Implications of Unlicensed Mobile Access (UMA) for GSM security

Sandro Grech*
Nokia Networks
sandro.grech@nokia.com

Pasi Eronen
Nokia Research Center
pasi.eronen@nokia.com

Abstract

Despite its imperfections, GSM security has stood well the test of time. In part, this security success has relied on closed platforms that prevent the end-user from tampering with the GSM protocol stacks. While it is possible to build phones that do not have such restrictions, this is difficult due to, e.g., legislation and technical complexity.

Unlicensed Mobile Access (UMA) is a new technology that provides access to GSM services over Wireless LAN or Bluetooth. It also challenges the assumption of closed platforms, since it is relatively easy to implement a UMA phone purely in software running on standard PC hardware and operating systems.

This paper examines the security implications of UMA for GSM security, focusing especially on the impact of open terminal platforms. We identify several areas where open platforms may increase risks to both honest users and network operators, and propose countermeasures for mitigating these risks.

1. Introduction

Mobile phones have become ubiquitous in many countries during the past decade. However, in some countries, such as the United States, it has turned out to be difficult to support adequate indoor coverage using cellular systems [39]. In response to this shortcoming, several industry players have formed a consortium to specify access to GSM and GPRS services over unlicensed radio technologies, such as Bluetooth and IEEE 802.11 Wireless LANs. The specifications resulting from the Unlicensed Mobile Access (UMA) consortium have been recently published [45, 44, 46], and deployment of the first commercial systems based on these specifications is expected shortly. The standardization work is continued by the 3rd Generation Partnership Project (3GPP) under the "generic access to the A/Gb interface" work item [6, 11, 10].

*Also with Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory

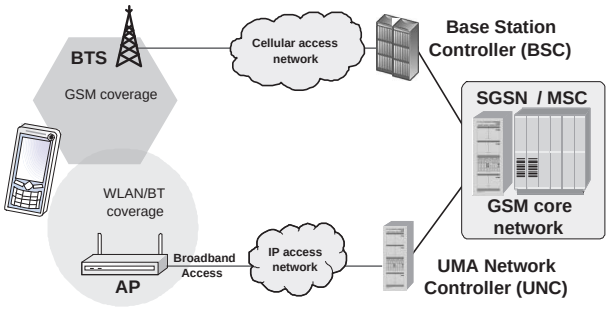

Figure 1. The UMA solution

Fig. 1 illustrates the basic principle behind the UMA solution. The existing cellular network remains unmodified, and a new network element, the UMA Network Controller (UNC), is introduced. UNC acts as a gateway between the mobile operator core network and Internet or a broadband IP access network such as ADSL or cable. The phone connects to the IP network using a standard WLAN or Bluetooth access point.

Since the GSM/GPRS core network remains unchanged, UMA can reuse many of the existing GSM security mechanisms; new mechanisms are defined only for protecting the communication between the phone and UNC.

In general, GSM security can be called a success story: subscribers do not get charged for calls they did not make, but get charged for calls they do make; eavesdropping is sufficiently difficult; and perhaps most importantly, security is mostly invisible to users and does not depend on the user always making the right choices (unlike on the Internet, for instance).

This success has not been due to exceptionally good technical security mechanisms or cryptographic algorithms (which turned out to be quite weak), but rather applying both non-technical and technical mechanisms in a particular usage environment. One important aspect of this environment has been the mobile phone that is practically always a closed (or semi-closed) platform that does not allow the

user, either deliberately or inadvertently, to tamper with the GSM protocol stacks or main phone functions dealing with the GSM/GPRS services.

While it is naturally possible to build GSM phones that do not have such restrictions, in practice they are rare due to several different reasons. 3GPP specifications require that changing the International Mobile Equipment Identity (IMEI) code of the phone must be sufficiently difficult: this implies that modifying the GSM stacks that handle the IMEI must be difficult as well [3]. These requirements may be further enforced by legislation related to conformance and type approval for radio and telecommunications equipment. The technical complexity involved with the radio frequency parts also puts this kind of project beyond the skills of most hobbyists.

It is expected that the first UMA-capable phones will be based on current GSM phones and closed platforms. However, it is possible to implement a WLAN/Bluetooth-only UMA phone, without the GSM radio parts, purely in software running on standard PC hardware and operating systems. Unlike building an ordinary GSM phone, this task is clearly within the capabilities of many hobbyists, and it is not totally clear what legislation would apply to such software.

The goal of this paper is to study the security implications of UMA for the security of the GSM system, focusing especially on the possibility of open terminal platforms.

We start by reviewing the GSM and GPRS security foundations in Section 2. The UMA security architecture as specified by the UMA consortium is then introduced in Section 3. The feasibility and the potential forms of open UMA terminal implementations is studied in Section 4. This is followed by Section 5 which provides a security analysis of GSM/GPRS mobile communication system in light of potentially malicious open mobile terminal implementations, and Section 6 which presents possible protection mechanisms. Related work is discussed in Section 7, and finally, Section 8 summarizes the conclusions of our analysis.

