

WHITE PAPER

Motorola Converged UMA Security Solution

September 2006



Due to the detailed information contained within, we request that account teams limit distribution to accounts under Motorola's terms for NDA. Please contact paula.mccarty@motorola.com or randall.martin@motorola.com for more information, or a member of the Motorola security team.

Securing UMA

A well-designed UMA security architecture provides a distinct competitive advantage for service providers and serves as a proving ground for the challenging security requirements of converged networks (e.g., fixed, mobile, IMS, VoIP).

CONTENTS:

3 **Part I – UMA Security Fundamentals: A Real-World Perspective**

3 Motorola Security Services Field Assessments

4 Standard UMA Building Blocks

7 Architected UMA Security

8 Summary

9 **Part II – A 360-Degree View of UMA Threats**

9 Threats to Subscribers

10 Threats to UNC and GSM/GPRS Core

11 Threats from Insiders

12 Cross-Domain Threats

13 Threats to Data Assets and Transactions

13 Threats from Poor Policies, Procedures and Processes

14 **Part III – A Holistic Approach to UMA Security**

14 Vulnerability Assessment and Evaluation

15 Security Gap Analysis

16 Security Architecture Design

16 Perimeter Defense and Zoning

17 UMA Access Perimeter Firewall

18 INC and IDP Security Configuration

18 UMA Network Element Hardening

19 UNC System Survivability

19 UMA Network Management Policies

19 OAM Interface Security

20 OAM Firewall

20 UMA Operational Security

21 Reference Architecture Methodology

21 Summary

22 Where is UMA on the IMS/FMC convergence roadmap?

22 About Motorola Security Services

22 About Motorola Services



PART I – UMA Security Fundamentals: A Real-World Perspective

When mobile service providers successfully deploy Unlicensed Mobile Access (UMA), their customers can move seamlessly between WiFi and GSM networks without being aware of the hand-off or the underlying technical complexities. The GSM/GPRS radio air network (RAN) provides mobility, and the wireless LAN provides high bandwidth and cost-effective IP connectivity. It's a magic combination that potentially enables a wealth of new value-added services and opportunities to build customer relationships.

The advantages of UMA are considerable, but so are the security issues. By opening up the mobile core network to public Internet access, UMA creates security challenges that service providers must address if they are to maintain high levels of network availability, billing accuracy, and user data privacy. UMA-related security threat vectors include:

- Public IP network users
- UMA subscribers
- Cross-domain attackers (e.g., GSM/GPRS subscribers)
- Attackers internal to the service provider's network

Motorola Security Services Field Assessments

As part of its security design work, Motorola has conducted vulnerability and operational security assessments of mobile service provider networks and enterprises in North America, Europe, Latin America, China, the Middle East, and other regions. Motorola has consistently found security

vulnerabilities and operational deficiencies in its assessments, and the UMA environment presents a particularly rich hunting ground for our security engineers who strive to discover weaknesses in security systems and operational processes before the hackers do.

For example, in a recent security assessment for a leading mobile service provider with a pilot UMA installation, the Motorola team uncovered a wide range of vulnerabilities. The team conducted the tests from outside of the network, using only the access privileges that a typical UMA subscriber would have (i.e., a dual-mode handset and a SIM card). Although this service provider has world-class data center security and standards-mandated IPsec protection for UMA subscribers, the Motorola "ethical hacking" team was able to penetrate the network and, using the UMA access network, map core IN resources. Once the team created a picture of the internal network and its hosts and controllers, it was

Why UMA?

UMA technology enables the delivery of high-quality mobile voice and data services over GSM and broadband connected Wi-Fi / Bluetooth® wireless networks located within homes, home offices and hot spots. Access via unlicensed spectrum is potentially available at a significantly lower cost than existing 2.5 and 3G mobile network technologies. As a result, subscribers can confidently use their mobile phone as their main communications device. Service providers can maximize their revenue potential and improve retention from their subscribers' use of the mobile phone or expand their footprint to new businesses.

Benefits

- Increase the use of mobile voice and data services
- Optimize the use of GSM radio network resources
- Reduce capital and operational expenditures on radio networks
- Bundle services to improve retention and increase share of consumer's total spend



possible to probe core systems for open ports, unnecessary services, misconfigurations, and user account data.

Vulnerabilities discovered in this particular UMA assessment were primarily in the area of GPRS core and related infrastructure. Also found were a number of improper configurations of the UMA implementation. Specific vulnerabilities included:

- A firewall with ports open, making possible the remote discovery, via the UMA interface, of internal network topologies and assets
- Enumeration of default names and passwords that gave access to key UMA infrastructure systems, leaving them open to misconfiguration, hacking and sabotage
- Numerous denial-of-service vulnerabilities that could lead to service disruption
- Potential for disclosure of subscriber identities and data
- Outdated network management protocols that allow hackers to take remote control of key UMA and related IN devices
- Numerous unnecessary services, unhardened systems, visible network interfaces and misconfigurations, which generally leave the GSM and UMA infrastructure open to many kinds of malicious attacks

In this particular assessment, many of the vulnerabilities discovered were only moderate threats, but several were serious enough to potentially affect network availability, integrity, billing, confidentiality and compliance. This is often the case in vulnerability and operational security assessments that Motorola executes for leading service providers around the world. All networks have some level of vulnerability (often due to GSM/GPRS misconfigurations), but UMA

heightens risk exposure somewhat, due to the integration of public IP access with the service provider's infrastructure. This paper makes the case that a well-designed wireless security architecture and related operational security policies are "non-optional" for service providers deploying UMA. Service providers must implement UMA properly and address any outstanding GSM/GPRS configuration issues that can be exploited through UMA access networks.

UMA deployed with a well-designed overall security architecture makes possible better home rate tariffs, competitive SOHO business services, high-bandwidth media streaming and home e-commerce applications, increased average revenue per user (ARPU), reduced churn, and leveraging of lower-cost fixed infrastructure. UMA is also an excellent proving ground for protection and mitigation principles that service providers can ultimately apply to IMS, SIP and VoIP infrastructure, and related service-delivery models. Indeed, UMA will likely play an ongoing role as a viable wireless access method in IMS/FMC networks (see page 22: "Where is UMA on the IMS/FMC convergence roadmap?").

