

Security Issues with the IP Multimedia Subsystem (IMS): A White Paper

Michael T. Hunter

Russell J. Clark

Frank S. Park

College of Computing
Georgia Institute of Technology
{frank,mhunter,russ.clark}@gatech.edu

Version 1.0
September 1, 2007

Abstract

The IP Multimedia Subsystem (IMS) is the basis for a significant new architecture for mobile applications incorporating voice, video and data services. The IMS is an overlay network on top of IP that uses SIP as the primary signaling mechanism. The IMS presents several new security challenges for both network providers and network users. This paper provides an overview of the IMS architecture and the security challenges that it raises. It is intended as the basis for developing a new set of research objectives around IMS security.

1 Introduction

The IP Multimedia Subsystem (IMS) is at the core of the upcoming next generation of telecommunication services. Developed by the 3rd Generation Partnership Project (3GPP), IMS is based on Session Initiation Protocol (SIP) [13, 16] signaling and the Internet Protocol (IP). The IMS architecture represents a significant change in the way telecommunication services are implemented and deployed. With these changes comes a new set of challenges to providing a secure and trusted set of services. This white paper outlines the security challenges for IMS.

Given that the IMS is based on SIP and IP, it inherits the numerous known security challenges with these protocols. In particular, there has been significant work in recent years on both the problems and solutions for SIP-based VoIP security [7, 9, 17]. This paper does not specifically address these issues. Instead, this paper focuses on the larger set of issues surrounding the IMS and its use by network providers.

The paper is organized as follows. The next section provides an overview of the IMS architecture with specific consideration given to security. Section 3 describes specific security issues from the network provider or carrier's perspective. Section 4 covers security from the application developer and user's perspective.

2 An Overview of the IP Multimedia Subsystem

The IMS is being developed as the next generation core architecture for converged voice and data services. While it was originally intended for 3GPP wireless, IMS has evolved to include multiple access technologies and is the basis for planned converged network services including both wireless and wired access.

The three primary goals most often cited for the IMS are Quality of Service (QoS), Charging and Billing, and Integration of Services. In short, the first two goals derive from the fact that modern networks are primarily based on the packet switched (e.g. IP) protocols that provide only a best effort service. Thus, most VoIP applications cannot provide any guarantees as to the user experience nor can they provide fine-grain charging and billing interfaces for the network provider. An important objective of the IMS standards is to create an architecture for deploying VoIP applications that provides for both QoS and charging.

The third goal of IMS is to provide an architecture for efficiently integrating multiple different services, that can be easily mixed and matched to meet the user's needs. The IMS is designed to eliminate the need to create the traditional stovepipe applications that must include all features in a single application and do not easily integrate with other applications. Instead, the IMS supports the notion of combinational services such as Presence, Location, and Push-to-Talk that can be leveraged for new applications.

The IMS architecture is a product of the 3GPP standards organization. Originally introduced in 3GPP Release 5, the IMS is defined as an overlay to the Packet-Switched (PS) Domain, most commonly deployed over IP. It is important to recognize that it is the functional interfaces that are standardized rather than the details of the individual components. This allows for significant variation in the internal design and implementation of IMS-based products.

The fundamental building block of the IMS is SIP, the Session Initiation Protocol [16]. SIP provides the primary signaling mechanism used between the components of the IMS architecture. However, SIP is just one of the many protocols that comprise the IMS specifications.

This paper will provide a brief overview of the IMS as a basis for a discussion of security. For a detailed description of the IMS one should refer to the 3GPP standards or one of the many available reference books on the subject [5, 14]. The basic IMS architecture is depicted in Figure 1. At the heart of the *IMS Core* is the *Call Session Control Function* or *CSCF*. This is the primary SIP signaling server that acts as the SIP rendezvous point. The CSCF duties are divided into three main categories, creating the three variants of the CSCF. The *Serving (S-CSCF)* is the central rendezvous point that plays a role in nearly all IMS sessions. The *Proxy (P-CSCF)* provides the external interface to the client user agents when they first contact the IMS. The *Interrogating (I-CSCF)* provides the external interface to other IMS network cores and plays an important role in both inter-carrier calls as well as roaming.

The *Home Subscriber Server (HSS)* provides a database of user credentials and configurations and identifies the home S-CSCF of the subscriber. It is consulted to authenticate a user and to determine which services a client can access. The *Subscription Locator Function (SLF)* is a simple database mapping subscribers to their home HSS and is only used when multiple IMS networks are linked together.