2. Background: GSM and GPRS security

GSM and GPRS security is covered extensively in literature such as [36] or [2]. The most important security features in GSM and GPRS systems can be summarized as follows:

- *authentication of the user* is based on a permanent subscriber-specific secret key, which is stored at the Authentication Centre and in the user's Subscriber Identity Module (SIM), a tamper-resistant smart card.

- *encryption over the radio interface* is achieved by applying a stream cipher keyed by a secret session key which is generated during the authentication procedure.

- *temporary identities* are used to protect subscriber location privacy by limiting the number of occasions when the permanent identity of the subscriber, the International Mobile Subscriber Identity (IMSI), needs to be sent out over the air unencrypted.

- *equipment identities* are used to prevent the use of stolen phones, or phones with severe malfunctions.

These mechanisms, especially the cryptographic algorithms used, have their own weaknesses, which are also covered widely in the literature (see, e.g., [16, 18, 38, 19]). However, attacks against the GSM radio interface are beyond the scope of this paper.

The security mechanisms described above also rely on non-cryptographic properties, and in particular, on having phones that can be trusted by non-malicious users, and cannot be too easily tampered by malicious users. For instance, although user authentication uses a tamper-resistant smart card—making it uneconomical to extract the secret key—an attacker who is able to install malicious software with unlimited capabilities on the user's terminal could still make calls that get charged to the victim. Similarly, the equipment identities rely completely on tamper resistant terminals: there is no secret key associated with the IMEI that could be used to prove that the terminal is really sending the correct equipment identity.

3. Unlicensed Mobile Access (UMA) overview

As described in Section 1, UMA does not introduce any changes to the existing cellular network. The new network element, UMA Network Controller (UNC) acts as a gateway between the IP side (typically consisting of a customer-owned WLAN access point and an ADSL/cable based broadband access network) and the cellular core network. The UNC is connected to the core network using the same A/Gb interface as GSM base station controllers (BSCs).

The user and control plane protocol stacks for circuit switched services are shown in Fig. 2 and Fig. 3. The shaded protocol layers represent protocols defined in [44] and [46]. The remaining protocol layers are unmodified protocols defined in 3GPP Release 4 and IETF specifications.

The protocol stacks resemble traditional voice-over-IP solutions, except that GSM signaling protocols are used instead of SIP or H.323. Another difference is that there is no direct terminal-to-terminal IP connectivity even when both parties use UMA: the user plane traffic always goes through the GSM core network. The main advantages of using the

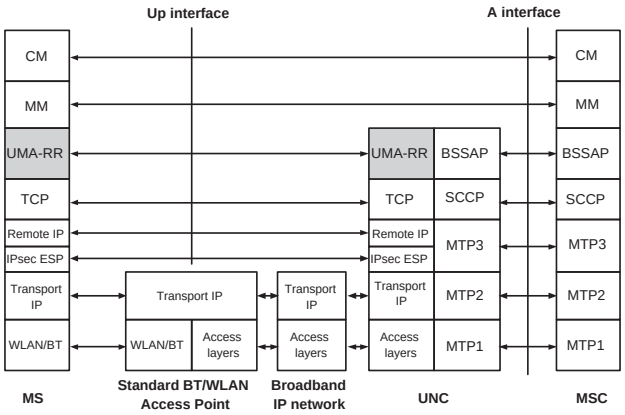

Figure 2. UMA circuit switched control plane protocol architecture (figure based on [44])

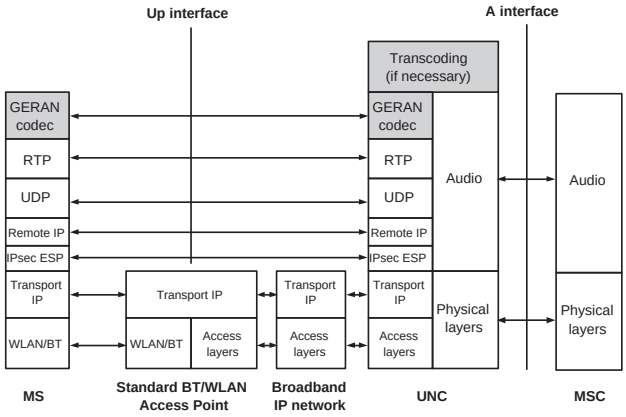

Figure 3. UMA circuit switched user plane protocol architecture (figure based on [44])

existing GSM protocols and services are easier deployment (for existing GSM operators) and the ability to do handovers between GSM and UMA during a call.

UMA also supports access to GPRS packet switched services. The protocol stacks are similar as for circuit switched case, replacing the lower layers from GPRS radio with IP.

The security requirements for UMA are described in [45]. The most important requirements in the scope of this paper are summarized below.

- *General:* unlicensed access shall not compromise the security of GSM and GPRS networks.
- *Authentication:* bilateral authentication between mobile station and UNC shall be supported.
- *Encryption:* signaling traffic shall be secured end-to-end (terminal to UNC) to protect subscriber data. UMA shall provide security at least as good as GSM/GPRS for all traffic between mobile station and UNC.

