HEAVY READING

White Paper

The New Frontier in LTE Security: Now for the Application Layer

Prepared by

Patrick Donegan
Senior Analyst, *Heavy Reading*
www.heavyreading.com

on behalf of

CLOUDMARK®

www.cloudmark.com

November 2013

Basic LTE Security Considerations

As LTE networks are rolled out around the world, and as subscribers begin buying and using LTE-enabled devices, it's becoming increasingly clear that 3G is just a warm-up, a practice run, for the mobile network as it undergoes the transition from delivering a mobile telephone service with some added data services to becoming a full-fledged Internet service provider (ISP) with added mobility.

The flat LTE network architecture with a single packet core for voice and data applications resembles an ISP architecture more than it does a traditional hierarchical mobile network architecture. LTE users consume two to three times as much data as their 3G counterparts, and that is increasing. And for the first time, operators are discovering that LTE is a technology that can legitimately be positioned as fixed broadband displacement technology, that will drive adoption by PC and laptop users, and that will be in semi-permanent use, driving high volumes of traffic for hours on end.

In terms of how the operator goes about protecting its network assets – as well as its customers' experience – against theft of private information, fraud and network disruption arising from cyber-attacks, many of the 3GPP's strong security mechanisms developed for 3G are carried over into LTE, together with some important enhancements. For device authentication, for example, LTE uses the same mechanism as 3G, albeit with an extended algorithm and key hierarchy. And just as in 3G, traffic is encrypted from the handset over the air to the eNodeB, albeit encryption of traffic from the eNodeB across the backhaul to the core is rendered optional for the first time using IPsec.

At the same time, the rollout of LTE also represents a fresh opportunity for mobile operators to update to best current practices in network security, since many have neglected to do so during the 3G era. A couple of simple examples are the use of Infrastructure Access Control Lists (IACLs) throughout their routing infrastructure to prevent packets from being sent directly to network infrastructure elements. Another is the compartmentalization of Authoritative DNS servers and Recursive DNS servers within the infrastructure. Separating out that part of the DNS which provides the IP address for a given URL, and that which locally caches the IP addresses of common URL requests, helps minimize the risk that an outage in one will impact the other. This is basic security practice 101 in network security circles, but many mobile operators have yet to do this.

An Increased Risk of IP Address Blacklisting

The rollout of LTE also exposes the mobile operator to a greater risk of IP address blacklisting, which often arises as a result of IP endpoints being identified as forming part of a botnet. This is already a well-established problem for ISPs, as well as an emerging problem for 3G operators. The problem manifests itself in different ways, but the rollout of LTE risks making the problem worse in the mobile network.

In a wireline ISP environment, blacklisting associates a rogue IP address with one physical connection at one physical location (such as a house) and blocks Internet access accordingly. It's different in a mobile environment. Since they were late to the IP networking game, most mobile operators only have a small pool of public IP addresses, but they typically have a great many more customers than most wireline ISPs in their market.

Because of the way Internet access is used in the mobile network environment – i.e., connections are torn up and down sporadically – mobile operators share this small pool of public IPv4 addresses across their subscribers. These are then converted into public Internet addresses via Network Address Translation (NAT) gateways, supporting multiple subscriber sessions at the same time.

In today's environment this means that if one of a mobile operator's private IP addresses is blacklisted for rogue behavior, it isn't the Internet access of just one mobile subscriber that is suspended, but that of many users – since, at any given time, that IP address is likely being shared by multiple subscribers.

But while mobile operators do have experience dealing with IP address blacklisting and the impact on their customers in the 2G and 3G eras, the problem risks being exacerbated with the rollout of LTE, for two main reasons:

- As has been well documented, LTE customers use their devices more than their 3G counterparts, which means more and longer connections to the Internet from the mobile network. This increases the "competition" between subscribers for IP address space for Internet access via their mobile operator. It therefore increases the numbers of subscribers that are impacted by the blacklisting of any one of the operator's IP addresses.
- As previously noted, the markedly superior performance of LTE compared with 3G renders it likely that rollout will drive greater adoption of LTE-connected laptops. In addition to driving more and longer Internet connections, consistent with the previous point, more LTE-connected laptops running on Microsoft Windows will also increase the risk of the end-user devices in the mobile network becoming infected by malware and becoming part of a botnet, since Windows is still the most common attack platform for the cybercriminals that operate botnets. And greater vulnerability to botnets means an increased risk of the operator's IP addresses being blacklisted. The fact that LTE leverages IPv6 doesn't solve the bottleneck, which remains in the NAT gateway, because most email (and hence spam) is sent over IPv4 and thus still pollutes the publicly visible pool of IP addresses. Hence, this means that LTE will also drive an increased risk of a ratcheting up in the numbers of mobile subscribers that are affected by IP blacklisting unless steps are taken to mitigate the problem.

LTE & IMS: Lower Costs & Higher Revenues

It's been around 10 years since the hype around IP Multimedia Subsystem (IMS) started gathering momentum. That lasted a year or two before the so-called "peak of inflated expectations" gave way to the slide down the so-called "trough of disillusionment." In more recent years, wireline operators have begun rolling out IMS, and now substantial rollouts are underway in the mobile network. And, of course, one of the major drivers of IMS adoption in mobile networks now is the evolution from 3G to LTE with the step-change in mobile network performance that it provides in terms of bandwidth, bandwidth efficiency and latency.

Until now, in the pre-IMS era, the critical benefit that operators have derived from LTE has been greater network efficiency, as well as the step change in the user's experience of data services and applications that it has enabled. Cost reduction targets also form part of the value proposition of IMS in the sense that the voice over LTE (VoLTE) standard is dependent on an IMS core and is now the driver of IMS for many operators.

VoLTE provides important cost reduction opportunities for the operator. These are derived from two main sources. To begin with LTE is more spectrally efficient than 3G so that rolling out VoLTE can enable operators to re-farm valuable spectrum, especially in the premium sub-1GHz spectrum bands. Migrating voice traffic from 2G and 3G to VoLTE also enables the operator to reduce its investments in its costly SS7 signaling infrastructure.

What was once the primary promise of IMS, and continues to be an important part of the value proposition, is that the introduction of the call control function enables a step change in the quality of applications that operators can offer. These include carrier-grade VoIP via VoLTE – leveraging conventional dial tone, quality of service (QoS) and billing data – as well as blended voice, data and video services and applications via the Rich Communications Suite (RCS) developed by the GSM Association.

VoLTE and RCS provide the mobile operator with a set of tools that they can leverage to build out superior multimedia services and applications with which to finally compete with the over-the-top (OTT) voice and messaging services offered by the likes of Skype, Google, Facebook and Whatsapp. While operators tend to recognize OTT players as adding value to their customers' experience, they also object to them taking up capacity in the mobile network and charging customers, typically without much, if any, revenue share for the operator.

Mobile operators once thought of VoLTE and RCS as key elements in their "fight back" against the OTT players, as part of their strategy for reversing often flat or declining revenues. Leading operators now acknowledge that they need to pivot their business models toward a focus on data, while also maintaining relevance in communications services. Most remain clear that competitive next-generation rich messaging services must be a core part of their product and service portfolio in order to achieve that – even though it's unclear whether or not these services will make a direct contribution to shoring up their revenues.

As shown in **Figure 1**, more than 10 years after the hype around IMS first started, the last 12 months have finally – at long last – seen the first initial deployments of both VoLTE and RCS services. Certainly not all of these have been an instant success. For instance, operators have yet to emphatically promote the "Joyn" branded RCS services launched in Europe. This is in part because these services have launched using the RCSe specification designed for use over 3G, rather than the more advanced RCS5 version that North American and other operators are using as they roll out in earnest in 2014.