The cellular subscriber connects to the IMS network through the *Gateway GPRS Support Node (GPRS)*. To the IMS core, this device performs the function of an IP router that connects the clients through the PS domain. Figure 1 highlights the fact that the *User Equipment (UE)* may connect to the IMS via cellular data, Wi-Fi, or in the case of dual mode devices, both cellular and Wi-Fi. Of course, direct wire IP devices are also supported.

The traditional PSTN is reached through one or more *Circuit Switched (CS)* gateways. In the above

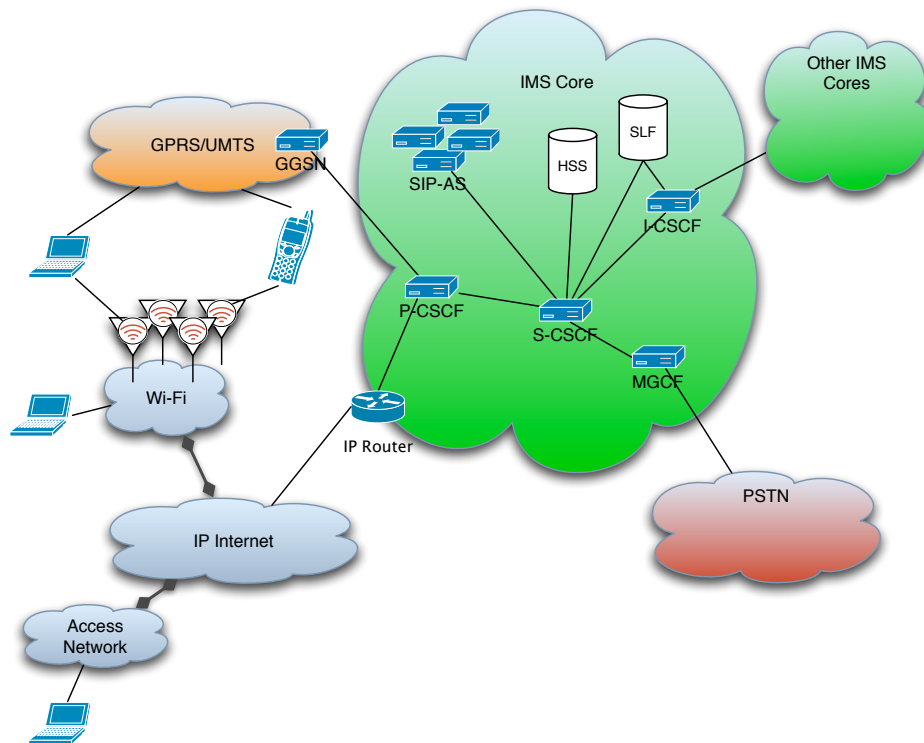


Figure 1: IMS Basic Architecture

diagram, this function is represented simply as the *Media Gateway Control Function (MGCF)*.

New services are deployed in the IMS architecture in the form of SIP Application Servers (SIP-AS). These servers are reached initially through SIP messages, forwarded to the correct SIP-AS by the S-CSCF based on triggers (configuration settings) that identify specific application requests. For example, the Presence service is implemented on a specific SIP-AS configured for providing this service. The goal is that a single Presence server could be deployed and then all future applications that require Presence could leverage that service. In a large scale, commercial deployment it is possible to imagine tens or even hundreds of distinct SIP-AS servers providing a wide range of services. These servers may also have non-SIP (e.g. media) interfaces that will also be part of the service infrastructure.

2.1 General IMS Security Issues

The IMS architecture presents significant security challenges that must be addressed by the carriers as IMS moves into widespread deployment. The generally open and distributed architecture creates the advantage of flexibility in implementation and deployment. It also creates a multitude of interface points that must be secured.

Security around the IMS is a significant part of the 3GPP standards work. The 3GPP working group responsible for overall security analysis is *TSG SA WG3*. In particular, this group is charged with considering new threats introduced by the IP based services and systems and setting the security

requirements for the overall 3GPP system. The stated objective of this group is to provide at least the same level of security and confidentiality as the 2nd Generation digital systems (e.g. GSM) and to improve upon this wherever feasible.