The resulting security architecture and protocols are specified in [44] and [46], respectively. Fig. 4 illustrates the constituent security mechanisms on which the UMA security architecture is based. The UMA specifications define the security for the Up interface between the terminal and the UNC. The specification of the other security layers shown in Fig. 4 is outside the scope of UMA, and are handled elsewhere, for example in IEEE, 3GPP and IETF.

Traffic between the phone and the UNC is protected by an IPsec ESP tunnel, which is established and maintained using IKEv2 [31]. The subscriber is authenticated using EAP-SIM [26], which is based on the SIM authentication

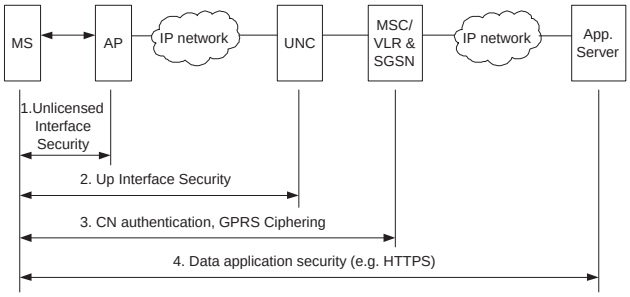

Figure 4. UMA security mechanisms (figure based on [44])

procedures exchanged within the IETF Extensible Authentication Protocol (EAP) framework [12]. Authentication of the UNC to the phone is based on X.509 certificates and, implicitly, on producing correct EAP-SIM requests.

The authentication between the phone and UNC does not replace the normal GSM authentication between the phone and the MSC. The keys resulting from the phone-to-MSC authentication exchange are also used in a UMA-specific challenge-response handshake between the phone and the UNC (see [44, 46] for details).

4. UMA and the rise of open mobile terminals

Current GSM/GPRS mobile terminal implementations are reasonably trustworthy, because even in open platforms like Symbian, curious (or malicious) users cannot easily tamper with the GSM/GPRS stacks. The terminal model implicitly assumed by the UMA consortium is that the ter-

minals will consist of dual-mode devices that can utilize both cellular and unlicensed access methods. With UMA, however, writing an open "UMA phone" implementation on top of a suitable platform such as a laptop equipped with an Internet connection and a smart card reader will become considerably easier.

In the context of this paper, an open mobile terminal is defined as a device that can communicate in a GSM/GPRS network by running the UMA protocol stack, or a part thereof, on top of readily available hardware and operating systems. For circuit switched communication, the software part consists of an implementation of UMA-RR [46], GSM-MM [7], and GSM-CM [7] protocols together with the necessary GERAN audio codecs [9] and Internet protocols as required by [44, 46]. For packet switched communication, the software includes GPRS-SNDCP [8], GPRS-LLC [5], UMA-RLC [46], and GPRS-GMM/SM [7] protocols.

Different types of terminal implementations falling under this definition may materialize in practice. Possible variants of the software-side may include:

1. Commercial software distributions with no malicious intention neither by the developers nor by the users. These implementations may be unwelcome by operators since they are beyond any operator control, compared to current terminal implementations that offer at least some level of type-approval. In addition, these implementations may include genuine bugs that could lead the network to encounter error cases that would not be encountered otherwise.

2. Free software distributions with no malicious intention by the developers, but allowing enough freedom to users to manipulate the behavior of the terminal, possibly including terminal behavior that would otherwise not be permitted in the mobile network, or even worse, causing intentional harm to the network (including other users).

3. Commercial or free software distributions with malicious intention by the developers. In this case, the users themselves may become the victims, for example through some backdoor or intentionally placed buffer overflow that allows unauthorized access to the mobile device and/or the SIM card.

The implications of these mobile terminal variants on the overall network security will be analyzed next.

5. Security analysis

The following sections will discuss these threats in light of the various software terminal implementations identified in Section 4.

5.1. Unauthorized access and identity spoofing

As described in Section 3, users connecting to the UNC are authenticated using EAP-SIM inside IKEv2, and to the GSM/GPRS core network using normal SIM authentication procedures. A potential attacker needs to have access to a valid SIM card that maps to a valid subscription. Thus, attackers cannot gain unauthorized access or spoof their identity simply by tampering with the protocol implementations of their own terminals.

However, the use of open platforms make it easier to insert malicious software in the terminals of honest users. Attackers could, for instance, distribute a virus or Trojan horse that communicates directly with the SIM card, and thus can hijack the victim's identity and subscription. While these kinds of attacks are possible and common on the current Internet, in GSM/GPRS networks the consequences could be much worse, since the victim ends up paying for calls made by the attacker. Furthermore, these calls could be made to expensive toll numbers, similar as "dialer" malware on the Internet [40].

Another possible attack vector is offered by the Bluetooth SIM access profile [20], which allows other Bluetooth devices to access the phone's SIM card. In this case, the phone itself does not need to be compromised: the virus or Trojan horse can access the phone from the victim's PC, provided that the laptop is paired with the phone, the SIM card does not require entering a PIN code when powered on (or the PIN is guessable), and the phone does not require explicit authorization every time the Bluetooth connection is used (which is probably the case if the victim actually uses the Bluetooth features often). This attack scenario is illustrated in Fig. 5.

