

Critical Elements of Pre-IMS Network Security for Wireless Carriers

White
Paper



High Performance Multi-threat Security Solutions

FORTINET™

Introduction

The capabilities of today's wireless mobile devices have advanced far beyond what they were only 10 years ago. Sending pictures using a built-in digital camera, changing ring-tones to popular musical tunes, surfing the Internet from a mobile device, or having a text message chat with another party would have been considered "*Star Wars*" technology in the early '90s, but are now considered mainstream "must-have" wireless functions.

And that's exactly what wireless telecom carriers want you to think. Most carriers have figured out that the key to their revenue and profit goals is not going to be based on getting customers to use more voice minutes. Instead, they're focused on getting customers to use "*richer*" media services, which generate incremental fees for the carrier.

"Rich" media runs along a continuum, from text messaging, fancy ring-tones and cell phone cameras at an entry level, to more sophisticated services such as VoIP, video, music, Internet Packet Television (IPTV), real time instant messaging (IM) and file transfer on the higher performance end of the media services scale.

The former (entry level) are called **Pre-IP Multimedia Subsystems**, commonly referred to as **Pre-IMS** services. The latter -- which operate on higher-performance 3rd generation (3G) and Fixed/Mobile Convergence (FMC) networks -- are referred to as **IMS** services. This article concerns itself with security issues for **Pre-IMS** services.

Pre-IMS can best be defined as enhanced media services that are somewhat beyond traditional voice services. Pre-IMS networks operate at both 2.5G and 3.5G performance levels and provide services such as Short Message Services (SMS) for voice and text messaging, and use a simple media protocol called MMS or Multimedia Message Services to accomplish tasks such as sending a picture or an audio file to another wireless subscriber.

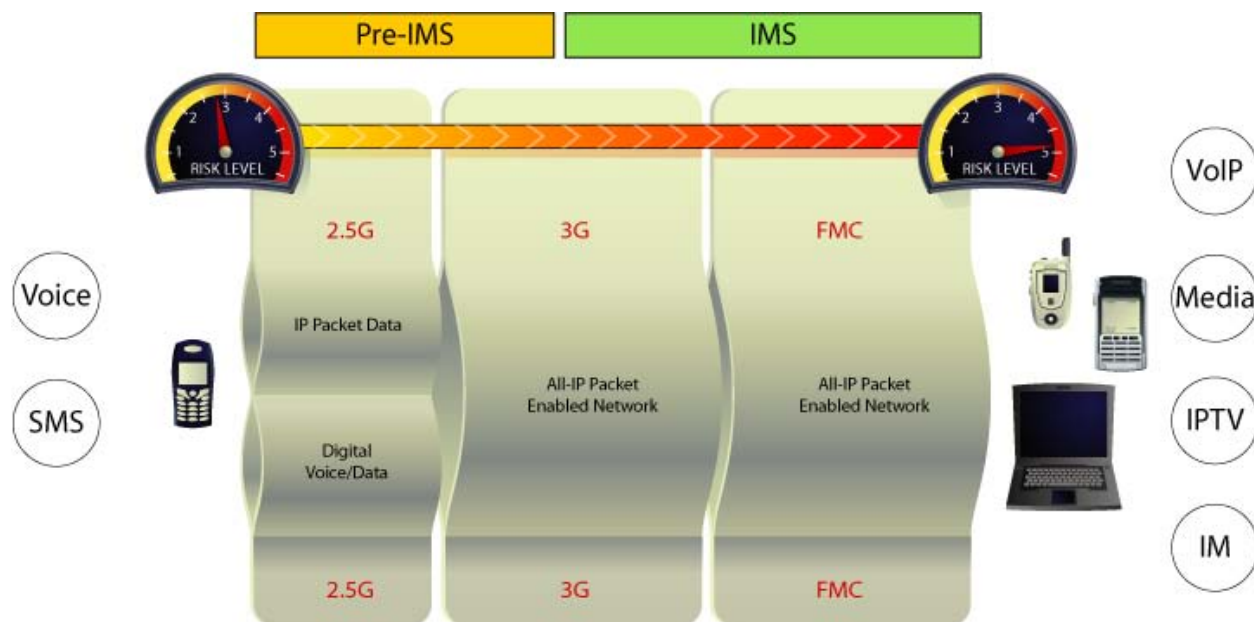
Like higher performance IMS networks, Pre-IMS networks also use SIP, or the Session Initiation Protocol, which is an open, standards-based technology based on the IP protocol standard. The SIP protocol is the primary means by which a Pre-IMS network sends text or picture messages over IP networks.

To mainstream the entry level of rich media functionality within their infrastructures, carriers are moving away from their previous dependence on more costly circuit-switched networks, to more open-based, IP-driven standard networks, allowing for greater flexibility, broader capabilities and lower operating costs.

Along with the many benefits associated with an open-standard network, there is also an increased potential for security risks. As part of the move to an open, standards-based architecture, telecom carriers are now faced with a host of new security threats that they were previously shielded from when they deployed closed and proprietary circuit-based networks.

The illustration in Figure 1 on the next page shows the comparison in performance between Pre-IMS and standard IMS networks as well as the increased security risks that are associated with each one.

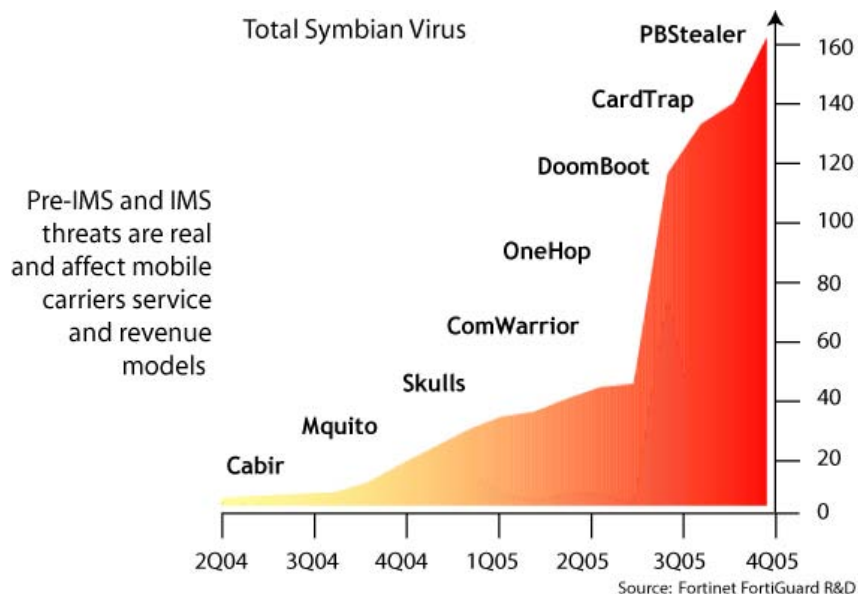
Figure 1: Comparing Pre-IMS to IMS Network Capabilities and Risks



Several of the security challenges that pose higher risks can be identified as follows:

- **Cyber-Risk Challenges** – which are technical threats to the open-standards model at the Application, Control and Transport layers of the infrastructure
- **Criminal Incentive** – attempts to defraud either subscribers and/or carriers in an effort to obtain monetary gain, notoriety, or credibility with their criminal peers.
- **Carrier Operational Challenges** – Technical threats to the open-standards model taking place at the Application, Control and Transport layers of the wireless infrastructure.

Figure 2: Pre-IMS Threats Are Real and Affect Mobile Operator Service and Revenue Levels



The illustration in Figure 2 on the previous page shows an example of how some of these risks have escalated over the past years. Because of increased risks, securing the infrastructure at all levels is now one of the primary objectives of today's telecom carriers as they move towards more open network architecture.