The overall IMS security architecture, described in [2], is limited in focus to the IMS components of the 3G architecture. Specifically, it deals with how the SIP signaling is protected between the subscriber and the IMS, how the subscriber is authenticated and how the subscriber authenticates the IMS. It does not specify access authorization mechanisms for the underlying Circuit Switched (CS) or Packet Switched (PS) domains. The larger 3G security architecture is defined separately [1]. There are several other important areas that are not defined in [2] that will be identified later in this document.

The IMS security architecture described in [2] is depicted in Figure 2. The architecture identifies five different security associations within the IMS.

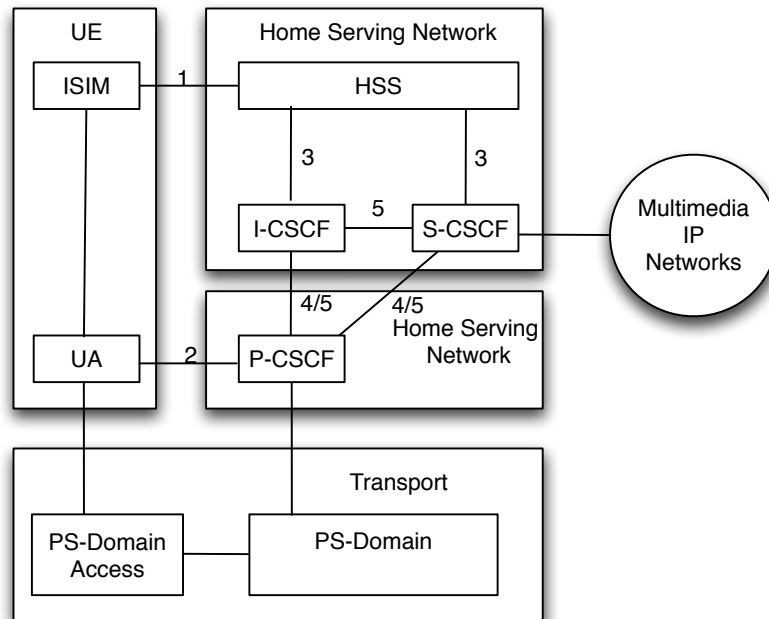


Figure 2: IMS Security Architecture

1. Mutual authentication between the UE and the IMS. The HSS delegates this to the S-CSCF but the HSS is responsible for generating the keys and challenges.
2. Secure link and security association between the UE and P-CSCF for authentication of data origin.
3. Provide internal security for the link between the CSCF and HSS. This is known as the *Cx* interface. This association plays an important role in securing the keys and challenges during the UE registration process.
4. Provides security between the P-CSCF and other core SIP services when the UE is roaming in a *Visited Network (VN)*.
5. Provides security between the P-CSCF and other core SIP services when the UE is operating in the *Home Network (HN)*.

One important aspect of the IMS security specifications is the realization there are already numerous initial deployments of the IMS where not all of the requirements of the standard can be met. For example, while IPv6 is specified by the IMS, in many cases it is being deployed on IPv4 infrastructure. Another significant issue is that current UE devices, especially mobile handsets, do not have the processing capabilities to support IPsec. In order to address these concerns the 3GPP developed the recommendations in [3] to propose solutions for early deployments of the IMS.

While the IMS standards identify specific challenges and provide solutions for these core security areas, there are several other areas that still need to be addressed in the deployment of IMS. This section identifies some additional aspects of the IMS that have implications for security management.

- **Quality of Service (QoS):** One of the primary goals of IMS is to provide QoS guarantees to users in order to meet the bandwidth and delay requirements of multimedia applications. As such, it is necessary for the IMS networks to provide secure QoS architectures that prevent a user, or group of users, from creating a traffic load that overloads the media resources in such a way that the QoS requirements of another user are violated. This is especially challenging in a multi-carrier environment across multiple IMS cores.
- **Charging and Billing:** Another important goal of the IMS is to provide a means for new data applications to be “onboarded” into the carrier networks in such a way as to be included in the carrier’s charging and billing systems. The interfaces to these systems are historically proprietary for each carrier and represent both a high barrier of entry for application developers and a high security risk profile for the carriers. The standardization of these interfaces is critical to the success of IMS in commercial deployment. The security of these interfaces will also be of paramount importance.
- **Enabling Services:** The IMS creates a modular architecture for providing application building blocks that can be combined into unique service offerings. Some of the most important enabling services include Presence, Location, Group List Management, Push-to-Talk over Cellular (PoC), Instant Messaging and Chat. Each of these enabling services must provide its own security architecture and policies to manage security issues including privacy, data integrity and usage fraud. For instance, privacy issues around Presence and Location services remain as major stumbling blocks to their widespread deployment.