As one of the initial contributors to the UMA standards effort, Motorola has considerable in-house security design experience in the UMA realm, including specialization in the area of comprehensive vulnerability and security architecture assessments for UMA. This paper discusses many of Motorola's hands-on best practices and security architecture principles.

Standard UMA Building Blocks

As defined by the Third-Generation Partnership Project (3GPP), UMA consists of a number of functional building blocks and related

Convergence Glossary

FMC - Fixed Mobile Convergence

IMS - IP Multimedia Subsystem

SIP - Session Initiation Protocol

UMA - Unlicensed Mobile Access

VoIP - Voice over IP

WiFi - Wireless Fidelity (generally, 802.11x related wireless LAN technologies)

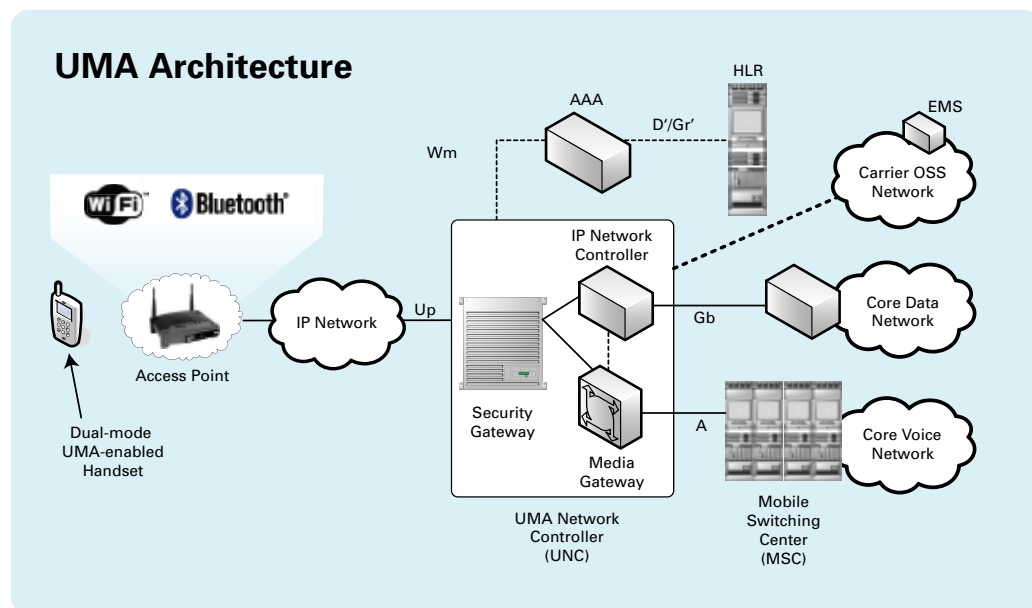


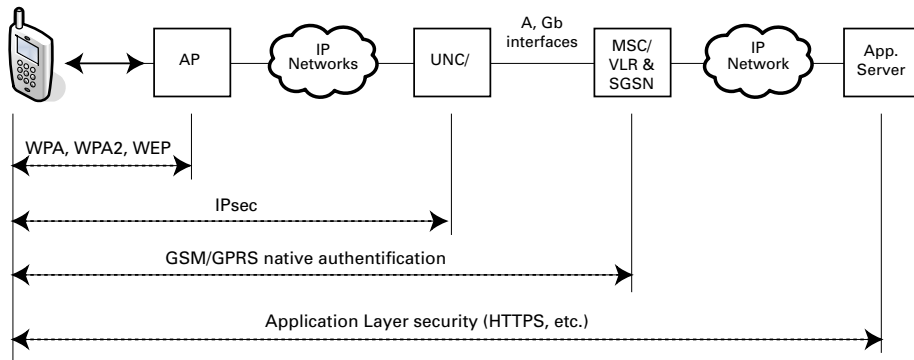
standards-based security elements. The wireless LAN domain of UMA is protected by the IETF IPsec and several 802.11 security standards, including WPA, WPA2 and WEP. A service provider can deploy the UMA Network Controller (UNC), which directly interfaces to the core network, in various ways, but the essential functional components of the UNC include:

- **Security Gateway (SGW):** Protects the confidentiality and integrity of user voice and data streams via IPsec sessions between dual-mode handsets (mobile stations or 'MS') and the service provider's core network.
- **Media Gateway (MGW):** Converts packet-based voice streams to circuit-based traffic and hands them off to the core voice network. The Media Gateway preserves the cellular

network's GERAN-based encryption and authentication methods.

- **IP Network Controller (INC):** Handles both circuit- and packet-based data services and routes this traffic to and from the core data network.
- **SS7 Gateway (SS7GW):** Can be a separate device or bundled into the other UMA components. The SS7 Gateway provides SS7 connectivity between the INC and MSC, terminating the SS7 links from the MSC and providing an IP-based SIGTRAN interface to the INC.
- **Load Balancing Router (LBR):** An optional device that provides fault-tolerant IP communications within the UNC, between the INC and SGW. The LBR also balances incoming signaling and packet data traffic to the INC, thus enhancing the reliability and scalability of INC service.





The standards specifications for IPsec tunnels between the handset and the UNC security gateway cover private/public key generation/exchange and encryption for data confidentiality/integrity, using some mix of crypto standards (e.g., IKE, EAP-SIM, AES, 3DES, MD5), which can vary for each UMA implementation. Once the service provider's authentication server (AAA) authenticates a dual-mode handset user with Radius, Diameter, or similar protocols, the user is then registered with the HLR (Home Location Register). At this point, the user can receive and originate calls as long as the IPsec tunnel remains active. Depending on what the handset provider supplies, HTTPS, SSL and other standards can protect (at the application level) UMA-user data traffic destined for Web servers and Internet services.

With all these security standards in place, it would appear that UMA is a very secure access method.