Figure 1: VoLTE & RCS Launches

SERVICE	DATE	COUNTRY	OPERATOR	COMMERCIAL LAUNCH
VoLTE	End 2012	South Korea	SK Telecom	More than 5 million subscribers using VoLTE
VoLTE	2012	U.S.	Metro PCS	Initial launch of commercial service
VoLTE	2014	U.S.	AT&T	Commercial launched planned 2014
VoLTE	2014	U.S.	Verizon Wireless	Commercial launched planned 2014
VoLTE	2014	China	China Mobile	Commercial launched planned 2014
RCS	End 2012	Spain	Vodafone	Initial pre-commercial launch of "Joyn" over 3G
RCS	End 2012	Spain	Telefónica	Initial pre-commercial launch of "Joyn" over 3G
RCS	End 2012	Spain	Orange	Initial pre-commercial launch of "Joyn" over 3G
RCS	March 2013	Germany	T-Mobile	Initial pre-commercial launch of "Joyn" over 3G
RCS	March 2013	Germany	Vodafone	Initial pre-commercial launch of "Joyn" over 3G
RCS	June 2013	France	Orange	Initial pre-commercial launch of "Joyn" over 3G
RCS	October 2013	U.S.	Sprint Nextel	Commitment to white-label RCS apps with Jibe Mobile

Source: Heavy Reading

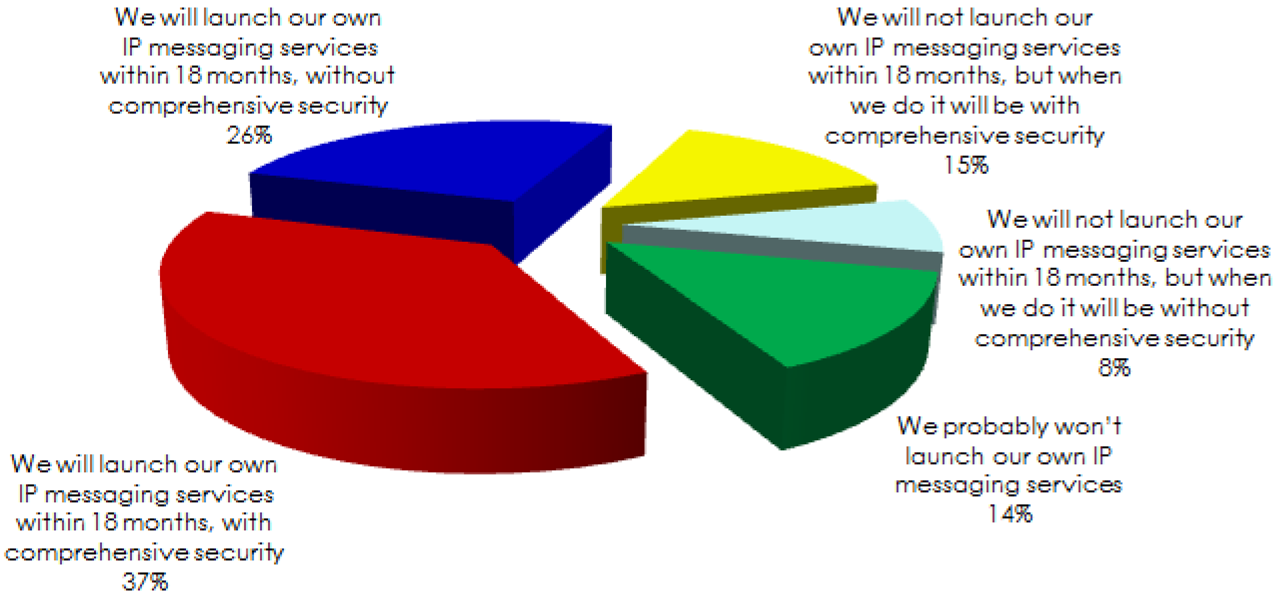
Interoperability of high-quality, secure, real-time, multimedia services over high speed wireless networks onto mobile devices was never going to be easy. And importantly the lack of initial momentum behind the early European launches of RCSe does not appear to be dampening commitment on the part of mobile operators. As shown in **Figure 2**, which is taken from a *Heavy Reading* survey of 66 mobile operators in the third quarter of 2013, 84 percent of mobile operator respondents expect their company to launch their own IP messaging service. Moreover, 63 percent of respondents expect that their companies will do that within the next 18 months.

Other than building and launching their own proprietary IP messaging solutions from scratch or arriving at a satisfactory revenue-sharing model with OTT players (something that continues to prove elusive after many years of trying), RCS continues to be the most viable option for most mobile operators to fulfill their goals in the next-generation rich messaging market.