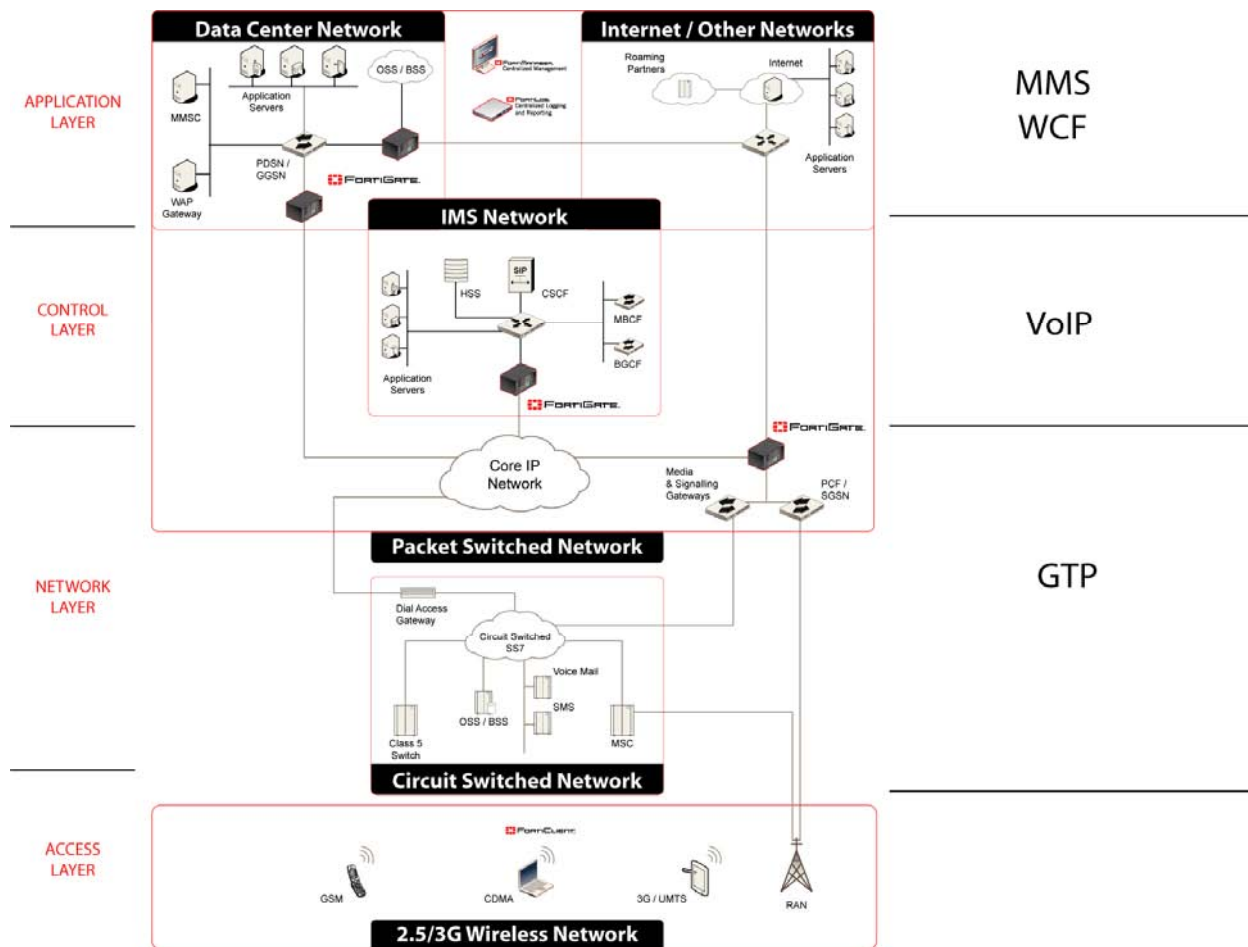
Understanding Pre-IMS Technology

Pre-IMS networks use an array of protocols – such as IP, GPRS, and MMS, as well as the most important and most prevalent SIP (Session Initiation Protocol) — for sending voice and/or data communications. These networks use the SIP protocol because it provides an easier and more open method of setting up and shutting down rich media applications over a wireless IP network. As the mobile world evolves towards greater Internet-enabled capabilities, SIP provides a pathway to build a single unified network, bridging the gap that previously existed between the mobile and Internet worlds.

Pre-IMS networks are comprised of four separate layers that work together to enable their media services (see Figure 3 on the next page). They are as follows:

- **The Application Service Layer** – which hosts such Pre-IMS applications as SMS text messaging, and MMS multimedia services supporting tasks such as audio downloading and playback, as well as sending pictures to another subscriber. This layer can also host WCF (Windows Communication Foundation) applications designed to run on Pocket PC, Windows XP and Windows Server 2003.
- **The Control Layer** – where the SIP protocols and signaling reside. The Control Layer is responsible for setting up the applications within the network and determining who has access to them. User and service administration as well as billing services are also handled in this layer.
- **The Transport Layer** – provides connectivity into the IMS network core, and determines how data packets travel from one device to another across the network. The device sends data through the Transport Layer, which then makes its way to the Control Layer, and finally to the Application Service Layer where the service is delivered to the user.
- **The Access Layer** – this portion of the network resides between the mobile device and the physical connection to the network (the cellular or radio tower). These towers provide the signaling that establishes the connection to the Transport Layer, providing access to the remainder of the network.

Figure 3: The Layers of the Pre-IMS Network Model



Understanding the Risks to Pre-IMS Networks

As the shift to an open network standard takes place, Pre-IMS networks have become more vulnerable to the same security risks as other IT open-standard networks, and the devices that run on them such as desktop or notebook computers. Since many of the so called “*smart cell phones*” and PDAs are running derivatives of operating systems such as Microsoft’s Pocket PC OS (which is based on Windows technology), these mobile devices and networks have also become targets of the same security threats as well. This includes risks such as viruses, worms, Trojan horses, Adware, Spyware and spam. For example a PDA that can receive e-mail attachments can also enable viruses, placing the device at the same level of risk to its operating system as a laptop or desktop computer.

The difference with an attack on a mobile device is that wireless users are often unable to take direct action to rid their device of a virus, as they would be able to on their desktop PC. Wireless users who receive a virus on their cellular phones can do little but call their wireless carrier. Therefore, if a virus is deployed, the wireless provider is ultimately responsible for resolving the problem. Of even higher priority is re-engineering a solution to prevent damage before the virus can spread and affect the rest of the network and user population.

Since the concept of viruses in wireless computing is relatively new, many carriers find that they are ill-prepared to address the problem on a global scale. If a large number of threats occur in a short span of

time, carriers will find that they are devoting a substantial amount of time and resources to addressing the problem, significantly increasing their operating costs and reducing their quality of service to users.

Threats to the Application Service Layer

One of the ways that hackers and cyber criminals gain access to Pre-IMS networks is through the Application Layer. Since SMS and MMS messages are two commonly used applications among wireless users, it is important to understand how these messages are sent and received over a Pre-IMS network. Below are three examples of wireless application threats and how they can impact Pre-IMS network security:

- **The SMS Text Message Service Threat** - Premium SMS services are promotional text messages that wireless carriers offer to businesses to promote a product, service, or media event. With this system, the promoter issues a request that the subscriber send a text message to a particular cellular number or text name in order to participate in a promotion. Television programs and advertisers use premium SMS services to allow viewers to submit votes or participate in a special contest or drawing. Premium SMS text message services are charged at a higher rate than standard text message rates. With the higher fees associated with this service, both the advertiser and the wireless carrier split the incremental charge, which, when multiplied by tens of thousands of participants, can add up to substantial incremental revenue for both the advertiser and the carrier.

The method by which the promotional fees associated with these Premium SMS services are sent to the advertiser leaves the network open to exploitation by cyber criminals. Using the SMS messaging system, cyber criminals issue a special offer by requiring that the user download a special application "*installer*" to their cellular phone in order to participate in the promotion. Once the software has been installed, it will replicate itself by sending a message to each number in the subscriber's cell phone address book using the same SMS service. It then begins to send an unlimited number of promotional messages from each replicated cell phone to the advertiser's account, thereby generating significant revenue credits for the cyber criminal. In most cases, users are not aware of the fraud until they receive their monthly statement and see the additional charges. By the time the carrier has been alerted and attempts to shut down the promoter's account, the funds have already been transferred to the criminal's account, which is typically located in an offshore bank well beyond the reach and jurisdiction of U.S. banking laws. Since the carrier is unable to reverse the charges, the customer and the carrier are stuck with the charges and must negotiate with each other to determine who will pay.

- **The MMS Service Threat** - The same principles involved with SMS text messages can also be exploited by cyber criminals in relation to MMS (Multimedia Messaging Service). With the richer media file structure associated with this service, each telecom carrier must establish separate profiles for each type of mobile device. This allows them to encode the multimedia data so it can be sent and received on all devices in a consistent fashion. In addition to pictures and animated images, MMS also allows a user to attach application files (such as games) to a text message so they can be sent to another mobile user whether the recipient is on the same wireless network or not.

Two specific examples of MMS threats are called "*ComWarrior*" and "*Mosquito*", which are application viruses that are embedded in online games designed to be played on cellular phones. To enable the game, the user is required to first register and pay for the game online. Normally this is a one-time charge. However, with the *Mosquito* virus, users would be charged a registration fee each time they launched the game, generating considerable revenues for the developer. Like the SMS scam, the threat would not be recognized until the subscribers received their monthly statements and notified the carrier, at which time the charges had already been transferred to the criminal's bank account, too late for any corrective action to be taken

- The Hidden Application Threat** - Instances where certain applications pretend to be something that they are not are exemplified by an application called RedBrowser. RedBrowser can be quickly downloaded and installed onto a mobile device from the Internet via Bluetooth or from a PC. Due to its relatively small size (only 54482 bytes), it can be downloaded fairly quickly. This application targets Java 2 Mobile Edition (J2ME), a technology which is used by approximately one *billion* mobile devices worldwide. RedBrowser claims to offer a “free-of-charge” SMS text messaging service that uses J2ME to attach to WAP-enabled sites (Wireless Access Protocol) without using a GPRS connection. In actuality, when an SMS message is sent, a Trojan horse virus sends the messages to several premium paid mobile services at a rate of \$5 - \$6 per message.

Telecom carriers estimate that approximately five percent of all SMS or MMS messages are infected by one or more of these viruses or criminal scams. This figure is expected to rise exponentially over the coming years, impacting an increasing number of wireless users. To reverse this trend, wireless carriers need to take steps to protect their network infrastructures and customers’ mobile devices. This can be best accomplished if carriers first understand how MMS messages are delivered over Pre-IMS networks.

Understanding MMS Messaging Interfaces

The MMS Messaging system has eight interfaces that are used to support specific capabilities and functions within the message delivery process. Depending on the type of application file and/or communication method, the appropriate MMS interface is assigned. The eight interfaces are given letter and number designations, titled MM1 through MM8. Figure 4 delineates the MMS interfaces and their corresponding functions.

Each message on the network is assigned an interface number based on its functionality and the type of device it is communicating with on the Pre-IMS network. Understanding how these interfaces are used for MMS messaging provides an insight into how they are exploited to deliver security threats.

The MM1 interface allows mobile devices to send and receive messages with a MMS Relay/Server where the messages are stored and forwarded. MM1 is the most important and most vulnerable of the eight MMS interfaces because of its widespread use among wireless users. The mobile handset is also connected to Bluetooth / WiFi and therefore extends the connectivity and hence the exposure to infection. The connection between Bluetooth to MMS Server can prove an expensive one for the end user! The MM3 interface supports gateways communications such as email with external service providers. The MM4 interface is reserved for intra-carrier communications and operations. The MM7 interface supports Value Added Service applications to send MMS messages, such as system administration-related notifications. The other interface types are not directly relevant to the transmission of content and are therefore excluded from this paper.