Unfortunately, UMA standards do not address all the threats that UMA potentially introduces into a service provider's network. As shown by Motorola's vulnerability tests, UMA, even with standards-based security in place, can introduce serious vulnerabilities for both subscribers and service providers. Standards by themselves don't guarantee UMA security—nor does "adding another box" in the form of security gateways, firewalls, intrusion detection and protection (IDP), or border controllers. Even a proprietary and expensive "self-defending" network management system is not the answer. What's really needed for long-term security is a standards-based approach, using best-of-breed products that are integrated with a comprehensive security architecture; this ensures that everything works together within the context of the mobile service provider's real-world business processes, in-place systems and human resources.

Architected UMA Security

Motorola's security reference architecture takes into account the **people, process, policy and technology** aspects of security in a holistic manner. This advanced security architecture is available as a key aspect of the *Motorola Converged UMA Security Solution*, which creates a proactive and **operational** security-management framework that is linked to the service provider's strategic business and competitive goals.

Motorola Converged UMA Security: Operational and strategic areas

Operational-level components

Security standards
Best-of-breed security products
Granular security architecture
Security-integration best practices
Policies that guide people and processes

Strategic components

Risk management
Compliance and governance
Business continuity
Financial oversight
IT portfolio/change management

Motorola's UMA security architecture starts with an in-depth assessment of the existing security policies, procedures and processes. Included in the initial assessment is an internal and external vulnerability scan, looking for weaknesses that can be exploited from the access network or the core infrastructure. The Motorola team analyzes the results of this assessment work thoroughly to uncover all security gaps and vulnerabilities. Based on the assessment and analysis, the team creates an in-depth security architecture and policy specification that covers all UMA-related areas of the service provider's network:

- **UNC communication interface security:** Focused on interfaces between UNC and all domains that it touches, including the access network, the core MSC network, and the OAM&P domain.
- **Host-based authentication and access control:** Strong password authentication, user-account management and monitoring, public key-based authentication, and ACL-based device-level access control.
- **Host-based security configuration:** System OS-based configuration: 3PV security feature configuration and provisioning.
- **UMA network segregation:** Security zoning design within the UMA network.
- **Perimeter defense:** Firewall/ACL-based perimeter definition and defense between different security domains.
- **UMA Intrusion Detection and Prevention (IDP):** Network-based intrusion detection, monitoring and reporting mechanism inside the UNC; includes IDP option to mitigate denial-of-service (DoS) attack from within the UMA network.
- **UNC system survivability:** High-availability framework to be provided at interface and host levels within the UNC communication network.
- **UMA network management policies:** Technical procedures, security provisioning policies, and security configuration management recommendations.
- **UMA service provider procedures and job functions:** Recommendations for UMA administrators' and service providers' job qualifications and skills requirements, key procedures and policies.

Summary

The *Motorola Converged UMA Security Solution* is delivered by the *Motorola Security Services* group. This solution integrates existing service provider resources, UMA security standards, and best-of-breed UMA products in order to align operational security practices with strategic risk management and business goals. The result is a great improvement in the security posture of the existing GPRS network, along with a more secure deployment of UMA. Well-executed security integration and policy design also has the benefit of ongoing optimization of security-related capital expenditures/operating expenditures (CAPEX/OPEX) within the “big picture” of competitive and financial strategies. When the service provider brings Motorola in as a partner to give UMA security the attention it deserves, the service provider’s infrastructure will be more open-ended and better prepared to evolve to IP-based value-added services, IMS, FMC, and other convergence initiatives.

The remaining sections of this paper describe Motorola’s comprehensive approach to UMA security, starting with an in-depth look at security threats (Part II), and continuing with a discussion of effective security-design methods for UMA (Part III).



PART II – A 360-Degree View of UMA Threats

There are a growing number of threats associated with “pure” GSM/GPRS cellular networks, but the addition of IP access to the mix has a multiplier effect because of the vast scale of the Internet’s open connectivity. If an Internet-based intruder located anywhere on the globe discovers just one overlooked configuration mistake or error, that intruder can compromise an entire service provider infrastructure.

Although both core network (CN) protocols and secure IPsec tunnels authenticate UMA subscribers, those subscribers nevertheless are potential threats. Unlike traditional RAN users, wireless LAN and Bluetooth users control the configuration and security methods of their own local networks. The Wired Equivalent Privacy (WEP) is a weak authentication and encryption algorithm, but it still is useful if better methods are unavailable. Motorola recommends WPA/WPA2 security whenever possible. But, service providers should be aware: in some cases, users may defeat wireless LAN security methods entirely, opening up the local network to external intruders who can choose from a range of attacks based on spoofing, masquerading, cloning, DoS exploits, etc.

Wireless LANs support very sophisticated end-point devices, including smart phones with fully functional operating systems, PDAs, and laptops with GSM/GPRS emulation hardware and software. Hackers potentially can use all these devices and the UMA access network to launch attacks and probes into the service provider’s core network. They also can use these devices to launch a wide range attacks on other subscribers.

There are many undiscovered security holes in a newly deployed UMA infrastructure, and known operational security weaknesses still exist in the

GSM/GPRS core network. Individually and collectively, these vulnerabilities introduce business risks that can affect network performance, availability, and quality of service, ultimately limiting the mobile service provider’s ability to generate revenue. Note that many of the threats discussed below are outside the realm of UMA security standards and the scenarios those standards are designed to address.

Threats to Subscribers

Attacks on UMA subscribers can originate from within the service provider’s UNC or other areas of the GSM/GPRS infrastructure. Malicious UMA subscribers who abuse their privileges also can direct attacks at other subscribers, as can outsiders who use a stolen or cloned GPRS data card to access the network.

An intruder from the public Internet or a malicious mobile user can send short, unwanted IP packets or SMS to UMA subscribers, causing victims to be inconvenienced, distracted, denied service, and/or wrongly billed. An SMS message periodically sent to a subscriber’s mobile that’s in idle mode can also drain the handset battery. Similarly, an intruder can send unwanted paging messages from within the access network to groups of mobiles. Malicious users can send spoofed requests from authenticated or un-authenticated

sources. In some cases, another user's device unknowingly participates in Distributed Denial of Service (DDoS) attacks on the UMA signaling channel. These are well-known attacks over cellular communication networks, and they are also a potential threat in the UMA environment.

