundled authentication – used by TISPAN
- Digest authentication with Transport Layer Security (TLS) (server side certificates) – used by PacketCable

Those solutions can be divided into two groups. First group consists of Early IMS (mobile) and NASS-IMS bundled authentication (fixed). They implement absolutely no IMS security features, however their IMS users are authenticated by underlying access network authentication and their identity and their IP address are sent to IMS network as the proof of authentication. Both solutions assume anti-spoofing mechanisms in access networks while forging of IP address would lead to forged identity in IMS network. The security level of IMS network corresponds to the security level of underlying access network.

The second group consists of Digest authentication with and without TLS (fixed). Digest access authentication is password based identification method that allows secure user identification without sending password in plaintext over the network. TLS is based on Secure Sockets Layer (SSL) and provides data integrity and confidentiality for reliable connection (Transmission Control Protocol (TCP)).

V. ACCESS SECURITY THREATS

Differences between IMS AKA and pre-IMS AKA solutions are reflected on IMS access security features: user-network authentication and IMS signaling protection (confidentiality and integrity).

Both NASS-IMS bundled authentication and Early IMS provide level of authentication security identical to level of corresponding authentication in access network but apparently they have no method for protection of IMS signaling due to lack of encryption methods. However, if connection between UE and the IMS network resides within the operator boundaries there should be no possibility for fraudulent party to intercept IMS signaling messages. Even if that would be the case, anti-spoofing mechanisms and access security that reside in access network prevent illegitimate access to the IMS services.

Digest authentication has two security issues:

- protection of IMS signaling
- protection of UE data

Digest authentication does not protect IMS signaling. Digest authentication uses Message-Digest algorithm 5 (MD5) cryptographic hashing algorithm together with nonce values to prevent cryptanalysis. It should be difficult to determine original secret input key value by knowing only algorithm output value. However attacker may try to test large set of inputs (dictionary or some other suitable list) with brute force attacks in order to find a matching output. If user password is too simple then attacker has a good chance to find it.

Digest authentication does not rely on use of smart cards for tamper-proof storage of user password. It is up to user to remember the password and so if users are given a chance to set password they tend to produce simple ones that will be easy to remember. This gives brute-force attacks a higher chance for success.

In order to prevent attacker to discover different parameters required for brute-force attack IMS signaling traffic must be protected. Digest authentication should be coupled with TLS to provide security for IMS signaling traffic.

User data must be protected at user equipment. Digest authentication requires user password. Password may be requested from the user every time, or it may be saved by softclient for future authentication requests.

When user types a password at softclient there are few security risks to be considered:

- software or hardware keyloggers
- person or a video recording device witnessing password typing
- keeping notes with complex (secure) passwords near by the computer

For password saved within softclient secure data must be protected from disclosure, modification or cloning to another computer by illegitimate person or malicious software.

Any of listed secure threats could lead to stolen credentials and illegitimate usage of IMS services.

VI. FRAUD VIABILITY

Security issues that have emerged with pre-IMS AKA access security solutions are tied to user equipment. UE based frauds lead to illegitimate use of IMS services with stolen credentials.

To become a serious threat such frauds must fulfill a few requirements:

- It must pay off. Gain should be higher then the total cost including risk of being caught.
- It must be simple. Complexity deters.
- It must be hard to detect
- If detected, the fraud's anonymity should be intact

A. Freud detection

One well-known telephony fraud was credentials stealing in NMT mobile network. Innocent user would not be aware of stolen identity up to the arrival of the monthly telephony bill.

In GSM and UMTS mobile networks user identity is firmly tied to UICC with security SIM / USIM application. To steal credentials, a fraud would first need to steel UE and user would soon realize that the mobile phone is missing.

There are two types of IMS clients. The first group stores security data onto UICC (smart card) that is inserted into UE. Secure data is not known to the user but resides in ISIM application on the smart card. Again, in case of stolen UE subscriber might notice missing equipment. Unlike stolen mobile phone IMS UE might be any kind of devices and that would make detection somehow more difficult.

Second group of IMS clients are not capable of using smart card as identification device (there is no ISIM/USIM application for security services and storage of long term secret key) but they rely on user knowledge of secret keys as identification method. That implies that whoever has knowledge of the secret keys can represent itself to the IMS network as the valid IMS client. SIP forking functionality enables user to be registered to IMS network with multiple contacts/terminals. So if the secret key is stolen and illegitimately used for access to IMS services the innocent user will have no indication of such actions. There are however two indications that something is wrong. If illegitimate user is being called by someone all IMS clients with the innocent user identity will be notified (ringing). Short ringing that stops without user answering the call or frequent “accidental” calls by unknown people are an indication of an invisible illegitimate user (with monthly bill as well).