From a security priority perspective, **the greatest security risk to wireless networks is the MM1 interface** that hosts applications such as e-mail, text and picture messages, and games. If a virus enters the network, it will typically come in through the MM1 interface after being sent to the subscriber from another wireless user. Because of its wide use and

Figure 4: The MMS Interface Model
(Bold Interfaces Require Security)

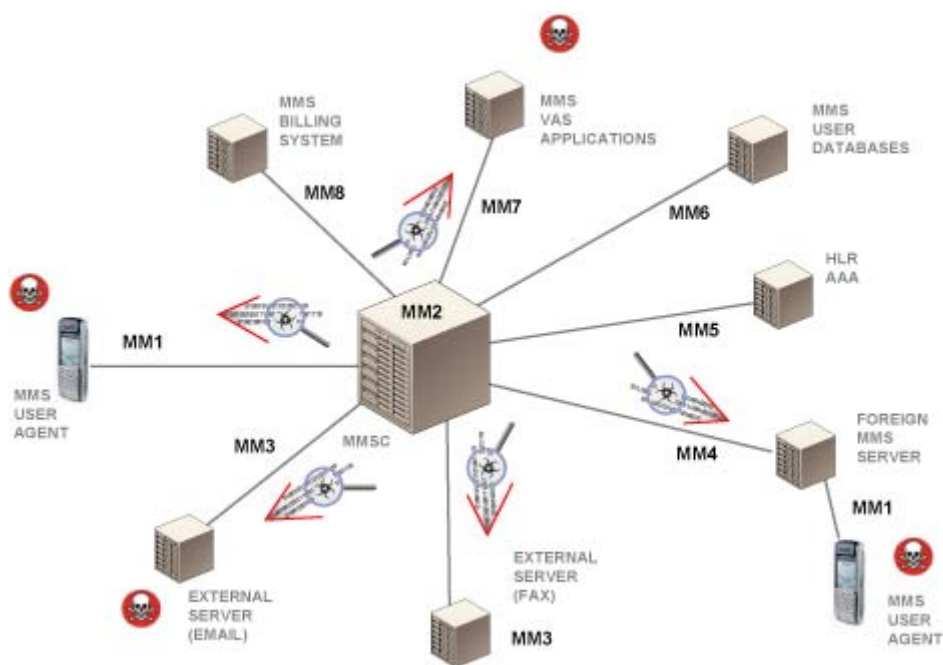
MMS Interfaces	
MM1	Application Send / Receive
MM2	<i>Reserved for Internal Processes</i>
MM3	Phone to E-Mail Messaging
MM4	Messaging from Other Carriers
MM5	<i>Home Location Register of User</i>
MM6	<i>Register User Database</i>
MM7	Value-Added Service Messages
MM8	<i>User Billing Database</i>

critical position as the delivery mechanism for messaging, it is the first interface that needs to be secured.

After MM1, the next level of security priority is the MM4 interface, which allows users on one wireless network to receive messages from subscribers on different networks. For example, in order for Wireless Carrier A to enable a subscriber to receive a text message with a picture attachment from Wireless Carrier B subscriber, Wireless Carrier A – using the MM4 interface — would design a profile representing both the unique device and the network attributes of the sender's network. They would also create profiles for every wireless carrier that offers a similar service, and for each device that is capable of delivering a picture attachment on both networks. Like MM1, the MM4 interface is another type of messaging application, making it just as susceptible to viruses as MM1-style messages. MM3 like MM4 extends the connectivity, providing the ability to use standard Internet style email to propagate malicious content.

The last area of priority vulnerability is with the MM7 interface, which is reserved for value-added service messages such as ringtones, generating and sending service notification messages to users, and sending and receiving simple video clips or animated static images. This interface represents an area of vulnerability from external messaging and needs to be secured in a similar fashion to that of the MM1 interface. The relationship among the MMS interfaces, the areas where they are most vulnerable, and their role within the Pre-IMS network environment is identified in Figure 5 below.

Figure 5: The MMS Interface Layers within the Pre-IMS Network Model



Web Content Filtering

The web browsers that are built into most cellular phones pose a different type of security vulnerability. Rather than external virus threats, the security issue with web content has to do with access to adult content. Access to this material can pose a legal, moral, or publicity-related threat to the wireless carrier if limiting access is not stringently enforced. In order to protect themselves from the threat of litigation or negative publicity, it is critical that wireless carriers have appropriate content filtering within their networks to ensure compliance with local, national, and federal laws regarding access to adult web content.

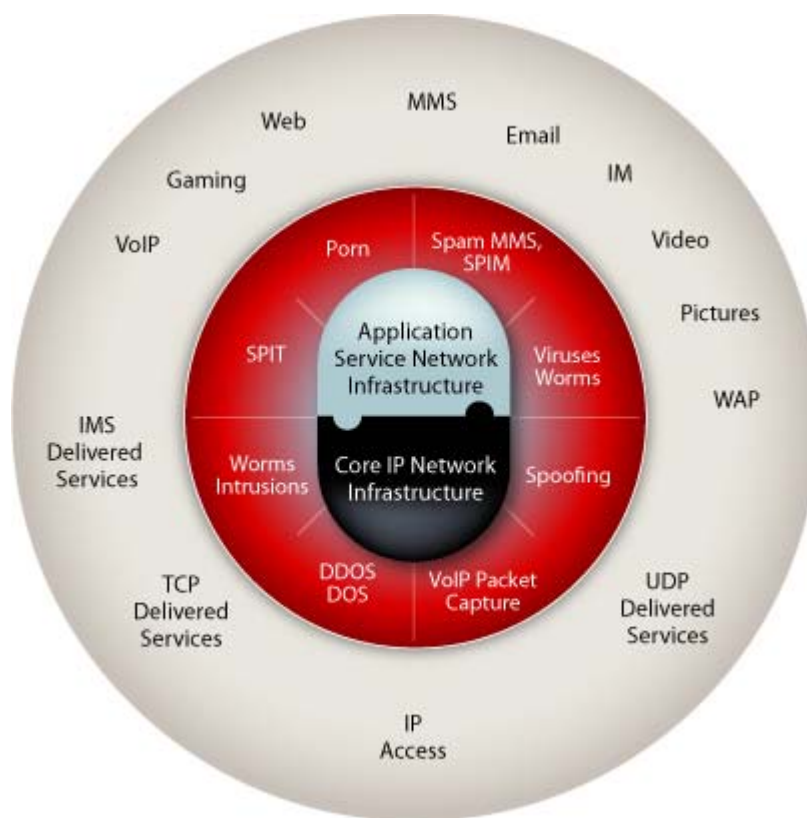
The most prevalent issue concerns the filtering of adult content in relation to underage wireless users. Wireless carriers must have effective web content filtering techniques within their Pre-IMS networks to

ensure that adults are the only ones who have been identified, authorized and granted access to view adult content from their cellular phones. With underage users that have their own Web-enabled cellular phones, or are part of a family-shared rate plan, this can be a challenge.

One way to meet this challenge is to enable adult content filtering at the Application layer through the use of a credit card authorization process that is tied to the user's cellular account number. When a user attempts to access an adult site using a web browser on the cellular phone, the network will verify that the user has a credit card in his or her name before it grants access. If the user does not, then access to the site would be blocked. Since most underage users do not have their own credit cards, this is usually an effective filtering approach.

Web content filtering is only one of many types of security risks that can attack wireless networks. Figure 6 on the next page, shows how these threats can occur at every layer of the Pre-IMS network model. Both the Control and Transport Layers also are vulnerable to a series of security risks which can be equally as threatening as those targeting the Application Layer.

Figure 6: Security Threats Occur at Every Layer of Pre-IMS Networks



Threats to the Control and Transport Layers

Security threats to the Control and Transport Layers of Pre-IMS, GPRS based networks take advantage of the GPRS Tunneling Protocol (or GTP) protocol which is used to deliver IP services to the wireless user. With GTP there is an identified start point and end point within an IP network on both 2.5G and 3G networks. Each mobile connection into the provider's network is initiated at the Serving GPRS Support Node (SGSN) terminating on a selected Gateway GPRS Support Node (GGSN) It is at the GGSN that the mobile connection links directly to the operators IP environment. after traversing their core infrastructure

within the GTP tunnel.. The GGSN on this network of tunnels can be compromised either by an overwhelming number of connections or badly formatted data packets, leading to poor network performance or a loss of service across the entire infrastructure.

Another threat to the Control and Transport Layers of a Pre-IMS network is *Address Spoofing*. When data is transmitted over wireless networks, users are billed by the byte, so the more bytes used while surfing the web or transmitting data, the more the customer is charged. If a hacker gains access to a user's account, he or she can tag onto the GTP protocol and use a victim's online address to surf the Internet. The billing system then charges the victim's account for the hacker's online time or byte usage thereby "*spoofing*" the system and avoiding any of the incurred online charges.

Other security risks enable malicious acts that impact network functionality. One of these is referred to as an "*under billing*" technique that uses the GTP protocol to bypass the network's billing system allowing one wireless user to communicate with another without incurring any usage charges. In other situations, a hacker can send malformed packets across the tunnel in an IP network, overwhelming it with badly-formed data resources. These malformed packets create problems for the carrier in maintaining high quality levels of service, as these packets impact quality for all the users on the network.

Like the MMS interface in the Application Layer, the Control and Transport Layers of the network also have three of their own GTP interfaces. They are:

- **Gn** – the interface that defines how packet data traffic travels between the GGSN starting point and the SSGN end point of the IP tunnel.
- **Gp** – the interface that defines how data travels between different wireless providers.
- **Gi** – the interface that defines how the tunnel uses the IP protocol to access IP services, including the Internet

To defend the Control and Transport Layers of Pre-IMS networks, wireless carriers must defend the GTP protocol, the data packets that use GGSN and SSGN tunneling, and each of the three GTP interfaces to prevent unauthorized address spoofing, over and under billing, and other forms of malicious network packet disruptions that enable cyber crime and result in poor network performance.