5.2. Exploitation of implementation weaknesses

A second type of attack may result from the fact that UMA exposes certain network elements and protocol layers[1] whose access was previously restricted to terminals that were reasonably well designed and implemented, and resistant to tampering by users. Thus, the network side implementations did not have to be designed for a hostile environment where users may intentionally provide malformed inputs or otherwise violate the protocol specifications.

For instance, buffer overflows have been the most common form of security vulnerability in the past decade [23], and there is no reason to assume that any software this complex would be totally free from such problems.

So far, attacks leveraging implementation weaknesses in GSM/GPRS network elements have been limited to GPRS, where malformed inputs can be generated using a PC. For

[1] more specifically, GSM-MM, GSM-CM, GERAN codec, GPRS-GMM/SM, GPRS-LLC and GPRS-SNDCP

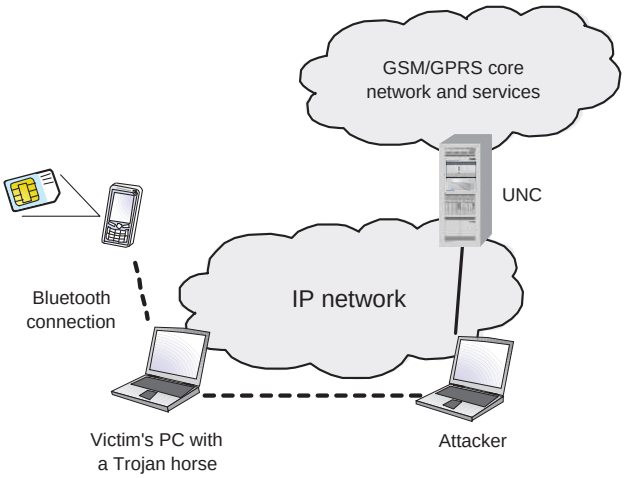

Figure 5. A Trojan horse in the victim's PC can access the phone and SIM card over Bluetooth.

instance, in [50] the authors report that a commercial GGSN could be crashed by sending a malformed IP packet from a PC, using a GPRS-enabled phone as a modem. With UMA, a software implementation could be modified to send malformed inputs and thus try to find implementation vulnerabilities in the network.

5.3. Denial of service

Denial of service (DoS) [35] refers to the prevention of authorized access to resources or delaying of time-critical operations [30]. This is typically performed by causing exhaustion of storage space, network bandwidth, computational or other resources necessary for the service availability. The source of the attacks can either be a single device—typically using a spoofed identity—or multiple devices, typically compromised by an attacker. The latter type of attack is generally referred to as distributed denial of service attack [17, 32].

As an example of the latter, if distributed widely enough, an attacker may include flooding agents in his software distribution, which can be later used to launch distributed denial of service attacks against the network. This particularly relevant in light of the fact that the attack agents can reside behind broadband connections, whereas most of the legitimate users are connected through low bandwidth cellular links. On the other hand it should also be noted that a potential attacker will face practical difficulties in distributing attack agents to victims that all share the same operator when attempting to launch distributed denial of service attacks. In contrast, most of the successful distributed denial of service attacks in the Internet have been targeted against globally reachable network entities such as web servers offering a public service.

A practical example of a potential form of distributed denial of service attack can be presented with reference to the GPRS PDP context activation procedure as illustrated in Fig. 6. This constitutes one of the GPRS-GMM/SM procedures defined in [7] and is used to establish a GPRS connection. Step 2 in Fig. 6 corresponds to the user authentication procedure outlined in section 2. This procedure involves verification of the SIM credentials through signaling between the SIM card and the HLR. Most importantly in the context of this discussion, steps 4 and 6 are stateful procedures. Backed by the common practice of pricing GGSN software licenses based on the number of supported active PDP contexts, an attacker could exhaust the effective network capacity by issuing a flood of PDP context request messages, either from a single or multiple devices.

Attacks based on resource exhaustion have been recognized earlier in the fixed Internet and the technique has been used for example to mount the widely publicized TCP SYN flood attacks [41]. In principle, any protocol where the server commits to extensive computations or to memory allocation prior to, or as part of client authentication, is vulnerable to denial of service attacks [33]. In the context of this paper, we argue that denial of service through resource exhaustion is also possible after a successful client authentication procedure. The GSM/GPRS authentication procedure verifies that the supplicant has a valid service subscription, but a successful authentication procedure does not imply that the user behind the device, or the device itself will not try to compromise the network. An attacker using a prepaid subscription is very difficult to trace. An attacker could also be masquerading behind a victim's compromised device, which in turn authenticates itself to the network transparently from the victim.

5.4. Eavesdropping

UMA requires traffic between the mobile terminal and UNC to be protected using IPsec. This will prevent even curious users who have the capability to tamper with their terminal protocol stacks from eavesdropping other users' communication. However, it should be noted that the UMA specifications [44] state that it is possible to use NULL encryption for the IPsec tunnel, for example in cases where high trust exists between the UMA operator and the access network provider.