B. Fraudulent user anonymity

Plain old telephony service (POTS) requires no user authentication. Operator identifies POTS user by end of twisted pair physical connection that connects the user with the operator. Access to the physical connection anywhere between the user and the operator allows illegitimate service usage.

Internet providers enforce user authentication due to charging and legal data retention requirements. User name and password are required in wireline networks for connection to Internet.

There is an apparent possibility for anonymous Internet modem connection when Internet providers allow Internet modem access by providing some publicly known username and password. However the user identity is revealed from identity of associated telephony user. That could be avoided by using a public payphone with help of acoustic coupler. Anonymous Internet access may be achieved with combination of fraudulent POTS usage of innocent user telephony line and Internet modem access as anonymous user.

In mobile networks, explicit user authentication for Internet connection is usually not required since users are already authenticated in the underlying mobile network. However prepaid mobile phone users can connect to the Internet and their identification is usually not checked at purchase of mobile phone.

Free Internet connection can be found in hotels, airports and coffee shops at WLAN hot spots.

Asymmetric Digital Subscriber Line (ADSL) access devices with integrated WLAN are gaining popularity due to ease of use and commodity of wireless access. The usual security problem is unconfigured WLAN access protection. With flat-rate Internet charges, innocent users are not aware of Internet connection illegitimate usage.

VII. PROTECTION MEASURES

IMS network protection measures:

- Number of contacts that a user may have registered should be set to 1. User credentials therefore could not be reused.
- TLS should be enabled
- Enforce longer passwords

IMS client protection measures:

- Password should be entered only once and locally stored by softclient – practical handling of long (strong) passwords; avoids keylogging threats
- Access to user data in softclient should be protected by password
- User data stored by softclient should be encrypted
- Encrypted user data file should contain computer specific data that could be used for computer identification to prevent usage of encrypted data file on another machine
- Operators should enforce usage of only specific securely approved softclients

VIII. SOFTPHONE SECURITY TEST

A few IMS softphone clients on Microsoft Windows platform were tested for UE data security. An assumption was that clients were designed to withstand exposure to various types of malicious software. Thus there were no expectations that simple security challenges to UE data would gain any success.

Following security problems were detected at various IMS softphones:

- exposure to keyloggers: user is forced to enter Digest password at every softphone startup
- unprotected access to user data: no password has been required for access to subscriber data in the softphone via softphone graphical user interface
- disclosure of password from client's shadowed password field
- credentials transfer: user data that resides in encrypted softphone configuration files can be copied to different computer and reused by identical IMS client without client configuration

Publicly available Revelation software has been used to reveal passwords from password fields disguised with asterisks. The program was run directly from USB stick.

IX. CONCLUSION

Use of IMS software clients with Digest authentication represents the biggest security risk among pre-IMS AKA access security solutions.

Crucial departure from standard IMS AKA solution in Digest authentication solution is replacement of temper free ISIM/USIM smart cards with error prone human/software client combination.

To compensate that newly introduced security threat special attention must be paid to security audit of IMS software clients.

REFERENCES

[1] RFC 3261 - “SIP: Session Initiation Protocol”

[2] 3GPP TS 23.228 - “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2”

[3] 3GPP TS 33.203 - “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G security; Access security for IP-based services”

[4] 3GPP TR 33.978 - “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security aspects of early IP Multimedia Subsystem (IMS)”

[5] 3GPP TS 21.133 - “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements”

[6] M. Hunter, R. Clark, F. Park (2007). "Security Issues with the IP Multimedia Subsystem (IMS): A White Paper".

[7] Bellovin, Steven M. (1996). "Problem Areas for the IP Security Protocols". Proceedings of the Sixth Usenix Unix Security Symposium: 1-16.

[8] Wardriving - http://en.wikipedia.org/wiki/Wardriving

[9] Script kiddie - http://en.wikipedia.org/wiki/Script_kiddie

[10] monitoring and spy tools - http://www.keyloggers.com/bigbrother.html

[11] Comparison of VoIP software - http://en.wikipedia.org/wiki/Comparison_of_VoIP_software

[12] SnadBoySoftware - Revelation - http://www.snadboy.com/