Pre-IMS Operational Infrastructure Security Requirements

Defending Pre-IMS networks involves more than merely putting up network roadblocks that curtail certain behaviors. Care must also be taken to ensure that any defensive measure does not disrupt legitimate network traffic. An effective security solution must analyze all network traffic, make an appropriate determination in separating which packets are good from those that are bad, and then take appropriate action to thwart any security risks before they can impact network traffic performance or disrupt network operations.

Therefore an effective defensive strategy must not only employ thorough security measures, but must also include sound management tools that can be deployed across each layer of a Pre-IMS network in order to combat security risks and cyber crime without disrupting overall network performance.

Below are some of the requirements that wireless carriers should take into account when considering vital administrative and management tools for deploying an effective Pre-IMS network defense strategy:

Application Layer Requirements

One of the areas that wireless carriers must be on guard against is an over-zealous defense strategy. Two things that wireless carriers need to take care to minimize are *False Positives* and *False Negatives*. If these occur at a high rate, then either a significant amount of legitimate data traffic will be blocked, or a large number of network threats will be allowed to gain network access.

Any deterrence solution should employ a combination of identification and analysis techniques coupled with rich, up-to-date security content to minimize false positives and false negatives across the network.

False positives occur when a network threat analysis triggers an alert and/or responsive action although there is no actual threat. When a detection solution produces false positives, it can disrupt normal business operations by interfering with legitimate traffic. The opposite error, *false negatives*, occurs when the detection system does not accurately detect an actual security threat, which usually results in the threat gaining network access, causing significant damage. In the case of false negatives, the defensive mechanism provides no warning about attacks—making the outcome particularly dangerous. While it is almost impossible to reduce false positives and negatives to zero, any deterrence solution should employ a combination of identification and analysis techniques coupled with rich, up-to-date

security content to minimize false positives and false negatives across the network.

Another over-zealous action that carriers need to be on guard against is the desire to put in place defensive actions that will block every occurrence of a particular data type. In the case of Symbian SIS install files (which were responsible for carrying the *ComWarrior*, *Mosquito* and *Doom Boot* viruses); an understandable defense response would be to block all Symbian SIS install files from gaining access to the network. But initiating such a broad-brush approach would also prevent users from installing *legitimate* application solutions on the Symbian platform.

Instead, a more reliable approach that would provide a good balance between effective security and *appropriate* access would be to employ the use of a *Data Analysis Filter*. This technique leverages a regularly-updated database of current virus descriptions and also scans a particular type of incoming files against the database in order to analyze and determine which install files should be granted network access. This poses less risk to network security, but also eliminates known threats without disrupting the flow of legitimate and/or safe data packets across the network.

Control and Transport Layer Security Requirements

Unfortunately, current wireless network designs have not been optimized for data communications. The restrictions imposed by IP protocols and the manner in which they encapsulate data generally impede the performance of data traffic over wireless networks.

To improve performance, developers created the WAP protocol. WAP stands for the Wireless Access Protocol. WAP works by stripping off the standard IP-protocol from the data packets and replacing it with UDP (User Datagram Protocol), enabling more efficient data packets, which improve network performance. When a user gains access to a website via a cellular phone, the device communicates with a WAP gateway, which reformats both the text and graphics to the WAP format.

With a WAP gateway in place on the network, wireless carriers have the ability to analyze WAP-formatted data packets before they enter the network and/or the user's wireless device, providing the ability to secure the Pre-IMS network from rogue or malicious applications that might enter in this fashion.

Management Requirements

Given the scope of potential security threats to a Pre-IMS network, it is important for network and security administrators to conduct in-depth trend analyses to detect the source of the threats and their repercussions on the network. Without sophisticated management tools, a network administrator cannot enlist the appropriate measures to best defend the network, improve performance, and/or enable new media services.

As part of an effective network management strategy it is important to generate reports that provide trend analyses that allow network and security administrators to take the necessary actions to resolve problems

or improve network capabilities. The information that network and security administrators can gain from a trend analysis report might indicate:

- How the network is performing at any layer
- What level of performance would be required to accommodate the current traffic load and the anticipated future traffic load
- A real time snapshot of what portion of the current wireless user base is using the network
- Which mobile devices are giving the network the most problems or are infected with the most viruses
- Which external wireless networks are the sources of the greatest security threats
- Which users or groups of users are generating the most revenue for the carrier

For example, if management tools indicate that the number of viruses on the network has escalated from 100 to 10,000 per day, with proper tools, network and security administrators could also quickly determine what factors caused that increase and what the primary source(s) were. Armed with that information, they could develop effective strategies to resolve the problems.

With superior management tools, carriers can also initiate more effective marketing promotions and higher quality customer service programs, issue more timely technical notifications, and/or initiate appropriate responses to thwart threats before they cause damage to the network.

Flexibility Requirements

Another important element in a Pre-IMS network is the degree of *flexibility* — the element that allows network managers and security administrators to quickly respond to changing network conditions. The use of an appropriate level of flexibility can mean different things depending on the network circumstances and the peripheral issues.

For example, some wireless providers can have tens of millions of mobile devices that are operational at any particular point in time. If half of their users are surfing the web at any given time, the WAP gateway on the network must be flexible enough to scale to a level that will filter all the incoming data traffic without bringing down the performance level for users who need the text messaging, voice, or file transfer features during that same period.

Flexibility also means efficient use of network resources. The ability to deploy solutions that address specific security issues on any layer of a Pre-IMS network not only provides flexibility but also delivers cost effectiveness. An essential requirement here is to ensure the ability to leverage a security solution that might have been originally designed for one layer, and have it work in the other layers just as well — either subsequently or simultaneously.

Performance, Scalability and Availability Requirements

Network performance, scalability and availability are critical to service delivery and to ensuring a high quality user experience

While not directly related to security, an important component in managing the capabilities of a Pre-IMS network is to appropriately match network performance to user requirements.

When networks are able to support rich media content such as real time video conferencing or movie casting, then robust network performance, scalability, and availability become essential in

delivering a quality user experience. But with data services such as text messaging and static picture attachments that employ store and forward techniques, the issues of robust performance, scalability, and availability become less critical. Under these circumstances, scalability depends more on the number of users that are simultaneously using the service rather than the type of data that is being transmitted. Therefore, wireless carriers need to make sure that they are not deploying a solution that is beyond their current network requirements capabilities.

The type of information being transmitted across a wireless network should also dictate the type of equipment used, so that it can best match the level of performance, scalability and availability necessary to meet user demands for each network environment.

Given the magnitude of issues that wireless telecom carriers need to consider in their efforts to better secure and manage their networks, it becomes exceedingly important that the solutions they choose satisfy each of the above-referred-to requirement-related issues. A solution that accomplishes this is the

FortiGate™ 5000 ATCA Multiservices Security Gateway Solution for Pre-IMS Networks.

The Fortinet Solution for Pre-IMS Networks

FortiGate™ 5000 ATCA Multiservices Security Gateway Solution

The *FortiGate* 5000 series ATCA-based platforms are carrier-grade network security solutions that are enabled by the modular *FortiGate OS™* distributed software system. The FortiGate 5000 provides scalable, multi-gigabit capacities that meet the most stringent carrier requirements for security, performance, reliability and availability.

The FortiGate 5000 Series solutions fulfill the promise of effectively securing Pre-IMS networks in the following ways:

- Providing a Robust Security Platform
- Supporting an ATCA Standards-Based Hardware Chassis and Server Blade Design
- Ensuring Network Performance and Service Integrity
- Ensuring Effective Management and Analysis
- Providing Flexible Pre-IMS Security Deployment

A Robust Security Platform

All FortiGate solutions, including the 5000 series, provide a *single source* solution for telecom carriers seeking to secure their Pre-IMS network in the most effective way possible. Traditional network security solutions involve the procurement of a variety of hardware, software and security subscription services from several vendors for each layer of the network model, which in turn requires an additional expense for each layer of desired security.

FortiGate Security Platform solutions simplify this process by providing a cohesive and integrated strategy of hardware, software and services that work together to form a highly secure solution that protects each layer within the Pre-IMS network. The three most critical components of this integrated solution are: *Targeted Security Modules*, *Updated Security Subscription Services*, and *Protection for GTP and MMS Interfaces*.

Component #1: Targeted Security Modules

As part of the FortiGate 5000 solution, Fortinet offers an extensive array of security modules that are designed to defend the network against the unique threats that target the individual layers of the Pre-IMS

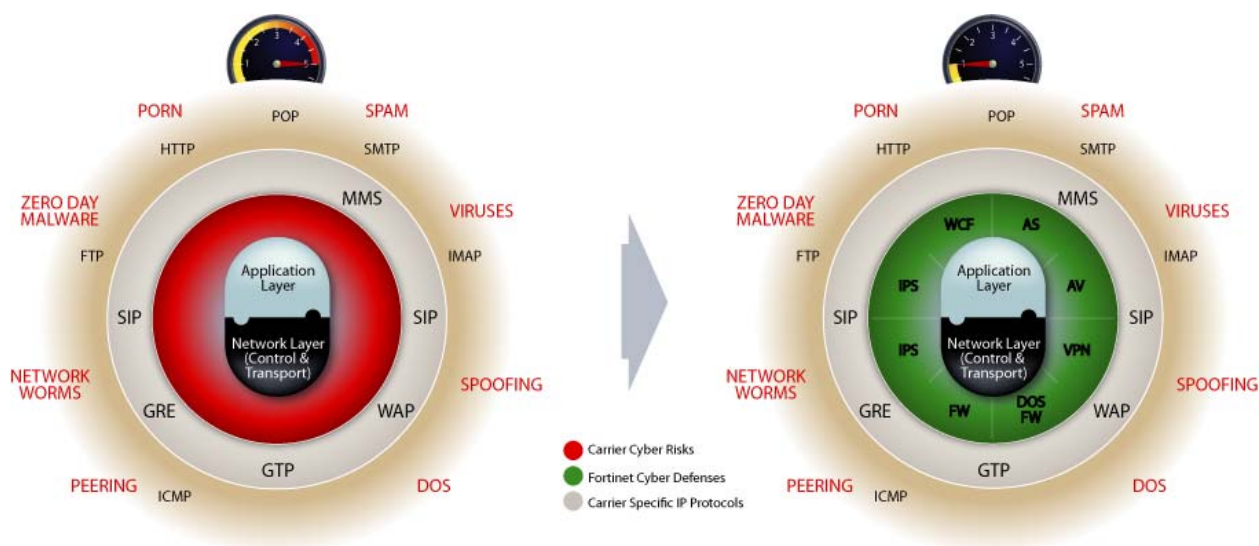
network. A list of these security modules and the types of threat that they provide protection for are listed in Figure 7 below:

Figure 7: FortiGate Security Modules Target Specific Network Layer Risks

Security Modules	Pre-IMS Risks
Application Layer	
Anti-Virus	Viruses, Spyware, Malware
Web Content Filtering	Inappropriate Web Content
Anti-Spam	Spam
Internet Protocol Suite	Service Protocol Intrusions
Control Layer	
SIP IPS	SIP Protocol Intrusions
Transport Layer	
Firewall	Topology Hiding, Network Policy Violations
Virtual Private Network	Illegal IP Traffic Capture

With the deployment of targeted security modules, a protective shield is formed that diminishes the security threats against the layers of the Pre-IMS network, leading to a fully protected network infrastructure, as illustrated in Figure 8 below.

Figure 8: Targeted Modules Provide Pre-IMS Network Layer Protection



Component #2: Updated Security Subscription Services

With the deployment of FortiGate Security Modules, the *FortiGuard™ Center* (the security subscription service for FortiGate products) provides a comprehensive source of information and software updates that are automatically pushed down to each of the security components that have been enabled by the carrier administrator. This ensures that each module is running with the most updated security descriptions at any point in time. This also provides automatic configuration on a real time basis and assures network and security administrators that they will always be working with the most current security knowledge available to thwart any potential security risks to the network.

The FortiGuard Center updates are cached in real time from the Fortinet global database to a locally-hosted service provider database. This hierarchical architecture enables service providers to flexibly customize their protection configuration while maximizing performance, ensuring security, and sustaining highly effective service levels.

With FortiGuard Center, carriers gain the following advantages:

- Automated Updates – Keeps defenses up-to-date against the latest viruses, Spyware, & heuristic engines.
- Industry-Leading Threat Response Time – Fortinet beats the competition, offering signature updates to block the latest attacks.
- Proactive Threat Library – Protection from thousands of popular OS and application threats and vulnerabilities.
- 24x7 Worldwide Coverage – Over 50 distribution servers are deployed in 12 different countries around the globe.
- Per Device Subscription Services – Significantly lowers subscription costs versus traditional per user licensing models.

Fortinet's security subscription services are created, updated and managed by a global team of Fortinet security professionals working around the clock, seven days per week, to ensure that the latest threats are detected and blocked before they can harm a network. This team constantly mines the Internet for new and emerging threats, and creates the security counter-measures that protect Pre-IMS networks against these threats.

With the combination of FortiGuard's Targeted Security Modules and Updated Security Subscription Services, Fortinet provides the fastest response times for providing new security updates in the industry. These software components work in conjunction with FortiGate ATCA-compatible server blade hardware to form a complete, integrated solution to ensure a robust Pre-IMS security platform.

Component #3: Protection for MMS and GTP Interfaces

To provide a highly effective level of security for all of the GTP and MMS interfaces, Fortinet offers FortiGate and FortiGuard real time scanning solutions. With FortiGate, the same appliance can perform scanning of all of the MMS interfaces, including the four most critical ones: MM1 (Handset), MM3 (Internet Gateway), MM4 (Operator Communications), and MM7 (Value-Added Services). The interfaces are constantly scanned on a real time basis by FortiGuard software and are updated via the FortiGuard Network. This ensures that the FortiGate appliance is using the most updated virus definitions, which will prevent any unauthorized intrusion from rogue or malicious software programs that might impact any portion of the Pre-IMS network.

In the event of a security breach, FortiGate will generate a security report based on the MSISDN (Mobile Station International ISDN Number) standard which identifies the details of a breach within the network,

the specific MMS interface, and the subscriber information that was responsible for the intrusion. The FortiGate solution for MMS security is illustrated in Figure 9 on the next page.

For securing the risks associated with GTP tunneling and the Gi Interface, FortiGate provides the following security benefits (see Figure 10):

- ✓ GTP packet sanity check, length filtering and type screening
- ✓ GSN tunnel limiting and rate limiting
- ✓ GTP stateful inspection
- ✓ Hanging GTP tunnel cleanup
- ✓ GTP tunnel fail-over for high availability
- ✓ GTP IMSI prefix (up to 1000) and APN (up to 2000) filtering
- ✓ GTP sequence number validation
- ✓ IP fragmentation of GTP messages
- ✓ GGSN and SGSN redirection
- ✓ Detecting GTP-in-GTP packets
- ✓ GTP traffic counting and logging

✓ Figure 9: How FortiGate Secures the MMS Interfaces

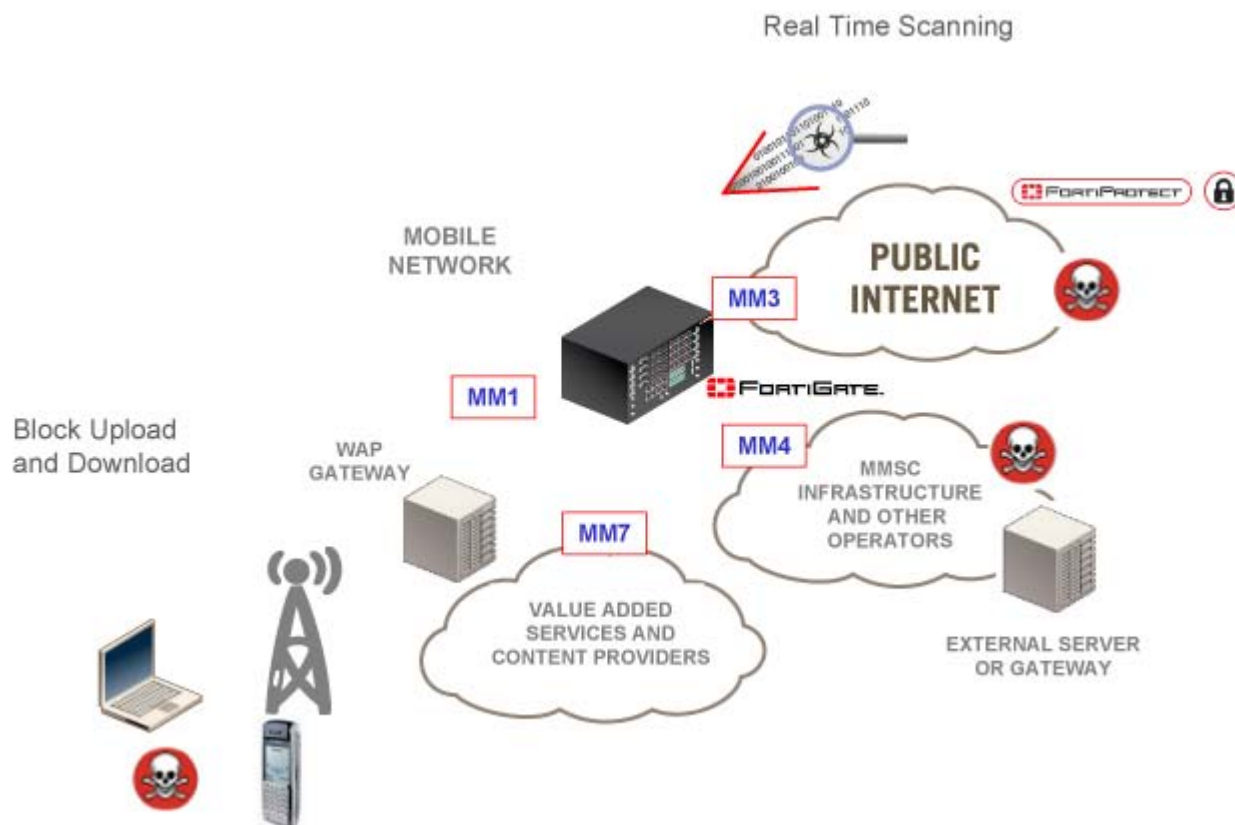
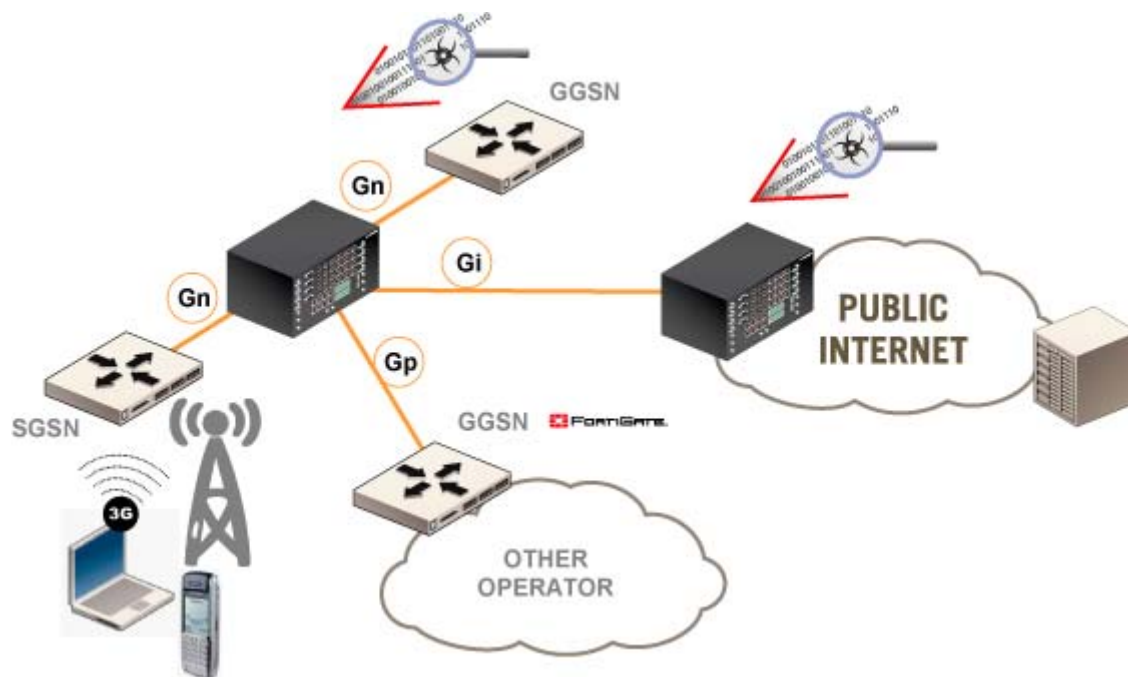