This exception is however based on a dangerous assumption. Trust between an UMA operator and an access network provider does not imply by any means that subscribers in an access network provider trust each other. For exam-

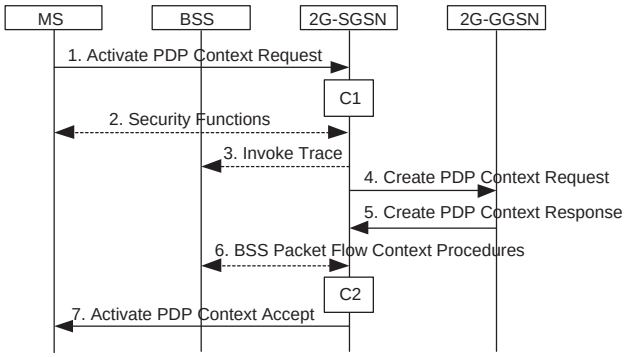

Figure 6. GPRS PDP context activation procedure (figure based on [4])

ple, communications from a subscriber connected through a WLAN link that uses weak security mechanisms is subject to eavesdropping from an attacker that resides within range of the WLAN link. In order to support the consumer's legacy WLAN equipment, the UMA specifications do not make any normative requirements on the security capabilities of the WLAN equipment. In addition, since operators do not necessarily have control on the subscribers' WLAN equipment, it is difficult to ensure that the recommended policies are conformed to. Consequently, operators should be very cautions when opting to use null encryption for the IPsec tunnel, thereby assuming confidentiality is accounted for at the lower layers.

Finally, it should be noted that a victim using a compromised terminal implementation does not have any guarantees of being protected from attacks against confidentiality of his communication, since the compromised implementation could send an unencrypted copy of the communication to the attacker.

5.5. Location spoofing

When the connection between the phone and UNC is set up, the phone sends its current (or last known) GSM location (cell identity), and the MAC address of the WLAN/Bluetooth access point to the UNC. These values can be used by the operator for several different purposes:

- The operator can prevent the use of UMA while roaming, or limit UMA access to certain locations (such as the subscriber's home).
- The connection can be redirected to another UNC. For instance, roaming agreements between operators could require that when the user is physically within the visited operator's area, the visited network's UNC should be used. This could imply that the user pays higher fees due to roaming.
- Location-based services provide different service based on the subscriber's location, and can be restricted to certain locations.
- Lawful interception can be based on the terminal's current location [1].

Since the values are provided solely by the terminal, a custom implementation could easily send incorrect values. This could be used to circumvent usage limits, avoid paying roaming charges, or mislead location-based services. It is worth noting that even non-malicious users may have an incentive to circumvent some of these restrictions.

6. Protection against the attacks

The potential attacks identified in the previous section fall roughly under two categories: either an attacker modifies his or her own terminal to, e.g., send malicious inputs, or an attacker compromises a victim's terminal through a virus or Trojan horse.

Potential countermeasures against these attacks include the following.

- Protecting non-malicious users' terminals
- Technical prevention of unapproved terminals
- Legal prevention of unapproved terminals
- Detecting and disabling misbehaving terminals
- Increasing core network resistance to attacks

6.1. Protecting non-malicious users' terminals

Most current mobile phones allow users install additional applications in the phone. Mostly these are written in Java, which prevents the applications from accessing the most sensive parts of the phone, such as the SIM card or the internals of the GSM protocol stacks. Some phones do allow users to download native binary applications, and may not contain effective mechanisms to limit their privileges. However, these phones are so far not very widespread, and manufacturers are introducing enhanced security mechanisms that are intended to limit the harm a downloaded Trojan horse could do (e.g., [42]).

On typical PC platforms, downloaded binary code typically runs with the same privileges as most other applications, and the focus is thus in detecting malware rather than limiting the damage. Approaches familiar from PCs, such as anti-virus and anti-spyware programs, may be applicable

for phones as well if using prevention mechanisms alone proves insufficient.

However, there is clearly a trade-off between making terminals as secure as possible, and allowing users to download and run useful applications that may legitimately need access to sensitive resources. Some people have expressed worries that, e.g., requiring approval procedures for all applications would cancel many of the benefits of having an open platform [34]—just think how popular PCs would be if they only ran Microsoft-approved software.

6.2. Technical prevention of unapproved terminals

One effective way to protect against many of the potential attacks covered in this paper is to limit access to the network only to operator-approved terminals. As described in Section 2, the current IMEI mechanism is not secure enough for this purpose, since it blindly assumes that terminals send the correct IMEI.

There have been proposals for introducing a more secure terminal identity that would include a secret key embedded in tamper resistant hardware. However, none of these proposals have materialized into specifications. An overview and discussion of some of these proposals is included in [14].

One reason for this may be associated with the fact that it is difficult, if not practically impossible, to introduce a tamper resistant mechanism while being backward compatible with devices that are only capable of supporting the current basic terminal identity based on IMEI. With UMA, the situation is different, however, since to-date there are no UMA terminals on the market yet. Consequently it would be possible to mandate that all terminals connecting to a network operator using UMA would need to implement more robust mechanisms in order to allow the operator to verify the terminal identity and deny access to any terminal which may potentially compromise the security of the system.