In addition, subscribers are vulnerable to a rapidly expanding range of Internet viruses, worms, Trojans, malicious codes, buffer overflows, etc. Subscribers can inadvertently transfer mobile viruses and other malware from other mobile and fixed devices via wireless or Bluetooth connections, or they can unwittingly download them from infected application servers on the service provider's network or the Internet. As with GSM/GPRS users, UMA subscribers are potentially open to intrusions and exploits that take advantage of unpatched application software vulnerabilities. Increasingly, downloaded mobile malware can spread rapidly and affect large numbers of user devices.

Threats to UNC and GSM/GPRS Core

UMA subscribers are potentially capable of a wide range of intrusions and exploits on the UNC, the GSM/GPRS core, and various OAM&P areas of the service provider's infrastructure. With its open interfaces and plentiful bandwidth, the broadband

access network is an "ideal" platform for launching attacks. Motorola's vulnerability tests in Tier-1 service provider networks have found that subscribers can take advantage of UMA high-speed bandwidth for DoS and resource saturation attacks that target core and OAM&P assets.

Subscribers using little more than a handset, a SIM card, and normal user privileges can potentially map the service provider's internal network, gain unauthorized access to hosts, and then proceed to exploit and control key hosts, gateways and servers. Threats to infrastructure from subscribers include:

Discovery and exploits

- Internal network discovery
- Topology mapping
- Host discovery
- Vulnerability discovery
- Vulnerability exploits

Network and host control

- Data manipulation
- Configuration modification
- Traffic redirection
- Unauthorized file installation
- System shutdown



In addition to mapping and taking control of various aspects of the service provider's infrastructure, there are other specific exploits that can originate from the UMA access network (inside the IPsec tunnel) and from the public interface to the UNC (outside the tunnel). For instance, users can send excessive (flooding) IKE requests to the UMA Security Gateway and back-end AAA server. The impact of this exploit is the overloading of the Radius interface and AAA servers, which prevents other subscribers from gaining access to the AAA for authentication. UMA and Internet users can potentially send excessive corrupted, invalid or malformed authentication and call-control messages to key UNC and core components (SGW, INC, AAA/HLR, SS7 gateway), resulting in DoS to signaling and authentication interfaces, and leading to the overloading of resources or system crashes.

There is also the potential for use of rogue end-user devices or wireless access points to enter the UMA network to steal airtime and disrupt services. This includes use of non-compliant or insecure mobile devices. The result is negative effects on both 802.11 wireless interfaces and the UMA transport network, and the potential for service deterioration because of incompatible, non-compliant or virus-infected devices.

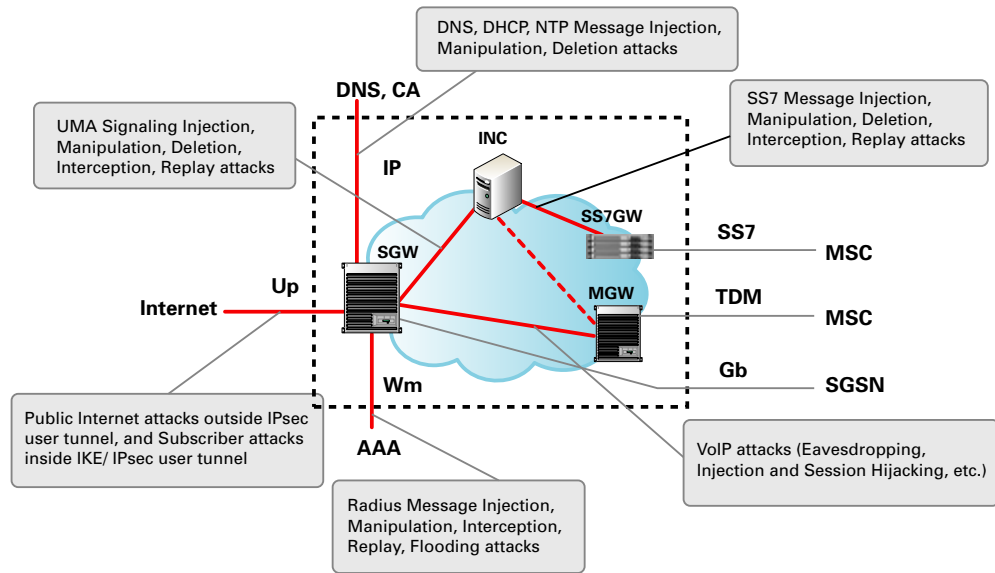
Threats from Insiders

Mobile subscribers and public Internet users are not the only major threats to UMA. Service provider employees with UNC, CN or OAM&P

access rights are also threats, capable of unauthorized intrusion via internal subnets or transport devices (routers/switches). Disgruntled employees can use a range of vulnerabilities exploits to compromise the UMA network via OAM access infrastructure and management hosts. Some of the threats associated with internal users include:

- Malicious exploits via policy or procedure weakness
- Malicious exploits via security-management weakness
- Gaining more privileges via social engineering attacks
- Unauthorized installation or modification of systems
- Unintentional attacks via configuration or provisioning errors
- Coordinated insider/outside attacks
- Disclosure of proprietary information by disgruntled employees to outsiders

The business implications of internally launched attacks are far-reaching, including loss of confidentiality, system integrity and system availability. The loss of UMA service capacity and performance can result in potentially serious economic consequences and brand damage. The diagram below shows access-network threats (Internet/Up) and some specific threats that can originate internally (UMA signaling, Radius, DNS, SS7, VoIP, etc.).



There are no strict boundaries between internal and external networks in today's IP interworking environment, so the policies and practices discussed later in this document (Part III) are a necessary aspect of securing UMA.

Cross-Domain Threats

The interaction of the UMA access network with the GSM/GPRS core opens up possibilities for numerous cross-domain attacks. Malicious GSM/GPRS users can launch attacks on unsuspecting UMA users; on the other side of the coin, the public-facing UNC interface opens a back door for attacks on the traditional GSM/GPRS network environment.