Direct Security Risks With IMS Applications

Irrespective of exactly when they expect their companies to launch their own IP messaging services, a narrow majority of mobile operator respondents expect that these services will be launched with comprehensive security. As shown in **Figure 2**, 14 percent of mobile operator respondents stated that they did not expect their company to launch its own IP messaging service; 34 percent expect a service to be launched, but *without* comprehensive security; and 52 percent believe a service will be launched *with* comprehensive security.

Figure 2: The IP Messaging Launch Plans of Mobile Operators



Source: Heavy Reading's 2013 Mobile Network Security Survey, October 2013

This raises the question, "What is meant by comprehensive security?" in the case of next-generation IP messaging, particularly the VoLTE and RCS5 applications over LTE that the likes of AT&T and Verizon Wireless are now working toward.

VoLTE and RCS introduce several new security risks into the LTE network. In this section we address what we define as "direct risks"; in the subsequent section, we address what we define as "indirect risks." This classification is not intended to imply a greater or lesser scale of risk posed to the operator or its customers by the threat type. Rather the intent is to distinguish new threats that relate to the introduction of the new IMS application suite from new threats that may arise as a consequence or knock-on effect of introducing this new suite.

3GPP Provides Some IMS Security – But It's Not Enough

Consistent with its focus over the years, the 3GPP provides excellent security for the new IMS core at the network and transport layers. It does this for the IMS core – e.g., on the interfaces that are exposed between operators and around IP addressing – much as it does for the 3G and LTE network architectures. But this still leaves the IMS network and users of IMS applications potentially vulnerable, particularly to malware and a variety of attacks at the application layer.

IMS applications will drive a lot of new Diameter and Session Initiation Protocol (SIP) traffic, which should cause an element of apprehension. After all, going back two or three years, the subpar performance of these two protocols in heavy-loading scenarios was the cause of some high-profile outages among the first commercial LTE launches in North America and Europe. That said, a lot of standards work is being put in place to enhance these protocols to deal with such overload scenarios without compromising the user experience, so tools are coming onto the market now to help address this vulnerability – provided that operators are willing and able to take advantage of them.

Of course, from a certain standpoint, one of the primary value propositions of RCS actually puts the mobile operator at a competitive disadvantage in terms of security compared with OTT players: The OTT messaging apps are nearly all walled-garden models. A Whatsapp user can only exchange messages with other Whatsapp users. Each user's interface to the app is controlled exclusively via Whatsapp. These OTT companies typically have their own dedicated security teams policing the walled garden against security breaches – actively seeking out ways to prevent people from gaming the system by registering thousands of fake accounts and the like, in order to protect their customers' messaging experience.

A core value proposition of the GSMA's approach through RCS is that interoperability is opened up to the mobile customer bases of dozens, ultimately hundreds, of mobile operators all over the world. But in setting out to enable interoperability with dozens or hundreds of different mobile operators, RCS exposes any one mobile operator to traffic from those dozens or hundreds of partner operators. And since any one mobile operator can only police its own RCS environment, it leaves itself exposed to incoming malicious traffic from those among its partners who have poor security practices. From a security standpoint, this is a vulnerability that the mobile operator needs to close off just in order to get onto a level playing field with the OTT providers. This potential vulnerability extends to all protocols being used to interoperate, not just RCS, and creates a case for operators to consider SIP firewalls at the edge of their network to protect their valuable signaling network from being attacked.

From the Security Offered by the SIM to the Wilds of the Internet

In terms of direct security risks posed by the introduction of IMS applications like RCS and VoLTE, the fundamental issue is that the mobile operator no longer restricts itself to opening its application programming interface (API) to its customers' highly-secure SIM cards, which has been the mobile operator's modus operandi until now. Rather, because VoLTE and RCS are IP applications, the operator has to open its API to the wilds of the Internet. And while that promises all manner of potentially exciting innovation from application developers, the act of exposing the network and the end user to the Internet in this way renders the operator and its customers vulnerable to the full gamut of Internet attackers.