Adopting a secure equipment identity does not necessarily rule out UMA clients running on PCs. Although the efforts of, e.g., the Trusted Computing Group (TCG), have been so far motivated mainly by media industry concerns, the remote attestation mechanisms could also prove that a PC is running UMA software that has been approved by the operator and has not been tampered with.

It is also worth noting that while a secure equipment identity relies on tamper resistant hardware, it does not completely lose its usefulness if an attacker manages to extract the private key from his or her terminal. The attacker can use the private key with a malicious software implementation, but if some misbehavior is detected, it is possible to place this IMEI on a black list. The attacker can, of course, repeat the same attack using a new terminal, but at least this places a certain cost on the attack.

6.3. Legal prevention of unapproved terminals

Unapproved terminals can also be discouraged using legal means. This cannot prevent a malicious individual or group from making a terminal, but it will at least limit their commercial distribution.

Most countries have some legislation about telecommunications terminal equipment (e.g., [24]), but it is not clear how these laws would apply to software-only UMA implementations. Some countries explicitly prohibit tampering with mobile terminal identities [43], and a software implementation that uses the equipment identity of some other terminal may violate these laws.

Another part of legislation that has been used to prevent user modifiable terminals is intellectual property rights. For instance, patent license agreements prohibit manufacturers from making DVD players that users can too easily tamper with, or have certain features deemed undesirable, such as high-quality RGB outputs or a working fast forward button [25, 27]. Cellular technologies are covered by a large number of patents as well, and license agreements could require, for instance, following the relevant 3GPP security specifications.

6.4. Increasing core network resistance to attacks

While making it difficult to launch attacks against the core network can play a part in securing the system, it cannot be assumed that such efforts will be totally successful. Therefore, the network elements have to be prepared to deal with malformed inputs and clients that do not follow the protocol specifications. In general, this means applying well-known guidelines for writing secure software (e.g., [48]).

In addition, network elements must be able to cope with potential denial of service attacks. This implies minimizing the resources used before the subscriber is authenticated, and after authentication, ensuring that a single subscriber does not receive an unfair share of the resources. For instance, the IPsec part in UNC can perform traffic shaping that limits each subscriber to, say, 50 kbps, which is sufficient for a voice call.

Dealing with denial of service attacks prior and during authentication is more difficult. IKEv2 includes a feature called “cookies” that is intended to make certain denial-of-service attacks with spoofed IP addresses more difficult. Once the source IP address is known with some degree of certainty, the UNC could throttle the number of connection attempts from a particular IP address, making a DoS attack against EAP-SIM authentication procedure and HLR more difficult.

It is worth noting that none of these countermeasures prevents an attacker from simply flooding the UNC’s net-

work connection with traffic—which is exactly what most distributed denial of service attacks on the Internet do [17]. However, protection against this type of attack is beyond the scope of this paper.

6.5. Detecting and disabling misbehaving terminals

While it is important that UMA networks are able to deal with, e.g., malformed inputs, UMA has an important advantage compared to the Internet. Very little communication occurs before authentication, and thus attacks and suspicious activities, such as searching for vulnerabilities, can be traced to individual subscriptions. This allows the operator to, e.g., terminate the subscription, and at least with postpaid subscriptions, hold the subscriber accountable for the actions.

There is also ongoing work in 3GPP that aims to selectively disable certain functions for misbehaving users, instead of closing the subscription completely [37, 49]. These features are expected to be especially useful if the terminal is compromised, and thus the subscriber is not the actual attacker.

Currently this work does not address exactly how misbehavior would be detected, since this part does not need to be standardized. One possibility would be to include intrusion detection features in the UNC for detecting when, e.g., the user is attempting to find exploitable vulnerabilities by sending malformed inputs.

7. Discussion and related work

The model developed by the UMA consortium is not the only emerging network convergence model; however, it is the only one that has focused primarily on integrating existing mobile phone circuit-switched services with unlicensed access technologies. 3GPP WLAN interworking model [13] focused primarily on packet-switched data services. In addition the Telecommunications Standardization Sector of the International Telecommunications Union (ITU-T) has recently launched a task force for specifying the Next Generation Network (NGN) concept [22], with the aim of facilitating the network and service convergence for fixed and mobile networks.

The common denominator between all of these convergence models is that they open the mobile network and its services to non-cellular domains and non-cellular terminals. 3GPP has recently started work on trust requirements for such open platforms [29, 28]. Currently the discussion is focusing on various “trusted computing” efforts; however, these proposals are somewhat controversial (see, e.g., Ross Anderson’s arguments against them in [15]) and it is not clear how successful they will be on PCs.

There are some non-PC devices that already include secure equipment identities. For instance, some cable devices conforming to the CableLabs specifications [21] include a private RSA key and a certificate from the manufacturer. Even if an attacker could recover the key from the tamper-resistant module, detecting misbehavior would allow denying access to this device. There have been proposals for adding similar functionality to IEEE 802 devices as well [47].

8. Conclusions

UMA provides access to existing GSM/GPRS services over unlicensed radio technologies. What makes UMA different from many other convergence proposals is that it reuses existing specifications and network elements that were designed in a time when closed terminal platforms was a reasonable assumption. In this paper, we have identified attacks that become possible when this assumption no longer holds, and proposed several countermeasures against them.