For instance, when UMA users target GSM/GPRS users, they can launch paging, SMS, virus injection, and other application-related attacks. This can cause legitimate cell phone subscribers to be over-billed, as well as waste network bandwidth

and exhaust air-interface resources. Of course, many similar exploits work in the opposite direction, i.e., from malicious GSM users into the UMA environment, due to improper configuration and lack of advanced security policies in the GSM/GPRS RAN and core domains.

From a security design perspective, UMA access networks and cellular access networks, together with the service provider's CN and OAM&P domains, form a single interacting architecture. Malicious users can deliver DoS attacks and other exploits in several ways to the core components, application services, and GSM user devices. Consequently, service providers must engage in a new type of security thinking, in which they are constantly aware that cross-domain GPRS data connections from either Internet access to UMA (Gi) or IPsec tunnels into UNC (Up) can penetrate the entire infrastructure.

Threats to Data Assets and Transactions

Many of the more spectacular DoS attacks that occurred over the past few years have focused on denying or disrupting services. However, many potential exploits and malware also target valuable data stored in various mobile devices and hosts. Attacks that target data can originate from the subscriber domain, the public Internet, the UNC or OAM&P domains, or the GSM/GPRS RAN. Data assets that can be compromised, deleted or disclosed are shown in table below.

Vulnerable Assets

Data in the UNC Subscriber Domain	Data in the UNC Subsystem Domain	Data in the OAM Security Domain
<ul style="list-style-type: none"> • Personal information and records stored in MS • Personal information entered by subscriber • Configuration data • Authentication credentials (IMSI, TMSI, Ki, other authentication and encryption keys) 	<ul style="list-style-type: none"> • Subscriber Identify • Subscriber personal information transported via UNC • UNC configuration data • IPsec authentication credentials • UNC OAM&P data • UNC administrative credentials 	<ul style="list-style-type: none"> • UMA network configuration data • Public key certificate • UMA administrative authentication credentials • Logging data • SNMP data • Business inventory data • System backup • Operational policies/procedures

When subscribers use mobile networks for online banking, shopping, entertainment, gaming and other applications, their transactions often contain sensitive information such as credit card and identity details. While using e-commerce services, UMA subscribers may give out information about themselves and their finances, which leaves service providers at risk in terms of customer liabilities and compliance with regulations. If UMA is to achieve its potential in terms of broadband media streaming and e-commerce services, service providers must provide a high level of data assurance so that user information will not be:

- Altered in any way (integrity)
- Intercepted or stolen due to insecure networks or storage (privacy/confidentiality)
- Originated from an unauthorized sender (authenticity)
- Have ambiguous transaction endpoints (non-repudiation)

Threats from Poor Policies, Procedures and Processes

UMA introduces vulnerabilities, not only from new network hardware and software, but also from associated operational processes and procedures. People and improper design, deployment, and

management of technologies are the weak links in today's security architectures. Hackers are everywhere, but it's just as likely that disgruntled employees will violate policy and exploit internal vulnerabilities. Likewise, poorly trained employees can unintentionally make provisioning errors and improper system configurations that open up vulnerabilities. The security weaknesses within operational processes are very complex and sometimes hard to detect, so assessment should be an ongoing process that is built into the operational security policies and procedures. Some examples of operational security vulnerabilities:

- Lack of strong authentication and access-control procedures
- Weakness in security-management processes and policies
- Poorly trained or unqualified administrative personnel
- Poorly managed software-update and patching processes
- Lack of security-audit and monitoring processes
- Lack of security-review and vulnerability assessments
- Lack of security design with a focus on manageability

PART III – A Holistic Approach to UMA Security

With the *Motorola Converged UMA Security Solution*, Motorola offers UMA service providers a wide array of best-in-class security design services—services intended especially for service providers who are moving aggressively into UMA and converged networks to meet competitive challenges and opportunities. Motorola has built scalable and secure reference architectures and security service frameworks to support the service provider’s specific business and operational requirements in all wireless environments, including WLAN, GSM/GPRS, UMA, UMTS, WiMAX, CDMA, Mesh Networks, Metro WiFi and IMS.

Motorola teams base UMA security architectures and best practices on the principle that only multiple, overlapping protection approaches—including secure zones and in-depth defense techniques—can mitigate the full spectrum of threats. The operational environment and its supporting security program must consider technology plus people, processes, and policy-oriented factors. Use of multiple, overlapping protection approaches ensures that the failure or circumvention of any individual protection will not compromise large areas of the service provider’s network—which is a serious possibility when service providers rank security as a low-level priority or regard it as an architectural afterthought. A combination of best-of-breed security product solutions and operational best practices will help counter evolving challenges and proactively protect the service provider’s service offerings. The goal is to create a strong operational security foundation and the capability to manage the full spectrum of new IP-based technologies and services—including VoIP, IMS, FMC, etc.

The first step in a typical Motorola UMA security design and integration effort is a detailed vulnerability assessment.

Vulnerability Assessment and Evaluation

The Motorola team starts a UMA security engagement with a comprehensive assessment of the service provider’s infrastructure. The team conducts an initial vulnerability scan in two steps: 1) network level vulnerability scanning of external interfaces to find weaknesses from outside, allowing evaluation of each external contact point, and 2) host-based scanning to gain insights into host and server internal configuration details; the team uses those details to evaluate weaknesses in access control and visible services, e.g., host-level IP configuration settings, user-account and access management, application software vulnerabilities, etc. This work includes both the UMA network segment and the GPRS network into which UMA is to be integrated.

Motorola’s wireless security experts analyze results from initial security assessments and host audits to discover any UNC and GSM/GPRS subsystem vulnerabilities. A weakness found in a single subsystem may not be an isolated event—it may actually affect the entire network. Examples of typical findings:

- UMA application software vulnerabilities
- Unhardened host UNC subsystem OS

- Weak authentication/access control to UNC
- UNC provisioning or configuration procedure errors
- Weak UNC interface communication protocols
- Unpatched UNC system-configuration bugs
- Insufficient coverage in firewall-access rule sets
- Weak or non-existent privacy and integrity protection
- A wide range of potential GSM/GPRS vulnerabilities and operational security weaknesses

In addition to the UNC and access networks, Motorola engineers analyze the core network and system configurations to determine their compliance—or lack thereof—with configuration requirements and to identify any poorly configured systems. This analysis focuses on system procedures to determine if there are any weaknesses in system authentication, access control, and security management processes, particularly in the OAM&P domain. The analysis also focuses on network filtering policies to determine if they are sufficient. This is particularly important for the UNC Security Gateway and, where applicable, other UNC internal firewalls.