Figure 10: How FortiGate Secures GTP Tunneling and the Gi Interface



Standards-Based ATCA Hardware Chassis and Blades

In addition to an effective software and update subscription strategy, telecom carriers must also ensure that each security device and module throughout the network adheres to a single and rigid hardware standard that supports one uniform platform. Today, that standard is ATCA, which has gained widespread acceptance due to the flexible functionality it provides to network administrators. By deploying ATCA-compliant hardware devices, administrators can mix and match different components with the assurance that each device will maintain a familiar degree of consistent functionality across the network wherever those devices are deployed.

Fortinet is the only Pre-IMS network security provider that supports the ATCA standard for all of its hardware devices.

Supporting each FortiGate ATCA hardware blade is the *FortiGate OS™*, which enables each FortiGate security software module. This empowers telecom carriers with a choice of the exact security solution that best fits the individual needs of their network, whether at the Application, Control, or Transport Layers, or any combination thereof. The FortiGate security platform approach provides assurance that the entire network infrastructure will remain highly secure.

To date, Fortinet is the only Pre-IMS network security provider that supports the ATCA standard for all of its hardware devices, providing administrators with the flexibility and control they are seeking to support their existing network security strategies.

Network Performance and Service Integrity

To enable robust network performance, bandwidth and throughput must be maximized. Traditional solutions that use standard computer configurations as the foundation of their network security solutions impose performance limitations to network bandwidth and throughput as part of their design. For example, network and security administrators operating a PC-based IPS security point product running over a 1-gigabit traffic can potentially see their total network throughput reduced to a mere 200 megabits

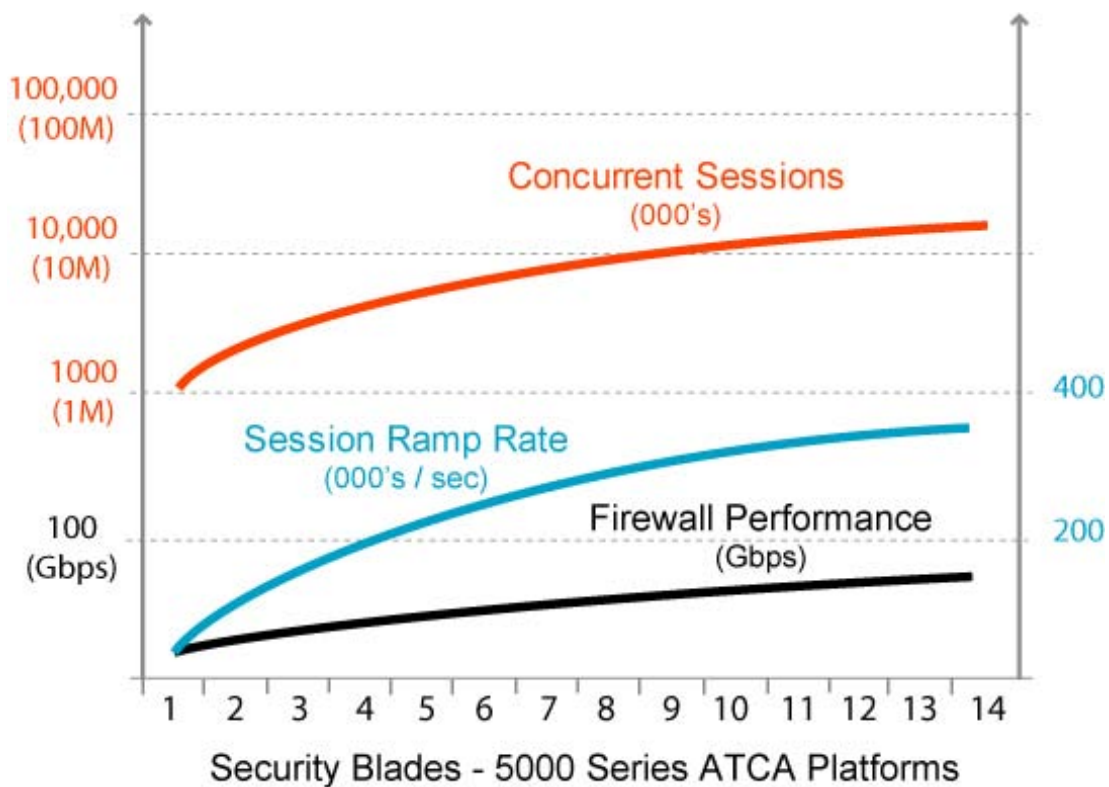
due to limitations imposed by the inherent designs of the architecture of the PC component running the security software.

The FortiGate 5000 Security Gateway solution employs a unique hardware architecture that is designed to maximize network bandwidth and throughput. FortiGate leverages the use of specially designed ASICs (Application Specific Integrated Circuits) that run specific portions of the security software, eliminating the bottlenecks that can otherwise restrict network performance. These ASICs are deployed within the FortiGate ATCA hardware blades, maximizing network performance at every level of the Pre-IMS architecture. So if Firewall, VPN, and IPS security are all turned on, the ASICs will ensure that the simultaneous use of all these modules will not affect the network bandwidth, throughput, and connections-per-second, nor impact overall network performance and service integrity.

The illustration in Figure 11 below illustrates how this ASIC design translates into robust network performance within the Pre-IMS network architecture while providing protection against the various security threats, and without degrading functionality or performance at each network layer.

With the FortiGate 5000's use of ASICs that are embedded in both the chassis and ATCA hardware blades, administrators can re-provision the blades from one network location to another without concern over degrading network performance in the new location. To accomplish this, all the administrator needs to do is re-license the FortiGate security software module for that new deployment scenario and install the FortiGate ATCA blade in the FortiGate ATCA chassis. Once accomplished, the ASICs will automatically detect the new location, register itself onto the FortiGuard Center, and download and install any new updates for that server. The ASICs will also ensure that the performance and service integrity of the server blade at the new location is equivalent to its performance at its previous location.

Figure 11: How ASIC Design Translates into Enhanced Network Performance



Effective Management and Analysis

Fortinet also offers a wealth of valuable management tools that provide detailed analysis of the status of each software, hardware, and service component within the FortiGate 5000 system. *FortiManager*[™] and *FortiAnalyzer*[™], for example, can collate data (such as information logs) from each of the FortiGate ATCA blades and use it to process detailed analytic reports that help network and security administrators and managers better understand what is taking place within each blade, layer, and network.

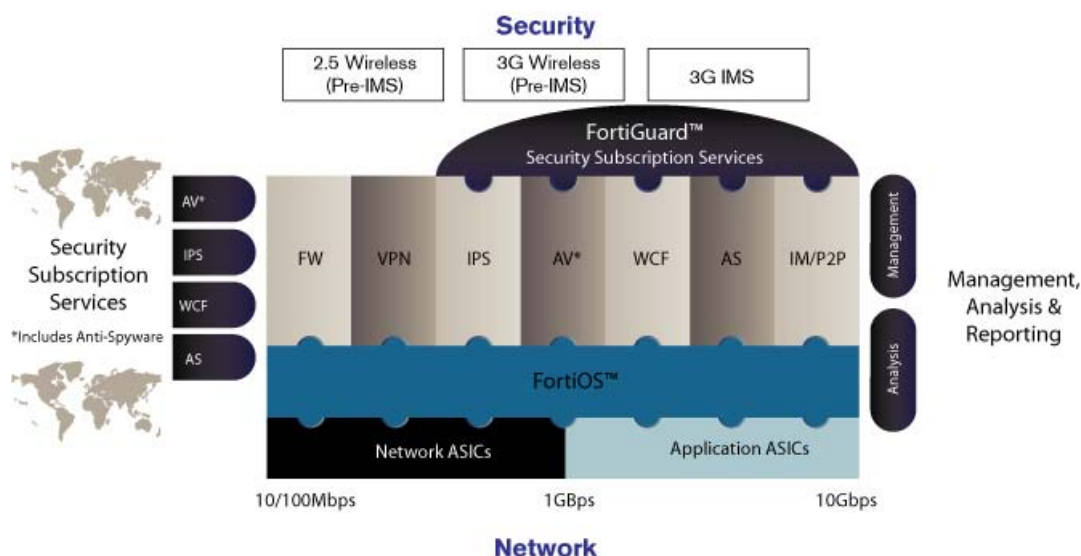
The *FortiAnalyzer*[™] family of real time network logging, analyzing, and reporting system is a series of dedicated hardware solutions that securely aggregate and analyze log data from FortiGate security appliances. The systems provide network and security administrators with a comprehensive report of network usage and security information, and support the needs of enterprises and service providers responsible for discovering and addressing vulnerabilities across FortiGate systems. The FortiAnalyzer appliance minimizes the effort required to monitor and maintain acceptable user policies, identifies attack patterns, prosecutes attackers, and complies with governmental regulations regarding privacy and disclosure of security breaches. FortiAnalyzer also accepts and processes a full range of log records provided by FortiGate systems including traffic, event, virus, attack, content filtering, and email filtering data. In addition, FortiAnalyzer provides advanced security management functions such as quarantine archiving, event correlation, vulnerability assessment, traffic analysis, and content archiving.