Additionally, a major issue remains around the notion of deploying third party application services within the IMS core in the form of new SIP-AS servers. These systems will be deployed using third party software but with a level of trust required because of their location within the IMS core. Standards and policies will need to be developed to determine how these systems will be integrated into the SIP signaling path, the application data path, and the charging and billing systems. Some notion of protection, such as independent network security zones, is needed to isolate application systems from each other and from the critical core of IMS services [4]. For instance, the Georgia Tech IMS lab is designed with separate security zones to isolate the application development environment from both the operational IMS core and from other application developers.

- **Regulatory Considerations:** As with most data and telecommunications networks, the IMS is being deployed in a complex world of regulatory constraints. As an international standard, the IMS will be deployed in environments with distinct, perhaps conflicting, policy requirements. Issues such as emergency service contact (e.g. E911) requirements, number portability, and widely varying personal privacy obligations mandate specific service availability and data access requirements. Additionally, mandates such as CALEA wiretap access for law enforcement create very specific demands on the network architecture which may result in a radical departure from the original network designs, especially with respect to the media stream. In some cases, “voice” applications will have distinctly different regulatory requirements from other “data” applications, making it more difficult to meet the design objectives of an integrated service network. For now it appears that CALEA does not apply to VoIP telephony but it remains to be seen how this will be applied to IMS deployed by traditional carriers [8].

- **Security Appliances and Performance** The security challenges of IMS, as with general VoIP and other network applications, have created the need for a set of additional services and functions focused on securing both the components of the IMS architecture and the overall services it provides. Numerous devices such as SIP-aware firewalls, Session Border Controllers (SBC) and other application specific gateways are all part of the proposed security solutions. As large scale IMS deployments become a reality, the performance of these devices as well as the fundamental architecture of their deployment becomes critical to the success of the security model.

3 Security Concerns for Network Providers

3.1 Toll Fraud

Based on SIP, the IMS provides for the separation of signaling and media pathways (at least logically), similar to the common channel signaling of SS7. Although this design provides several benefits, it hampers the ability of carriers to audit or confirm that the User Agent's (UA) reporting mechanism is functioning correctly. This inability of carriers increases the possibility that users may utilize unauthorized services, resulting to both intentionally and unintentionally executed toll fraud.

Most UAs are developed and manufactured by third parties rather than the carrier itself. For this reason, and as the diversity of UAs increases, it is impractical for the carrier to validate the security of each UA prior to allowing access to its network. It is also risky for the carriers to assume that the UA on its network will function correctly. When mobile devices rely on connection resources provided by the carrier (such as cellular network towers), the carrier may have the ability to collect and audit the data flow to verify that the terminal is functioning correctly. However, with the introduction of dual mode phones, much of the traffic reaching the IMS will arrive via facilities which are not tightly controlled by the carrier.

If UAs are connected directly to the public Internet, it is very possible for users to communicate directly using Peer-to-Peer, direct addressing, which could conflict with carrier pricing structures. In the IMS, the HSS provides the mapping between the UA's IP address and the public identity provided during the SIP REGISTER process. However, the discovery of associated IP addresses is not difficult. During the call setup phase, a callee's IP address is provided to the caller to establish a separate data channel. Once a UA obtains an IP address of the callee's UA, it can simply send a CANCEL request to the core network and establish its own connection to the callee directly, using the same data and voice communication as in the paid service.

SIP proxy servers can also be used maliciously to create a toll fraud. Although proxy servers are commonly used legitimately within a commercial environment in a form of PBX phone systems, the same technology can be exploited within a personal environment to share the same account amongst a community of users. This exploitation can be easily implemented due to the lack of physical location constraints of the phones that existed on a traditional PBX. Proxy servers utilize already-standardized SIP redirect responses (3xx) to direct traffic to the proper UA, making it legitimate for anybody to implement. By making a UA a proxy server or building a dedicated proxy server that registers to the IMS network, a group of users could potentially share the billing identity associated with the given account. This raises complex policy questions for IMS carriers and could require intricate security enforcement to implement.