Other areas of concern are: system or network single points of failure; insufficient traffic isolation; weak encryption or hashing algorithms; and a range of deficiencies in the areas of backup, fault tolerance and capacity/load management, any or all of which could affect end-to-end UMA and GPRS/GSM performance.

Security Gap Analysis

After Motorola engineers scan, audit and evaluate UNC and core-systems components, they move on to conduct a security gap analysis. A security gap is anything that fails to satisfy industry-standard requirements or limits future capabilities

within the UMA operational environment. The scope of the gap analysis includes technology, policies, processes and management procedures.

Gap analysis gives the mobile service provider a clear view of what resources and costs are necessary to achieve the appropriate level of security. Good security is not free, but studies show the cost of responding to security breaches after they occur can be up to 10 times more than the cost of preventing those breaches in the first place. Some typical gap areas that Motorola engineers regularly discover are:

- Non-compliant crypto configuration in IKE and IPsec
- Non-standard key distribution procedure
- Insufficient or non-existent confidentiality, integrity and availability protection
- Lack of access-control policies for UNC subsystems management
- Weak password authentications
- Use of unhardened systems and end-user devices
- Use of inconsistent procedures in system provisioning

To be effective, this exercise must also include the GSM/GPRS security gap analysis, which can uncover a range of weaknesses, including:

- GTP flooding vulnerabilities
- Border Gateway attack vulnerabilities
- Over-billing and billing system vulnerabilities
- Gi bandwidth saturation and overload vulnerabilities
- Mobile client network access exploitation vulnerabilities
- Mobile-Mobile attack vulnerabilities
- Roaming partner network access exploitation vulnerabilities

The Motorola team then presents the results of their gap analysis to the service provider in clear business language, with an emphasis on how proper security architecture and policy design can mitigate risks while also creating a seamless UMA/cellular experience for customers.

Security Architecture Design

Motorola's security architecture design covers the end-to-end aspects of UMA security from subscriber authentication to intrusion, including exploit and DoS protection for all of the UNC, CN and OAM&P interfaces. A defense-in-depth or "layered" network design ensures the network can resist penetration, limiting an attacker's ability to discover the internal UMA network. Network IP addressing plans, network routing policies, and isolation of network and management interfaces reinforce this design.

The layered network design minimizes cross-domain vulnerabilities by emphasizing:

- Logical and physical isolation of bearer, signaling, charging, OAM&P traffic
- Use of private IP address for internal network communications
- Enforcement of access rules between/among domains

On the subscriber side, the design service covers all details of IKE and IPsec provisioning procedure. To ensure seamless authentication, the design service defines Radius client and server configuration provisioning on Security Gateway and AAA.

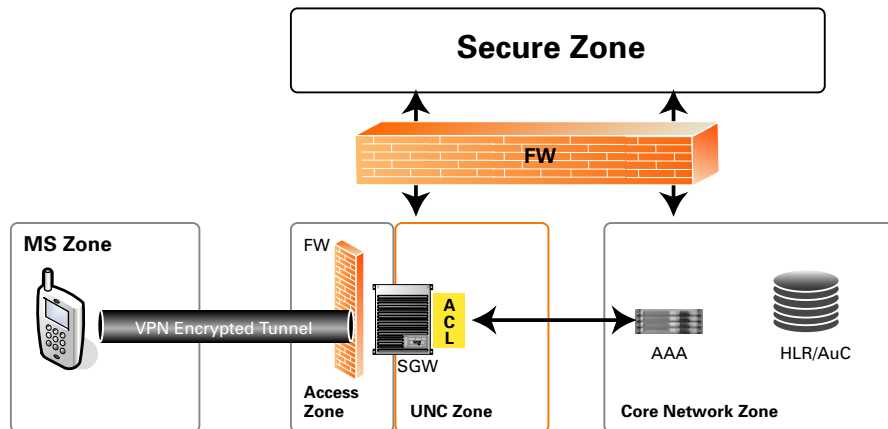
Inside the service provider's infrastructure, all access to the internal network must be authenticated and filtered by firewalls or ACL at the edge between two separate domains or zones. Uplink screening at UNC and GGSN ensures the packets destined to the internal network are dropped and all ICMP packets are filtered to limit internal network discovery. Security hardening on hosts and servers ensures that each network element can protect itself.

The ultimate goal of the layered network design and the UNC component protections (discussed below) is to ensure that the UMA and GSM/GPRS service will keep running in the face of attacks from subscribers, DoS attacks from the public Internet, cross-domain attacks, application attacks, and specialized attacks from OAM&P network-transport and network management components.

Perimeter Defense and Zoning

One of the key methods in the Motorola approach is the use of security zones that form layers of defense in depth to protect UMA and its connections to the core GSM and GPRS networks. Each zone is a set of users and/or systems that operates under a common security policy. The zoning approach defines a logical security boundary for better management of security and application of a common security procedure or process. Examples of UMA security zones are:

- **Subscriber Zone:** Contains UMA subscriber, UMA terminal, and service use policies. This is an untrusted zone.
- **UMA Access Zone (Up interface):** Contains Security Gateway (SGW), FW (recommended) and transport network devices (switch/router etc). AZ is a public zone, and SGW is reachable from any public IP space.
- **UNC Zone (Security Gateway to INC):** Contains all UNC subsystems and access-control procedure/policies. UZ, configured to be a trust zone, is established via internal IP subnets or physical VLANs.
- **Secure Zone:** Contains OAM&P management elements and IP service-support systems, as well as administration and maintenance users and operational policies.
- **Core Network Zone:** Contains AAA, HLR/AuC, MSC, SGSN, HLR, and MGW, etc. CNZ is an internal secure zone.
- **GSM/GPRS RAN Zone:** Includes radio access networks and various switches, and the controllers that support the RAN.