The operator may develop its own API, use the Web Real Time Communication (WebRTC) – the API being developed by the World Wide Web Consortium for multimedia IP browser-to-browser applications – use the GSM Association's One API or choose another option. And care should be taken to ensure that the API is securely coded in terms of how credentials, password management and the like are handled. But even secure coding can't be so complex as to inhibit the API from being used to maximum commercial effect, so some form of compromise between security and ease of use has to be made in the coding process. This ensures that no matter the API, the exposure to the Internet that comes with both VoLTE and RCS creates a vulnerability that must be protected against.

In the case of both application developers or partners in the service delivery ecosystem – be they other operators seeking inter-operability or third-party hosting partners – operators need to have the right level of service-level agreement (SLA) with these partners to ensure that the right incentives and disincentives are in place to ensure a high level of security in the way that they do business.

Direct Security Risks That Are Specific to VoLTE

VoLTE is only the latest in a very long line of voice communications services to be delivered by service providers, from Alexander Graham Bell's original invention to switched analog telephony, the digitalization of the PSTN, analog cellular, digital cellular, fixed-line VoIP and now OTT VoIP delivered over the mobile network. And while nearly all the focus around mobile network security today is on attacks that are delivered to data-oriented devices using data applications and protocols, it's worth considering that pretty much every voice service has been subject to some kind of security attacks, going back more than two decades, as shown in **Figure 3**.

Figure 3: Voice Telephony Attacks Over the Last 20 Years

DATE	VULNERABILITY	RISK TO VOICE SERVICE USERS
Late 80s, early 90s	Cell phone scanning	1G analog cell phone calls (e.g., TACS) listened in to by third parties using a low-cost scanner.
Early 1990s	Network switch vulnerability	Kevin Poulsen hijacked a phone company switch in LA, blocking all contestants to a radio station completion to win a car (except calls from his friends).
1990s	GSM mobile voicemail PINs	U.K. tabloid journalists exploited the failure of high-profile individuals to change the default voicemail PIN setting to remotely retrieve personal messages.
2011	Malicious robocalls	Robocalls placed to Canadian voters, misleading them to believe their polling station had changed.
Dec. 2012	Cisco VoIP phones	Cisco VoIP phone vulnerability shown whereby patching with malicious code turned it into a listening device. The phone then recorded words spoken close by and allowed recordings to be retrieved.
March 2013	Enterprise VoIP networks	Department of Homeland Security warning to U.S. operators of flooding attacks on fixed telephony services of government departments, aiming to extort cash payments as the price of ceasing attacks.
June 2013	Skype for Android app	The XDA-Developers Forum warned of a bug in the Skype for Android app. An attacker's Skype voice allowed the Android inbuilt lock screen to be bypassed, thereby giving the attacker access to the smartphone. The vulnerability was proven on Huawei Premia, Samsung Galaxy and Sony Xperia devices.
Sept. 2013	Robocalls to cell phones	Bank of America settled $32 million customer lawsuit for debt collection robocalls to customers' cell phones.

Source: Heavy Reading

What is most instructive from **Figure 3** is the trend toward attacks on VoIP networks and applications, of which VoLTE is only the latest in a long line. One example is the June 2013 vulnerability in the Skype for Android App. This is triggered by an initial Skype VoIP call over the 3G or LTE network. Another is Bank of America's decision in September 2013 to settle for paying $32 million in compensation for running an aggressive program of harassment robocalls that explicitly targeted its customers' mobile phone numbers to demand debt repayments.

As voice communications start to become transmitted as VoIP packets with VoLTE, and as mobile operators open up their APIs to third-party application developers, VoLTE users will become exposed to many of the same types of recent attacks on VoIP services that are itemized in **Figure 3**, as well as the new ones that attackers currently have in the works but have yet to launch.

Certainly there should be no concerns regarding the authentication of conventional end-user devices, such as smartphones. The type of spoofing of VoIP endpoints that can be done in the public Internet environment, and that can serve as a platform for attacks on voice services, is protected against by the strong authentication that the 3GPP provides.