The *FortiManager*[™] System is an integrated management and monitoring tool that enables enterprises and service providers to easily administer large numbers of FortiGate Antivirus Firewalls. It minimizes the administrative effort required to deploy, configure, monitor, and maintain the full range of network protection services provided by FortiGate devices, and supports the needs of enterprises and service providers responsible for establishing and maintaining security policies across multiple, dispersed FortiGate installations.

Telecom carriers that already have other fraud detection technologies can use these analytic reports to detect anomalous behavior or activity within an individual subscriber's account in order to prevent a security breach from impacting the rest of the Pre-IMS network.

The illustration in Figure 12 below shows the relationship among the four components of the FortiGate Security Modules, the FortiGate ATCA hardware blades, the FortiOS operating system, and the FortiGuard Security Subscription Services — and how they work together to ensure the most complete and robust security solution possible for today's Pre-IMS networks.

Figure 12: The Integrated FortiGate 5000 Network Security Solution for Telecom Carriers



Flexible Pre-IMS Security Deployment

The FortiGate 5000 series for Telecom Carriers affords network and security administrators the highest degree of flexibility in how they deploy security across their Pre-IMS networks. This multi-layered approach allows them to deploy security at any layer that is appropriate, whether for the Application, Control, or Transport Layer of the Pre-IMS network.

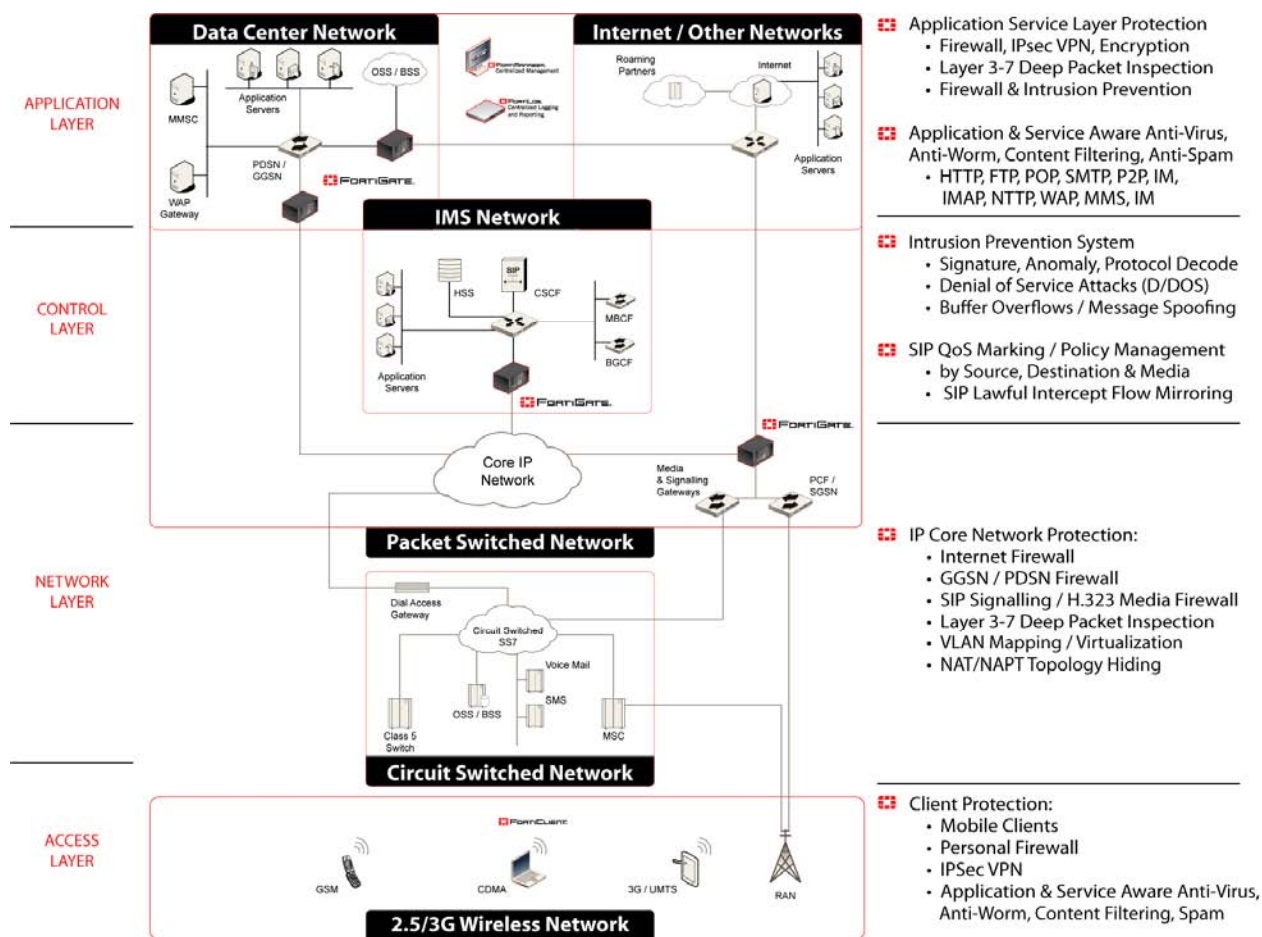
Securing the Access Layer

Access Layer security is addressed with the *FortiClient™ Mobile*, a software solution that resides on a Symbian, Windows Mobile 5 or Linux-enabled Smart Phone or PDA.

With conventional network security solutions specifically designed for a particular network layer, administrators are often locked into dedicating that solution solely for one area. For example, a security server designed to address a threat at the Application Layer can only be used in that layer. In the event that a new security threat surfaces to attack the Control or Transport Layers, the administrator cannot re-deploy that solution to other layers without severely degrading overall network performance. With FortiGate 5000, solutions can be deployed across multiple layers while maintaining high levels of network performance. This provides the unusual combination of effective security, high performance AND cost effectiveness across the Pre-IMS network.

The flexible capabilities inherent with the FortiGate 5000 Security System design can be deployed across any layer of the Pre-IMS model as illustrated in Figure 13 below.

Figure 13: The FortiGate Flexible Security System Supports Each Network Layer



Summary

Wireless telecom carriers ready to embark on the new frontiers of rich media services to drive ARPU and reduce costs have begun to embrace the Pre-IMS network standard and the technological benefits associated with its architecture to effectively deliver new services to their subscribers. Legacy network security strategies that were acceptable under closed, circuit-based architectures have been completely revisited and redesigned to fully protect networks from new security threats that jeopardize network uptime, service availability, and carriers' profits.

To successfully secure IMS and Next Generation services, security strategies must take into consideration the unique attributes of each layer of the Pre-IMS network model, namely the Application, Control, Transport, and Access Layers, as well as each individual subscriber's mobile devices. This requires deploying multi-layered security solutions at each layer to protect the network against security threats both now and in the future.

Fortinet is the only single-source partner that empowers telecom carriers with the capability of securing next-generation Pre-IMS infrastructures and services. With Fortinet, telecom carriers have the tools, technologies, and solutions to enable a robust security strategy and provide management with the assurance that new application services can be *securely* deployed to their telecom customers. With Fortinet, carriers can seize new market opportunities as they arise, and grow revenues that will meet both today's and tomorrow's business goals.

For more information about Fortinet carrier security solutions please visit the Fortinet solution website at: <http://www.fortinet.com/products/carrier.html>

About the Authors

Freddy Mangum - Vice President, Products

As Vice President of Product Management, Emerging Technologies, Freddy Mangum is responsible for driving strategy and demand for Fortinet's products. Freddy brings to Fortinet more than 12 years of sales, marketing and business development experience with companies in the networking and security markets. Freddy holds a B.S. in economics with honors from George Mason University and has completed additional studies at American University, Georgetown, University of Colorado, Stanford and Princeton.

Darren Turnbull – Senior Consulting Engineer

As a Senior Consulting Engineer within the Solutions and Carrier Business Group at Fortinet, Darren Turnbull has been responsible for ensuring the development of Fortinet's mobile carrier solution meets both the functional and performance requirements demanded by today's mobile operators. Prior to Fortinet Darren spent several years at Cosine Communications and British Telecomm in the UK in a variety of senior operational and network design roles.