Motorola’s approach establishes policy enforcements via firewalls for deep packet inspection between different IP domains or zones, and between different IP subnets. A recommended OAM firewall separates OAM traffic from all other network traffic, protecting all management devices and operational configuration data, as well as subscriber databases, from malicious access. Motorola recommends a UMA perimeter firewall (Security Gateway) to protect the Up interface as a first line of defense that blocks all unauthorized access and data transfers to the internal UMA network from outside the IPsec tunnel.

UMA Access Perimeter Firewall

A well-designed and well-configured UMA SGW supports a range of subscriber-authentication methods, including IKE v2, EAP-SIM and EAP-AKA. The SGW also provides a highly intelligent and proactive intrusion-protection model that is fully integrated into the service provider’s network. Ideally, the SGW should provide an industry-tested, hardware-based solution for high-performance DoS prevention, firewall filtering, network-address translation, authentication, and session-admission control.

A key part of the SWG’s protection capabilities are access control lists (ACLs) that prevent or restrict IP traffic from traversing the UNC based on a variety of layer 2-4 parameters. Before traffic can be routed through the SGW, each packet is individually validated for both uplink and downlink directions, thus ensuring network security and providing routing enforcement within the service provider’s infrastructure. Filters that limit traffic to a specific set of destination IP addresses can be enforced. Commonly used filters include protocol identifier, port address and TOS bits. Traffic that violates the ACL either can be silently discarded or logged for further analysis. Motorola’s security engineers can configure other key SGW features, including:

- **IMSI filtering:** Subscriber IMSI filtering further restricts access to AAA/HLR resources using pattern-matching customer-assigned IMSI values (MNC/MCC) in initial EAP-SIM response/identity messages. IMSI filtering also is a mechanism to detect fraud, through analysis of the fraud log/alerts.
- **Dynamic session control:** Dynamic pinhole creation and destruction on a per-tunnel basis. This feature allows the SGW to dynamically

restrict ingress and egress traffic, based on policy feeds related to authentication and authorization. When a subscriber's traffic is routed to the SGW, it works with INC to function as a network-based firewall, dynamically opening/closing ports (pinholes).

- **Traffic shaping and bandwidth policing:** The SGW can shape traffic according to traffic class on all inbound traffic as a means to prevent DoS attacks. By ensuring that each class of traffic is limited in bandwidth, the SGW sees to it that each traffic type always has the necessary resources, which, in turn, guarantees a minimal level of service at all times, and prevents service abuse and fraud by malicious subscribers.
- **Cookie-based pre-authorization:** The SGW performs cookie-based pre-authorization as a means to combat a distributed DoS attack. A cookie-based challenge can respond to each IKE message, prior to undertaking full authentication, to filter out attackers.
- **Address-spoofing protection:** The SGW implements IP address-verification schema by validating each inbound packet's source address against the IP address assigned during UMA authentication. This prevents IP address spoofing by the end device. The SGW inspects both signaling and user data packets to protect subscriber devices from unknowingly participating in DDoS.

INC and IDP Security Configuration

The UMA SGW plays a large role in protecting the UNC from threats originating in the public Internet and subscriber base. However, the Motorola Security Services team can deploy security features in other areas of the UNC as well, particularly in the INC, and via an Intrusion Detection and Protection (IDP) function that can be deployed inside the UNC network. The UNC's IDP will identify threats based on well-known threat

signatures inside packets (deep packet inspection). It will also conduct authentication-failure analysis to protect against repeated logins and brute-force attacks on AAA. The IDP has specific protections for a number of key interfaces at the UNC perimeter, for example:

- VoIP signaling protection stops malformed or unauthorized streams from being injected into SGW-MGW connections.
- The IDP's SS7 *signaling features* block SS7 (SIGTRAN) attacks and protect against resource exhaustion through SS7 interface overloading.
- *OAM attack protection* blocks unauthorized access to OAM systems via telnet, FTO, SNMP, etc.
- The IDP also conducts inline *antivirus scanning* to keep malware out of all traffic streams that enter/exit UNC interfaces.

The INC is the key point of control for circuit- and packet-based user data streams that traverse the UNC. Although the INC is protected by the SGW and any IDP internal to the UNC, Motorola recommends the use of several advanced security features in the INC itself. For instance, the INC's IMSI-spoofing check can protect against an unauthorized device spoofing an IMSI to gain network access. The INC's IMSI black/white listing feature enforces network policy by allowing only "known-good" IMSI traffic to pass through to the core network. The INC can also maintain an Access Point white list that allows "known-good" AP traffic to pass. Motorola always recommends hardening access interfaces, which limits exposure of INC to unnecessary network segments and interfaces.

UMA Network Element Hardening

Before a network element is connected to the UMA network, each of UNC subsystems must be

security hardened. This includes—but is not limited to—the system OS; application software packages; user-account management; IP communication protocols; third-party vendor equipment configuration; system growth/degrowth; security backup; and security patches.

UNC System Survivability

This design task reviews network resilience and reliability design, system data backup and recovery capabilities in order to look for potential system capacity degradations. The cause of system network failure could be anything from a single point of failure to insufficient configuration data backup. Survivability design may also identify a minimum configuration mode, where the system can fall back to a simplex mode that has less capacity, but more resilience. This applies to UNC and any of its subsystems. Included in a typical survivability checklist are the following items:

- Where is the configuration data stored?
- How often and securely is the configuration data backed up?
- How is the data recovered from a failure?
- How is an expected data change recorded, tracked, reported and recovered?
- Where are the SW and HW active-standbys on each traffic plane?
- Are all communication links redundant?
- If a failure occurs, what are the effects on system capacity, users and services?
- What is the potential business or revenue loss resulting from the above?
- Is there a recovery strategy for reacting to the above?