Direct Security Risks That Are Specific to RCS

Besides the new security issues that are generic to all new IP services delivered over IMS, there are some that are specific to RCS. For example, RCS creates a new bearer upon which file transfer protocols can be delivered onto mobile devices. Until now, file transfer has only been possible on a mobile phone via email or Web browsing. But now RCS will also support file transfer, creating a new vector for pushing malware onto mobile devices.

Another risk is that of social engineering, leveraging chat sessions. This has been seen on many social networks and IM networks such as Yahoo Messenger, where a chat-robot starts a conversation with someone, often impersonating a female, and attempts to entice the recipient into clicking on a link. The link may be to a spam site, fraud or phishing, or even a link to malware download. The unique dynamics of a chat session (start with "Hi, how are you?" and build on that) make this approach a likely vector for spear phishing and malware infection particularly.

Indirect Security Risks of Combining IMS & LTE

As previously noted, in addition to the new security risks that are native to the new multimedia applications that IMS supports, there are a number of indirect or secondary security impacts that the operator must also protect against.

The first is that rich messaging will be a much more attractive platform for generating SMS spam than the original 2G and 3G SMS technology and architecture. Because SMS is based on circuit-switched technology, there is a physical limitation of around one per second on the number of SMS messages that any one SIM card can send out. Clearly, that is more than enough for any one subscriber. And as has become clear in recent years this has also proven to be plenty of capacity for SMS spammers who are able to leverage so-called SIM boxes or racks of SIM cards to achieve rates of SMS spamming in the several hundreds or even thousands per minute, albeit still within the physical limitation of one per second per SIM card.

As rich messaging is rolled out with LTE, this shifts the goalposts decisively in favor of the spammer, because it is now possible to send text messages via the IMS network rather than the legacy bespoke SMS infrastructure. This will inevitably lift the one message per second constraint on the volume of text messages that can be sent per SIM card. Exactly how high the new bar will be remains to be seen, but with the right level of commitment, in theory, it will be possible to configure an approach that allows dozen, hundreds or even thousands of spam messages per second to be dispatched.

Again, this breakthrough in technological performance shouldn't be considered in isolation. It would certainly be powerful in its own right, but, to make matters worse, it will also hit the market at a time when demand for plain old text messaging will have peaked or will be peaking, hence, at a time when operators will be bundling more and more text messages into subscription fees either for a lower rate – or indeed, entirely for free.

Hence, the launch of rich messaging with LTE creates greater SMS spam challenges for the operator, driven by a perfect storm of higher capacity and lower costs. The very arguments promoted by the carriers as the reasons why RCS will be successful – i.e., ubiquitous communication between any two phones, regardless of operator, contrasting with the walled-garden approach of the OTT vendors – are also extremely attractive to spammers, who will see the prospect of cheap, fast sending of spam to any phone, regardless of operator, as very attractive.

Video Messaging: A Tool for DoS Attacks

Consider also the impact of video messaging. The impact of millions of spam text messages, weighing in at one or two hundred bytes per message is relatively benign in terms of network capacity, although many an SMSC (especially an unprotected one) has been known to fall over at times of peak usage.

Now consider the impact of a spammer who can leverage LTE and RCS to generate huge volumes of video messaging spam, each one weighing in at a minimum of a few megabytes each, depending on the maximum data volume prescribed by the operator. In the hands of a spammer, video messaging becomes a medium worth exploring not just for embedded malware to trigger theft of personal information and financial fraud, but potentially as a tool to execute denial of service (DoS) attacks as well. There is also the additional risk that since much higher spam volumes can be dumped onto the LTE network so much faster, the bar will also be raised for law enforcement agencies when it comes to trying to apprehend spammers and catch them in the act.

Rich media applications don't just generate security issues that are confined to the IMS domain. So in addition to ensuring that VoLTE and rich media services are secure within their own environments, security strategy must protect the network and subscribers against the risks arising from the new IMS platform also being interconnected to legacy networks and services such as SMS and circuit-switched fall back (CSFB). So not only can legacy SMS services be delivered over the newer IMS infrastructure to reduce costs, but text messages composed by a user using a rich media service can also be delivered over the legacy SMS network infrastructure to another user with only a 2G or 3G handset. And inevitably where new and legacy networks and services are interconnected in this way there is an exposure to malware spreading from one into the other, or for malicious actors to discover ways to spoof, fake or otherwise circumvent security restrictions.