Toll fraud attacks can affect landline and cellphone services in different ways. In the case of landline VoIP services, many of the pricing structures are typically based on unlimited usage within geographical boundaries. This method of attack will be able to cross those boundaries without the appropriate extra charges. For example, a UA with an unlimited state-wide plan will now be able to make international calls by IP dialing after discovering the callee's IP address. In case of the

cellphone, many pricing structures are usage based, typically per minute and per kilobyte of usage. Toll fraud attacks can falsify the usage minutes of call duration and will also be able to make any type of data transfers between UAs with little or no chance of detection by the core network.

3.2 IPv4 vs IPv6

The original design of IMS assumed that IPv6 would be the common protocol version on the Internet by the time IMS was scheduled to be deployed. Unfortunately, IPv6 has yet to be largely deployed in the Internet and the original design of IMS had to be modified to function in both IPv4 and IPv6. Many of the features assumed in IPv6 need to be explicitly addressing when using IPv4. For instance, the abundance of unique IP addresses through IPv6 would have eliminated the need for NAT traversal features. IPSec features in IPv6 are also assumed to provide secure data transport throughout the network.

3.3 NAT and IPSec

Even with IPv6 solving the address depletion problem, Network Address (and Port) Translation is a tool that can play an important part in networking. NAT provides some level of security by limiting the direct access to the hosts behind the NAT, while allowing internal hosts to initiate a connection with outside hosts. The benefit of NAT also extends to management of the network where an administrator can monitor a single point in the network to evaluate the data exchange from the Internet to its LAN. NAT also allows for the deployment of multiple UAs without the need for an official ARIN address assignment.

Regardless of the benefit that NAT provides, NATs “violate the fundamental semantic of the IP address, that it is a globally reachable point for communications” [9]. SIP assumes that all IP addresses used in the message are globally reachable. SIP messages originating from a UA on a private network will be unroutable when the response is sent back. It is therefore necessary to deploy SIP-aware NAT devices as well as NAT traversal mechanisms within the IMS.

IPSec features provide for the overall confidentiality, integrity, and authenticity of every packet sent and received. IPSec not only provides encryption of the payload, but also guarantees connectionless integrity and origin authentication of the individual packet. Although IPSec offers many security benefits, this is not fully compatible within a network behind the NAT. The nature of NAT requires manipulation of the packet header, to replace the private IP address and port numbers with globally routable address and port, and visa versa. However, modifying the header content violates the IPSec’s integrity guarantee and origin authentication, which invalidates the packet, and consequently it can no longer considered trusted. Methods to provide same level of security in a NAT environment is to tunnel IPSEC in UDP to the end host, or perhaps even to have separate key exchanges between a private host to a NAT router and from NAT router to the destination host, possibly with the same being necessary by the remote peer. This complication introduces the potential for interoperability problems, which could lead to a lack of adoption stretching past the date when IPv6 becomes widely available.

3.4 Authentication

Authentication is commonly categorized in three ways: something you have, something you know, and something you are [12]. Although the ideal authentication protocol would utilize all three of these factors, the authentication process would become too cumbersome to common users to do this every time they wish to use a device. Current GSM cellphone authentication is accomplished by using a shared secret key between the carrier and the user. The secret key is usually stored in the

Subscriber Identity Module (SIM) that can be removed to allow device-independent identification. Unlike most cellphone devices, landline VoIP phones and other softphones are not equipped with any media designed to store a secret key. Even if there were a practical way to store such information that did not parallel SIMs, standardization on particular methods of communication would have to occur to leverage it. For this reason, username/password authentication is being used for devices that do not currently have a shared secret key. However, the current username/password authentication implemented in IMS is prone to brute force attacks and replay attacks, among others.

For example, Home Subscriber Server (HSS) is designed to accept the IP address of the latest REGISTER request as the client's IP address. Because the authentication is vulnerable to replay attack until the next REGISTER request is due, an adversary is able to re-register using the same challenge response with different IP address to redirect all the features to any other preferred destination. This effectively creates a denial of service and identify theft risk to the legitimate user. Also with the lack of two-way authentication, an adversary can hijack the session using the man-in-the-middle attack.

3.5 Gateway Attacks

IMS gateways are arguably the most vulnerable hosts in the network due to their exposure to the public and the impact that they can have when compromised. More specifically, Signaling Gateway (SGW), Media Gateway Control Function (MGCF), and Media Gateway (MGW) require some level of conversion in content forms, which requires legitimate manipulation of the content. Whenever a data is converted to different media, integrity checks should be in place to verify that 1) content converted is the same content as before in different format and 2) resulting data is still considered benign. It is possible for an adversary to perform an inverse conversion from a malicious script (that may look benign prior to conversion) to something that may harm the network after it has been converted.