UMA Network Management Policies

Another aspect of advanced UMA security architecture design is the specification of technical

procedures, security provisioning policies, and security configuration for UMA network management, which must be formalized, optimized and aligned/integrated with the existing network management policy framework. Policy areas include:

- Password authentication procedures and policies
- Policies on use of telnet, FTP, rlogin, etc. within internal network
- User-account management policies
- System-configuration backup policies
- System-credential protection policies
- System-information/documentation policies
- Time-based provisioning policies
- Bandwidth policing policies
- Remote access procedures and policies
- Key distribution procedures and policies

OAM Interface Security

The Motorola UMA security solution protects both southbound and northbound interfaces to OAM. Depending what's available in the service provider's infrastructure, the security design enables HTTPS- or SSH-based secure communication protocol for administrative-user access; GUI and sFTP for software download and performance management; and SNMPv3 for fault management (DES, MD5, SHA-1). Motorola's UMA design recommends configuration of the OAM network using dedicated logical/physical OA&M interfaces and IP subnets, thus ensuring security in network operation and management activities. If the mobile service provider does not have this sort of protection in place for GPRS domains, this must be addressed immediately, or the UMA work will be in vain.

Access to OAM devices and the network is based on strong user authentication and access control.

All user logins and passwords are encrypted when transmitting to the network, using two-factor authentications, where possible, and SSH for secure remote-terminal access (replacing telnet, rsh, FTP, rlogin, etc.). IPsec VPN is mandatory for remote-access users.

OAM Firewall

This firewall, which separates the OAM network (also subscriber databases) from the rest of the UMA and core transport network, protects the OAM network from malicious access and DoS attacks. To reduce deployment costs, Motorola recommends the OAM firewall be part of the platform integrated with UNC firewall/IDP. The following firewall/IDP capabilities apply:

- Port filtering
- IP filtering
- IDP and DoS protection
- IP spoofing
- SYN attack
- Application proxy (for OAM transactions)

UMA Operational Security

Security industry studies and forensics have repeatedly found that people are the weak link in most security architectures. The fact is that the majority of security breaches and vulnerabilities can be traced back to human actions, many of which involve unintentional errors. Consequently, Motorola's operational security for UMA is deployable via a wide range of policies to ensure that people have the right procedures and processes in place—which means that security technologies can then do their job unencumbered by major human-factor weaknesses.

In order to provide the highest possible level of UMA/core protection, effective network security policies and procedures must take into account an organization's strategic and operational requirements; financial budgets; size and location; risk tolerance; legal and regulatory environment;

threat impact; network architecture; and security controls, etc. Key aspects of Motorola's operational security policies include recommendations for:

Processes:

- Improved administrative access-control procedures
- Enhanced administrative user authentication
- Improved administrative user-account management procedures
- Enforcement of password policy via password complexity check, Aging, Failed attempt, Idle user session timeout, etc.
- Role-based Access Control (RBAC) to minimize privileges for human users
- Security policy reviews for up-to-date security patches, secure configuration backup and patch-management processes
- Network security monitoring to enable audit trail, alarm and security-log correlation, and accountability review
- Restriction of the use of telnet, FTP and rlogin within an UMA internal management network
- Ongoing network and host vulnerability assessments to identify the security gaps in operational procedures, software and network configuration, and thus help UMA service providers understand their network-security posture and survivability needs

People:

- Subscriber privacy and service privileges
- Administrative user role definition
- Administrative user right and privilege definition
- Definition of job functions for key UMA service providers and related staff members
- Job qualification recommendations (UMA technical knowledge, vendor certification, etc.)

The operational UMA security capabilities recommended and specified by Motorola will ensure that security is integrated with everyday business activities and routine processes. With

this holistic and operational approach, the unique Motorola security integration and reference architectures can support high levels of overall network availability and reliability, while at the same time reducing operating expenses and decreasing network maintenance costs associated with security.

Reference Architecture Methodology

Motorola's UMA security design service complies with industry standards. In particular, the following three main security risk-analysis methodologies are used for the purpose of UMA design analysis:

- ETR 332: "Security Techniques Advisory Group (STAG); Security requirements capture." ETR 332 defines threat assessment principles for telecommunication systems.
- ITU X.805: "Security architecture for systems providing end-to-end communications." ITU X.805 is utilized as an architectural approach to analyze the UMA infrastructure from different layers, planes and dimensions.
- The National Security Agency (NSA) INFOSEC Assessment Methodology (IAM). The National Security Agency (NSA) INFOSEC Assessment Methodology (IAM) is also referred to here as a guideline of how the information security assessment should be conducted and delivered.

In addition, the Motorola UMA security design service complies with the following industry standards and best practices: ISO17799, NRIC Best Practices, UMAC Technical Standard Specifications, 3GPP Technical Specifications, NIST Published Guidelines and ANSI T1M1.

Summary

Current UMA standards and security products do not specifically address many of the threats within the context of a converged network environment to which UMA exposes a service provider's

network. Consequently, an experienced and disciplined approach, using best practices that identify critical security assets, weaknesses, threat vectors and risk tolerance, is required to tackle UMA security challenges. With the *Motorola Converged UMA Security Solution*, it's possible to have a comprehensive plan that will allow proactive mitigation and incident management on an ongoing basis. The Motorola process involves several key steps:

- Conduct a thorough *vulnerability and operational security assessment*, ideally before a service provider introduces UMA into the network and periodically thereafter.
- Design and deploy a *holistic security architecture* that includes the "people, process and policy" aspects of security in a zoned-based, defense-in-depth model unique to each service provider.
- Ensure the proper configuration of UMA *standards and best-of-breed security products*, and their integration within the UNC and core GSM/GPRS domains, using the security architecture as an end-to-end guideline.

With well-managed security integration and a well-designed security architecture, UMA can achieve its potential, creating a robust foundation for the deployment and management of new technologies and value-added services, higher ARPU, and greater customer loyalty. The fact is that, based on Motorola field assessments and UMA security reference architecture work, security is potentially a make-or-break issue for UMA. The good news is that UMA security is a potential competitive advantage and differentiator, considering that both business and residential customers are increasingly willing to pay for voice/data privacy/confidentiality/integrity, fraud protection, and high levels of service availability.