The most effective countermeasures involve allowing access only to operator-approved terminals. This is a somewhat unfortunate and controversial conclusion, since open platforms also have many important benefits for innovation and ability to provide the services users want also in the future. It is also a proposal that is difficult to implement in a way that would be compatible with existing terminals, and it is not expected that the first UMA phones would have such features. Therefore, other suggestions given in Section 6, especially increasing the core network’s resistance to attacks, and the ability to detect misbehavior, are also important.

There are also several aspects of UMA security that were not addressed in this study. Since the UMA specifications have been published only recently, it is possible that they contain problems with potential security implications. Even the GSM specifications, which have been around for a long time, have not necessarily considered an authenticated but malicious subscriber who may, for instance, mount a denial-of-service attack. Future work is also required to determine the security impact of UMA in roaming situations, to identify better countermeasures against denial-of-service attacks, and to investigate mechanisms for detecting misbehavior and fraud.

9. Acknowledgement

The authors would like to thank N. Asokan, Dan Forsberg, Minna Kangasluoma, Pasi Kovanen, Tomi Mikkonen, Valtteri Niemi, and Kaisa Nyberg for their comments on earlier versions of this paper.

References

[1] 3rd Generation Partnership Project (3GPP). Lawful Interception Requirements. Release 4, TS 33.106 V4.0.0, Mar. 2000.

[2] 3rd Generation Partnership Project (3GPP). Security related network functions. Release 4, TS 43.020 V4.0.0, Nov. 2000.

[3] 3rd Generation Partnership Project (3GPP). International Mobile station Equipment Identities (IMEI). Release 4, TS 22.016 V4.2.1, June 2002.

[4] 3rd Generation Partnership Project (3GPP). General Packet Radio Service (GPRS) Service description; Stage 2. Release 4, TS 23.060 V4.9.0, Dec. 2003.

[5] 3rd Generation Partnership Project (3GPP). Mobile Station – Serving GPRS Support Node (MS–SGSN) Logical Link Control (LLC) layer specification. Release 4, TS 44.064 V4.3.0, Mar. 2003.

[6] 3rd Generation Partnership Project (3GPP). Feasibility Study on Generic Access to A/Gb Interface. TR 43.901, Aug. 2004.

[7] 3rd Generation Partnership Project (3GPP). Mobile radio interface Layer 3 specification; Core network protocols; Stage 3. Release 4, TS 24.008 V4.14.0, June 2004.

[8] 3rd Generation Partnership Project (3GPP). Mobile Station (MS) – Serving GPRS Support Node (SGSN) Subnetwork Dependent Convergence Protocol (SNDCP). Release 4, TS 44.065 V4.3.0, Sept. 2004.

[9] 3rd Generation Partnership Project (3GPP). Speech codec list for GSM and UMTS. Release 4, TS 26.103 V4.4.0, Dec. 2004.

[10] 3rd Generation Partnership Project (3GPP). Generic Access to the A/Gb interface; Mobile Generic Access Interface Layer 3 Specification. Work in progress, TS 44.318, Jan. 2005.

[11] 3rd Generation Partnership Project (3GPP). Generic Access to the A/Gb interface; Stage 2. Work in progress, TS 43.318, Jan. 2005.

[12] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz. Extensible Authentication Protocol (EAP). IETF RFC 3748, June 2004.

[13] K. Ahmavaara, H. Haverinen, and R. Pichna. Interworking architecture between 3GPP and WLAN systems. *IEEE Communications Magazine*, 41(11):74–81, Nov. 2003.

[14] A. Al-Adnani. Intermediate report on terminal security for UMTS. 4FP/ACTS USECA (UMTS Security Architecture) project deliverable D05, available from http://isrc.rhul.ac.uk/useca/Deliverables/D05.PDF, July 1999.

[15] R. Anderson. Trusted computing frequently asked questions. http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html, Mar. 2003.

[16] E. Barkan, E. Biham, and N. Keller. Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In *Advances in Cryptology – CRYPTO 2003*. Lecture Notes in Computer Science, vol. 2729, Springer, Aug. 2003.

[17] S. Bellovin. Distributed denial of service attacks. Available from http://www.research.att.com/~smb/talks, Feb. 2000.

[18] O. Benoit et al. Mobile terminal security. Report 2004/158, Cryptology ePrint Archive, http://eprint.iacr.org/2004/158, July 2004.

[19] A. Biryukov, A. Shamir, and D. Wagner. Real time cryptanalysis of A5/1 on a PC. In *Fast Software Encryption – 7th International Workshop*. Lecture Notes in Computer Science, vol. 1978, Springer, Apr. 2000.

[20] Bluetooth SIG. SIM Access Profile Interoperability Specification 0.95, Aug. 2002.

[21] CableLabs. Data-Over-Cable Service Interface Specifications (DOCSIS 1.1) Baseline Privacy Plus Interface Specification. SP-BPI+-I11-040407, Apr. 2004.