3.6 Denial of Service

The IMS faces the threat of Denial of Service attacks from several sources, and has a much wider exposure to DoS attacks than any previous telecommunication infrastructure. One obvious threat is that posed by its connectivity to the Internet. While there are technologies that can mitigate DoS attacks from the Internet, the fact remains that a determined attacker with sufficient resources can cause at least temporary disruption to any Internet host, and thus a carefully planned attack on an IMS implementation (or an upstream "bottleneck") could result in degraded service capability. Another consideration is the danger of powerful and configurable UAs that are vulnerable to compromise. The scenario in which many users viewed malicious content and subsequently suffered a compromise could result in numerous UAs flooding the IMS with requests and thus denying service to uncompromised customers. Further, a compromised UA could serve as an IMS application exploit vector, which could lead to even worse consequences than DoS.

3.7 Network Topology

Many carriers prefer that their network structure and capabilities of their service be kept confidential and proprietary. Needless to say, there are many ways to discover bits and pieces of information from closely examining the packets. For example, the number of CSCF servers in the network and how the packet is being routed can be revealed when observing the *via*, *route*, *record-route*, or *path* headers of the SIP packets. In order to conceal the topology of the internal network, information revealing headers such as the *via* header can be encrypted until it passes the IMS border gateway.

4 Security Concerns for Network Users

4.1 Denial of Service

While Denial of Service is usually thought of as a threat to a network provider, the IMS presents a novel set of conditions, some of which could be commandeered so that an individual user could fall victim to a DoS. One of the most fundamental guarantees that IMS provides is that of quality of service guarantees for a UA to receive content. While the IMS cannot account for “layer 1” problems, such as a sudden loss of signal or RF interference, it is the IMS’s responsibility to ensure that the provisioned bandwidth is made available to the UA. A malicious entity could seek to make some or all of this bandwidth unavailable to the legitimate UA, which would constitute a DoS. Even if the adversary were not attempting to steal the bandwidth for his own use, the IMS must still guard against any situation in which an adversary could consume a legitimate user’s bandwidth, even by throwing it away (“layer 1” attacks notwithstanding).

4.2 User Agent Applications

Another important consideration is the IMS’s essential role in providing safe application content to the UA. As the IMS infrastructure allows for a much richer array of application content to be delivered, the threat landscape to the UA broadens to include threats to each application. This is especially true given the important IMS goal of enabling carriers to act as providers of third-party application content. While the reward to carriers of bringing on third-party applications is compelling, the security threat to the UA posed by malicious content (as generated by compromised or legitimate-turned-unscrupulous application service providers) poses serious risks to UAs, and hence user assets.

4.3 Identity and Presence Considerations

Of paramount concern to a user is the security of their personal data. As mentioned above, the broadening of applications available poses a threat to the security of user terminals, and thus to all the information that is stored on or passes through the device. But the IMS is also designed to facilitate enabling services to users that leverage social networking concepts at an architectural level. For example, IMS subscribers may designate various groups of friends, family, or colleagues as having access to *presence* [15] data, which informs these groups of various attributes of the user, such as current status, availability, and location. Rather than defining these groups on a per UA basis, these groups are instead managed by the IMS so that the user can expect them to be functioning while associated with any UA. Along with the benefits of these features come associated risks: The various presence data must be safeguarded against eavesdropping even “privilege escalation” within a user-defined group.

Even without capturing any of a user’s personal information, a serious threat to a user is posed by the potential of an attacker to pose as someone else and be accepted by the IMS. Users will be able to create multiple distinct public identities (e.g. business vs personal) that are tied to a single private identity. Users will come to expect strong guarantees about identity as the information becomes more accurate through a modernized architecture, but as expectations grow, so too grows the risk posed by a falsified identity. This is obviously a risk to carriers, since theft of service would be inevitable, but it is also a threat to individual users, since an attacker acting as them and using the IMS to assert their identity to other people or services could result in financial (or

personal/intangible) losses.