Virtualization & Security in the LTE Network

The rollout of LTE and now IMS in the mobile network is occurring at a time when software-defined networking (SDN) and virtualization are dominating the forward-looking network evolution deliberations of telecom operators. Many are already quite advanced, as are other large enterprises, when it comes to virtualizing the IT side of the house, but increasingly they are also looking to these same principles as they strive for roadmaps for their own telecom network infrastructure that will support a quantum leap in capacity, performance and flexibility without an associated quantum leap in costs.

This means that, at some point in the roadmaps of most mobile networks, some aspects of these networking principles will inevitably start to be introduced. Once they are represented in software as virtual network functions, different functionality in the mobile network can be managed automatically and remotely at substantially lower cost.

Security considerations are fast coming to the fore as operators contemplate the implications of multi-tenancy or mixing multiple different applications on the same server. As virtualization begins to take shape in the mobile network, the operators will need to evolve fundamentally different security models to support that transformation. This may be five to 10 years away for some operators, but it is happening more rapidly for the world's leaders. Indeed, a case could quite easily be made that a type of virtualization of the mobile packet core is already underway in the case of some operators.

Security is often pointed to as an outstanding early candidate for virtualization. The value proposition is clear enough: Security can be enhanced if threat detection capability is pushed out from the center toward the edge of the network, to better protect the core. And by virtualizing those security instances in software, that objective can be achieved at low cost.

On the other hand, of course, distributing security policy so that it is no longer confined to one central physical location and one single domain carries with it its own security risk because the security is then distributed across more physical locations and execution on the security strategy – for example, with respect to managing software patches, security configuration standards – is liable to be devolved outward from a small core of security-savvy personnel to several other people who are unlikely to be as well trained in security.

With virtualization increasingly figuring in network evolution planning scenarios, security solutions will increasingly need to be virtualize-able in software to give operators the greatest possible flexibility as they evolve their network and network security architectures.

A Holistic Application Security Framework

Each mobile network is different in regards to the security architecture that is in place for security at the application layer, as well as the technology platforms that support it. As the network evolves from 3G to LTE, and as rich messaging and VoLTE applications are rolled out over IMS, these security architectures and technology platforms also need to evolve.

Within the mobile network environment the messaging security architecture should be optimized to protect against both email and SMS spam. And as LTE is rolled out, operators must protect against the risks introduced by IMS at the application layer by means of what is sometimes referred to as application firewalling. This needs to protect the direct security vulnerabilities introduced by IMS, such as the mold-breaking exposure of the operator's API to the Internet. It also needs to protect against the indirect consequences, including: the enhanced capability that the LTE network gives the spammer to generate higher volumes of spam and at lower cost compared with 3G; the unique negative impact on the network of video messaging spam; and the heightened vulnerability of the operator's customers to being cut off from service as a result of blacklisting activity out in the Internet.

Mobile messaging security that was originally designed for 2G and 3G services should have a clear roadmap enabling the latest rich messaging services and legacy SMS to be protected by the same solution. And as LTE is progressively scaled up, giving the operator the look and feel of a full-fledged ISP, operators that offer both fixed and mobile services should also consider extending a common security framework across their fixed and mobile networks. Investing in different blacklists and other filters for each fixed and mobile network domain makes less and less sense in the case of email and rich messaging. The same case can be made where the operator rolls out its own social networking applications.

And lastly, the security architecture must be virtualizable. As the operator evolves the network to be increasingly software-defined, control and bearer planes needs to be separable and capable of being distributed across platforms other than the vendor's own.

Background to This Paper

About Cloudmark

Cloudmark (www.cloudmark.com) builds messaging security software that protects communications service provider networks and their subscribers against the widest range of messaging threats. Only Cloudmark Security Platform delivers instant security and control across diverse messaging environments, enabling communications service providers to create a safe user experience, protect revenue and safeguard their brand, while streamlining infrastructure and reducing operational costs. Cloudmark's patented solutions protect more than 120 Tier 1 customers worldwide, including AT&T, Verizon, Swisscom, Comcast, Cox and NTT.