Appendix: The Pre-IMS Security Checklist

The table in Figure 14 below provides a checklist of specific features that wireless carriers should consider when evaluating any Pre-IMS network security solution:

Figure 14: Checklist for an Effective Pre-IMS Network Security Strategy

Security Layer Requirement	Check Off ✓
Application Layer Requirements	
Protection from ComWarrior Virus	
Protection from Mosquito Virus	
Protection from RedBrowser Applications	
Protection for Symbian OS wireless devices	
Minimization of False Positive Reporting	
Minimization of False Negative Reporting	
Web Content Filtering	
Control Layer Requirements	
GTP Protocol Analysis	
SSGN Protocol Analysis	
GGSN Protocol Analysis	
Protection from Address Spoofing	
Protection from Over Billing	
Protection from Under Billing	
Protection for Gn, Gp, and Gi Interfaces	
Support for WAP Gateways	
Transport Layer Requirements	
Scalability	
High Performance	
Flexibility	
Trend Analysis	
Access Layer Requirements	
Protection at the Mobile Device Level	
Security Support for Microsoft Windows Mobile Devices	
Security Support for Symbian OS Mobile Devices	
Management and Analysis Requirements:	
Ability to Scale to Meet Throughput Requirements for Rich Media Applications	
Provisions for Future Growth to Accommodate Tomorrow's Application Needs	
Ability to Maintain High Availability	
Provision for Multiple Layers of Backup Redundancy	
Flexible Network Management and Administration Tools	
Ability to respond rapidly to changing Security Threats	
Online Reporting of Security Threats	
Built In ASICs to Accelerate Network Performance	
Ability to Mix and Match Components to any Layer	
Automatic Software Update for each Hardware Device	
Support for the ATCA Hardware Standard	

Glossary

3G - Usually used in the context of cell phones, 3G is short for *third-generation* technology. The services associated with 3G provide the ability to transfer voice data, for example, from a telephone call, and non-voice data, for example from downloading information, exchanging email, and/or instant messaging. In marketing 3G services, video telephony has often been called the "killer application" for 3G.

3GPP - The 3rd Generation Partnership Project (3GPP) is a collaboration agreement that was established in December 1998. It's a co-op project among ETSI (Europe), ARIB/TTC (Japan), CCSA (China), ATIS (North America) and TTA (South Korea). 3GPP specifications are based on evolved GSM specifications, now generally known as the UMTS system.

ASIC - An ASIC (Application-Specific Integrated Circuit) is an integrated circuit (IC) customized for a particular use, rather than intended for general-purpose use. For example, a chip designed solely to run a cell phone is an ASIC. In contrast, the 7400 series integrated circuits are logic building blocks that can be wired together to perform many different applications. Intermediate between ASICs and standard products are application specific standard products (ASSPs).

ATCA - Advanced Telecommunications Computing Architecture is the largest specification effort in the history of the PCI Industrial Computers Manufacturers Group (PICMG), with more than 100 companies participating. AdvancedTCA as it is known, is targeted to requirements for the next generation of "carrier grade" communications equipment. This series of specifications incorporates the latest trends in high speed interconnect technologies, next generation processors, and improved Reliability, Availability and Serviceability (RAS).

False Negative - The term False Negative is used when spam email is not detected as such but rather classified as non-spam email. A low number of false negatives are an indicator of the efficiency of spam filtering methods. A False Negative occurs when filtering allows a spam email to be delivered to a user's inbox.

False Positive - The term False Positive is used when spam filtering or spam blocking techniques wrongly classify a legitimate email message as spam and as a result interfere with its delivery. The term False Positive is also used when antivirus software wrongly classifies a file as a virus. The incorrect detection may occur either by heuristics or by an incorrect virus signature in a database. Similar problems can occur with antitrojan or antispyware software.

FMC - Fixed/Mobile Convergence (FMC) became one of the key trends of the telecommunications industry in 2005. The IP Multimedia Subsystem (IMS) is a standardized Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardized implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. IMS was originally designed for mobile networks, but with the addition of TISPAN in release 7, fixed networks are supported too. This is called Fixed/Mobile Convergence (FMC).

GGSN - The GGSN is the node which carries out the role in GPRS equivalent to the Home Agent in Mobile IP. It is a router which detunnels user data from GPRS Tunneling Protocol and sends out normal user data IP packets.

GPRS - General Packet Radio Service (GPRS) is a mobile data service available to users of GSM mobile phones. It is often referred to as "2.5G", that is, a technology between the second (2G) and third (3G) generations of mobile telephony. It provides moderate-speed data transfer by using unused TDMA channels in the GSM network. Originally there was some thought to extend GPRS to cover other standards, but instead those networks are being converted to use the GSM standard, which is the only kind of network where GPRS is in use.

GTP - GPRS Tunneling Protocol (or GTP) is an IP based protocol used within GSM and UMTS networks. The GTP protocol is layered on top of UDP. There are in fact three separate protocols, GTP-C, GTP-U and GTP'. GTP-C is used within the GPRS core network for signaling between GPRS Support Nodes (GGSNs and SGSNs). This allows the SGSN to activate a session on the users behalf (PDP context activation), to deactivate the same session, to adjust quality of service parameters or to update a session for a subscriber who has just arrived from another SGSN.

IPTV - Internet Protocol Television describes a system where a digital television service is delivered to subscribing consumers using the Internet Protocol over a broadband connection. This service is often provided in conjunction with Video on Demand and may also include Internet services such as Web access and VOIP where it may be called Triple Play, and is typically supplied by a broadband operator using the same infrastructure.

J2ME - Java Platform, Micro Edition or Java ME (formerly referred to as Java 2 Platform, Micro Edition or J2ME), is a collection of Java APIs for the development of software for resource-constrained devices such as PDAs, cell phones and other consumer appliances. Java ME is formally a specification, although the term is frequently used to also refer to the runtime implementations of the specification. Java ME was developed under the Java Community Process as JSR 68. The evolution of the platform has abandoned the umbrella Java Specification Request in favor of separate JSRs for the different flavors of Java ME.

MMS - Multimedia Messaging Service (MMS) is a technology for transmitting not only text messages, but also various kinds of multimedia content (e.g. images, audio, and/or video clips) over wireless telecommunications networks using the Wireless Application Protocol (WAP). It is standardized by 3GPP and 3GPP2.

Pre-IMS - The IP Multimedia Subsystem (Pre-IMS) is a standardized Next Generation Networking (NGN) architecture for telecom operators that want to provide mobile and fixed multimedia services. It uses a Voice-over-IP (VoIP) implementation based on a 3GPP standardized implementation of SIP, and runs over the standard Internet Protocol (IP). Existing phone systems (both packet-switched and circuit-switched) are supported. The aim of Pre-IMS is not only to provide new services but all the services, current and future, that the Internet provides. In addition, users want to be able to execute all their services when roaming as well as from their home networks. To achieve these goals, Pre-IMS uses open standard IP protocols, defined by the Internet Engineering Task Force (IETF). A multimedia session between two Pre-IMS users, between an Pre-IMS user and a user on the Internet, and between two users on the Internet is all established using exactly the same protocol. Moreover, the interfaces for service developers are also based on IP protocols.

SIP - Session Initiation Protocol (SIP) is a protocol developed by the IETF MMUSIC Working Group and is the proposed standard for initiating, modifying, and terminating an interactive user session that involves multimedia elements such as video, voice, instant messaging, online games, and virtual reality. In November 2000, SIP was accepted as a 3GPP signaling protocol and permanent element of the IMS architecture. Along with H.323, it is one of the leading signaling protocols for Voice over IP.

SIS – Is the filename extension for installation package files for the Symbian OS operating system.

SMS - Short Message Service (SMS) is a service available on most digital mobile phones that permits the sending of short messages (also known as text messages, or more colloquially SMSes, texts or even txts) between mobile phones, other handheld devices and even landline telephones. Other uses of text messaging can be for ordering ringtones, wallpapers and entering competitions.

SSGN - The SGSN is the node which in some sense carries out the same function as the Foreign Agent in Mobile IP. However, an SGSN is actually considerably more complex since it also does the full set of interworking with the connected radio network. This means that the functions carried out by the SGSN vary quite considerably between GSM and UMTS.

Symbian OS - Designed for mobile devices, Symbian OS is an operating system with associated libraries, user interface frameworks and reference implementations of common tools, produced by Symbian Ltd.. It is a descendant of Psion's EPOC. Symbian is currently owned by Ericsson, Panasonic, Siemens AG, Nokia, and Sony Ericsson.

UDP - The User Datagram Protocol (UDP) is one of the core protocols of the Internet protocol suite. Using UDP, programs on networked computers can send short messages known as datagrams to one another. UDP does not provide the reliability and ordering guarantees that TCP does; datagrams may arrive out of order or go missing without notice. However, UDP is faster and more efficient for many lightweight or time-sensitive purposes. Also its stateless nature is useful for servers that answer small queries from huge numbers of clients. Common network applications that use UDP include the Domain Name System (DNS), streaming media applications, Voice over IP, Trivial File Transfer Protocol (TFTP), and online games.

VoIP - Voice over Internet Protocol (also called VoIP, IP Telephony, Internet telephony, and Broadband Phone) is the routing of voice conversations over the Internet or any other IP-based network. The voice data flows over a general-purpose packet-switched network, instead of on traditional, dedicated, circuit-switched telephony transmission lines. Protocols used to carry voice signals over the IP network are commonly referred to as Voice over IP or VoIP protocols. They may be viewed as commercial realizations of the experimental Network Voice Protocol (1973) invented for the ARPANET. Voice over IP traffic can be deployed on any IP network, including ones lacking a connection to the rest of the Internet, for instance on a private building-wide LAN.

WAP - Wireless Application Protocol is an open international standard for applications that use wireless communication (for example, Internet access from a mobile phone). WAP was designed to provide services equivalent to a web browser with some mobile-specific additions, being specifically designed to address the limitations of very small portable devices. It is now the protocol used for the majority of the world's mobile Internet sites, otherwise known as WAP-sites.

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated multi-threat security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, Web content filtering, VPN, spyware prevention and antispam--providing customers a way to protect multiple threats as well as blended threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified eight times over by the ICSA (firewall, antivirus, IPsec, SSL, IDS, client antivirus detection, cleaning and antispymware). Fortinet is privately held and based in Sunnyvale, California.

FORTINET
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1-408-235-7700 Fax +1-408-235-7737
www.fortinet.com

©2006 Fortinet, Inc. All rights reserved. Fortinet, FortiGate, FortiOS, FortiAnalyzer, FortiASIC, FortiLog, FortiCare, FortiManager, FortiWiFi, FortiGuard, FortiClient, and FortiReporter are registered trademarks of the Fortinet Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners. Licensed under U.S. Patent No. 5,623,600

WPR124-0606-R1