[22] J.-Y. Cochennec. Activities on next-generation networks under global information infrastructure in ITU-T. *IEEE Communications Magazine*, 40(7):98–101, July 2002.

[23] C. Cowan, F. Wagle, P. Calton, S. Beattie, and J. Walpole. Buffer overflows: attacks and defenses for the vulnerability of the decade. In *Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX '00)*, Jan. 2000.

[24] Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity. Available from http://europa.eu.int/comm/enterprise/rtte/dir99-5.htm, Mar. 1999.

[25] DVD Copy Control Association. CSS Technology License: Procedural Specifications. Version 2.6, available from http://www.dvdcca.org/, Jan. 2005.

[26] H. Haverinen and J. Salowey. Extensible Authentication Protocol method for GSM Subscriber Identity Modules (EAP-SIM). Work in progress, IETF draft-haverinen-pppext-eap-sim-16, Dec. 2004.

[27] G. Hinze. Exemption class 3 – DVDs with unskippable promotional material. Testimony at US Copyright Office hearings, http://www.eff.org/IP/DMCA/copyrightoffice/20030513_unskippable_dvd.php, May 2003.

[28] Intel. Trust Requirements for Open Platforms in WLAN-WWAN Interworking. 3GPP TSG SA3 working document S3-040480, available from http://www.3gpp.org/ftp/tsg_sa/, July 2004.

[29] Intel. WID for Trust Requirements for Open Platforms in 3GPP. 3GPP TSG SA3 working document S3-040843, available from http://www.3gpp.org/ftp/tsg_sa/, Oct. 2004.

[30] ISO 7498-2:1989. Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989.

[31] C. Kaufman. Internet Key Exchange (IKEv2) Protocol. Work in progress, IETF draft-ietf-ipsec-ikev2-17, Sept. 2004.

[32] F. Lau, S. H. Rubin, M. H. Smith, and L. Trajovic. Distributed denial of service attacks. In *IEEE International Conference on Systems, Man, and Cybernetics*, Nashville, TN, USA, Oct. 2000.

[33] J. Leiwo, P. Nikander, and T. Aura. Towards network denial of service resistant protocols. In *Proceedings of the Sixteenth Annual Working Conference on Information Security (SEC2000), IFIP Series*. Kluwer Academic Publishers, Aug. 2000.

[34] S. Litchfield. Hands off our smartphones! http://www.allaboutsymbian.com/features/viewarticle.php?id=145, Feb. 2005.

[35] P. G. Neumann. Inside risks: denial-of-service attacks. *Communications of the ACM*, 43(4):136–136, Apr. 2000.

[36] V. Niemi and K. Nyberg. *UMTS Security*. John Wiley & Sons, Nov. 2003.

[37] Nokia. Selective Disabling of UE Capabilities. 3GPP TSG SA3 working document S3-040873, available from http://www.3gpp.org/ftp/tsg_sa/, Oct. 2004.

[38] J. Rao, P. Rohatgi, H. Scherzer, and S. Tinguely. Partitioning attacks: Or how to rapidly clone some GSM cards. In *Proceedings of the 2002 IEEE Symposium on Security and Privacy*, May 2002.

[39] T. Rappaport, A. Annamalai, R. Buehrer, and W. Tranter. Wireless communications: past events and a future perspective. *IEEE Communications Magazine*, 40(5):148–161, May 2002.

[40] S. Saroiu, S. D. Gribble, and H. M. Levy. Measurement and analysis of spyware in a university environment. In *Proceedings of the 1st Symposium on Networked Systems Design and Implementation (NSDI)*, Mar. 2004.

[41] C. L. Schuba, I. V. Krsul, M. G. Kuhn, E. H. Spafford, A. Sundaram, and D. Zamboni. Analysis of a denial of service attack on TCP. In *Proceedings of the 1997 IEEE Symposium on Security and Privacy*, May 1997.

[42] Symbian. Platform security - a technical overview. Technical paper, available from http://www.symbian.com/developer/techlib/index.html, Feb. 2005.

[43] UK Legislation. Mobile telephones (re-programming) act 2002. Available from http://www.legislation.hmso.gov.uk/acts/acts2002/20020031.htm, July 2002.

[44] UMA Consortium. Unlicensed Mobile Access (UMA) Architecture (Stage 2). R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.

[45] UMA Consortium. Unlicensed Mobile Access (UMA) User Perspective (Stage 1). R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.

[46] UMA Consortium. Unlicensed Mobile Access (UMA) User Protocols (Stage 3). R1.0.0, Technical specification, available from http://www.umatechnology.org/specifications/index.htm, Sept. 2004.

[47] J. Viega. Proposal for device identification PAR. Presentation at IEEE 802.1 meeting, available from http://www.ieee802.org/1/files/public/docs2004/, Oct. 2004.

[48] J. Viega and G. McGraw. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley, 2001.

[49] Vodafone. Selective Disabling of UE Capabilities. 3GPP TSG SA1 working document S1-050081, available from http://www.3gpp.org/ftp/tsg_sa/, Jan. 2005.

[50] O. Whitehouse. GPRS wireless security: Not ready for prime time. Technical white paper, available from http://www.atstake.com/research/reports/, June 2002.