4.4 Personal Data and Privacy

As mentioned above, users are trusting more and more personal data to digital technology. One area of active research centers around the privacy concerns raised by location data [11]. The GEOPRIV working group in the IETF is actively working on standards for location data privacy [6]. Many UAs employ Global Positioning System (GPS) technology that allows the user to know, and potentially share, his or her location information. Even without built-in GPS, most carriers are developing some form of location determination service and the location service is a core enabler of the IMS. However, the uptake of location-based services has been slow as carriers seek the correct mixture of demand, availability and marketability, and in part because of lingering privacy concerns associated with sharing personal location data. The IMS offers a chance to standardize the dissemination of this data between application service providers and UAs, and thus can be viewed as a great asset to privacy advocates. On the other hand, the IMS also inherently enables third-party applications to access this data, and therefore takes on great responsibility for the proper management of user preferences in this regard.

Another user concern is that of voice and data privacy, namely encryption. As discussed above, complex and incompatible regulatory climates make the encryption of voice and data difficult. Encryption schemes have been proposed [10] that use VoIP infrastructure for key exchange and rely on the UA to encrypt subsequent transmissions. Several factors make this solution complex. As discussed above, the current lack of IPv6 deployment makes many encryption schemes that rely on end-to-end integrity difficult [3]. Also, unfortunately, the UA often does not have sufficient CPU and battery power to support voice encryption, and even if it did, such a system could run afoul of regulatory requirements for wiretapping. Therefore, IMS operators, if they are to implement any encryption whatsoever, quickly find themselves in the position of having to manage any encryption on behalf of the user. Carriers also must contend with the threat of malicious users trying to disguise certain exchanges in order to avoid appropriate billing. Third-party application developers could have a legitimate desire to encrypt sensitive data between the UA and their application without allowing access by a carrier (such as social security numbers or medical information). Accommodating all of these conflicting requirements creates an environment that promotes a “lowest common denominator” for security, even by the best-intentioned developers, and therefore poses a risk to user security.

5 Conclusions

This paper provides an overview of the IMS architecture and of the issues related to IMS security. There are numerous challenges to the secure implementation, deployment and use of the IMS. The next step for the ongoing research project is to identify specific areas that will be addressed in the near term research efforts.

References

- [1] 3GPP. Security architecture. Technical Report TS 33.102 V7.1.0, December 2006.

- [2] 3GPP. Access security for IP-based services (release 7). Technical Report TS 33.203 V7.6.0, June 2007.
- [3] 3GPP. Security aspects of early IP multimedia subsystem (IMS) (release 7). Technical Report TS 33.978 V7.0.0, June 2007.
- [4] Bob Bellman. Exploring IMS security mechanisms. *Business Communications Review*, January 2006.
- [5] G. Camarillo and M. Garcia-Martin. *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*. John Wiley and Sons, 2006.
- [6] J. Cuellar, J. Morris, D. Mulligan, J. Peterson, and J. Polk. RFC 3693: Geopriv requirements, February 2004.
- [7] D. Endler and M. Collier. *Hacking Exposed VoIP: Voice over IP Security Secrets and Solutions*. McGraw-Hill, 2007.
- [8] FCC. Communications assistance for law enforcement act and broadband access and services. Technical Report 04-187, August 2004.
- [9] D. Kuhn, T. Walsh, and S. Fries. Security considerations for voice over IP systems. Technical Report 800-58, January 2005.
- [10] Vijay Arvind Balasubramaniyan Lei Kong and Mustaque Ahamad. A lightweight scheme for securely and reliably locating sip users. In *Proc. IEEE/IFIP Network Operations & Management Symposium*, 2006.
- [11] I.i.f. LIF privacy guidelines. Technical report, September 2002.
- [12] C. Mellow. Authentication methods and techniques. Technical report, February 2007.
- [13] L. Ong, I. Rytina, M. Garcia, H. Schwarzbauer, L. Coene, H. Lin, I. Juhasz, M. Holdrege, and C. Sharp. RFC 2719: Framework architecture for signaling transport, October 1999.
- [14] M. Poikselka, A. Niemi, H. Khartabil, and G. Mayer. *The (IMS): IP Multimedia Concepts and Services*. John Wiley and Sons, 2006.
- [15] J. Rosenberg. RFC 3856: A presence event package for the session initiation protocol (SIP), August 2004.
- [16] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. RFC 3261: SIP: Session initiation protocol, June 2002.
- [17] D. Sisalem, S. Ehlert, D. Geneiatakis, G. Kambourakis, T. Dagiuklas, J. Markl, M. Rokos, O. Botron, J. Rodriguez, and J. Liu. Towards a secure and reliable VoIP infrastructure. Technical Report D2.1, January 2005.