White Paper

The 7 Deadly Threats to 4G

4G LTE Security Roadmap and Reference Design

By Tyson Macaulay
VP Global Telco Strategy, McAfee

Table of Contents

Executive Summary

The transition to a broadband wireless service portfolio ushers in new vulnerabilities and threats to telecommunications and service provider organizations. As carriers deploy wireless Internet technologies to enable long term evolution (LTE) networks, attackers can use old Internet techniques to new effect through these broadband data services, targeting mobile devices and infrastructure.

Most carriers and service providers are fully occupied with the task of switching from circuit-switch, third-generation wireless (3G) technologies to fully Internet Protocol (IP)-enabled, fourth generation (4G), end-to-end technologies. They aren't fully aware of or focused on malicious actors. Why should they be? Mobile threats to date have largely been reported in relation to "smart" devices and user data, not operator infrastructure. Additionally, many service providers are still planning 4G or are in the deployment stage with limited 4G operational experience.

Devices are simply the most obviously vulnerable aspect of the 4G network—the weakest link. LTE introduces new "weak links" throughout carrier infrastructure, as well as greater bandwidth and newly connected devices to exploit. Operators must take steps now to harden their nascent LTE infrastructure, to mitigate risk, gain operational efficiencies, and maximize potential revenue:

- Early action—designing security into the LTE deployment—will help preserve 4G bandwidth for legitimate uses, including the reliable service required for Voice over IP on LTE (VOLTE).
- Proactive security costs less to deploy and manage than post-rollout bolt-ons.
- Early, planned actions will alleviate service disruptions, whether caused directly by a security attack or indirectly by the need to take infrastructure offline for a security workaround.
- The security capabilities built into LTE can also enable operating savings, which can offset deployment costs.
- Security systems function as dual-purpose, value-added service offerings, whose revenue can add to the bottom line and increase subscriber stickiness.

This paper provides a detailed review of seven threats that take on unique profiles within 4G networks. It also offers a security reference architecture to efficiently counter these threats with minimal cost or service disruption.

A True and Cautionary Tale

One day, an operator activated a new mobile broadband network across a large geography. Over the next few months, traffic more than tripled. Cybercriminals were consuming the spectrum in both directions as they scanned and attacked devices. Angry users and skeptical regulators complained that the much-vaunted, new spectrum wasn't delivering the expected performance. The carrier faced a series of serious risks: penalties and fines for false advertising, subscriber dissatisfaction and resulting "churn," operational costs way outside plans and projections, and an opportunity for rival wireless services.

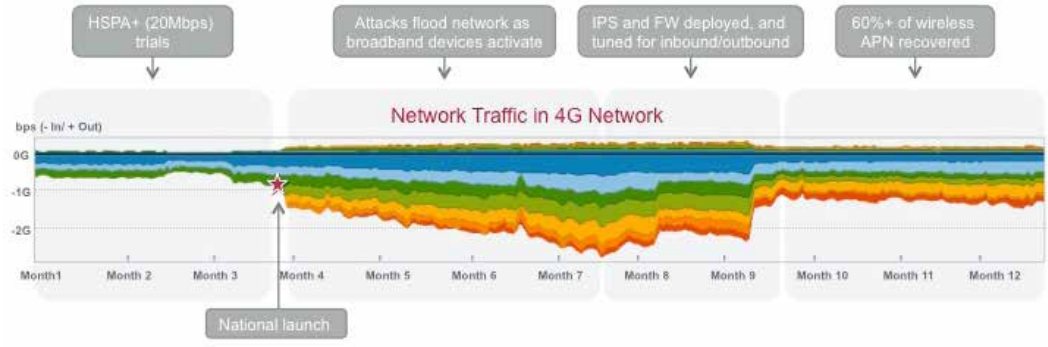

Figure 1. Attack traffic flooded the operator's new wireless broadband network.

A safe outcome

Through traffic and log inspection, the carrier discovered that more than half of the new traffic was coming from attacks. The remedy was an immediate deployment of network security gateways (firewall and intrusion prevention systems) that could monitor for and drop this traffic.

Any emergency rollout of equipment into an active network is a perilous and unusual move for any service provider. However, in this case, the aggregated business risks outweighed the risk of service disruption caused by an emergency deployment of security equipment into the network. The carrier's swift action allowed it to recover 60 percent of its 4G spectrum and backhaul network, reduce capital and operating expenses by an estimated 20 percent to 40 percent, and delay network and equipment purchases that required large un-forecast expenses.

Multiple Market Forces

The preceding example showcases the danger of 4G service activation without an adequate 4G security architecture. It happened because, like other operators, the carrier thought about 4G in terms of legitimate subscriber traffic and its impact on the equipment and processes in the wireless, backhaul, and core network.

However, the voyage to 4G will be buffeted by many other external forces. In addition to a litany of new devices and services that go beyond traditional handsets, criminals will capitalize on the large, new attack surface presented by wireless broadband (compared to 3G data services). Their efforts will be enabled by the vulnerabilities and lack of maturity that come with new and disruptive technologies like 4G.

Increasing malware

Data-capable smartphones and tablets paired with large, wireless data pipes now attract significant attention from cybercriminal networks, today's "organized crime." From a negligible baseline, malware-based threats to mobile devices were up 4,000 percent in 2012 and expanded a further 30 percent in the first three months of 2013, according to McAfee® Labs™.[1]

Malicious software developers now readily take techniques developed for personal computers and adapt them to the limited footprint and technologies of mobile devices. For example, ZITMO stands for "Zeus in the Mobile," a reuse of the widely adopted Zeus toolkit that makes malware programming easy for non-technical criminals. ZITMO perpetrates financial fraud by hijacking browsers and SMS authentication techniques.

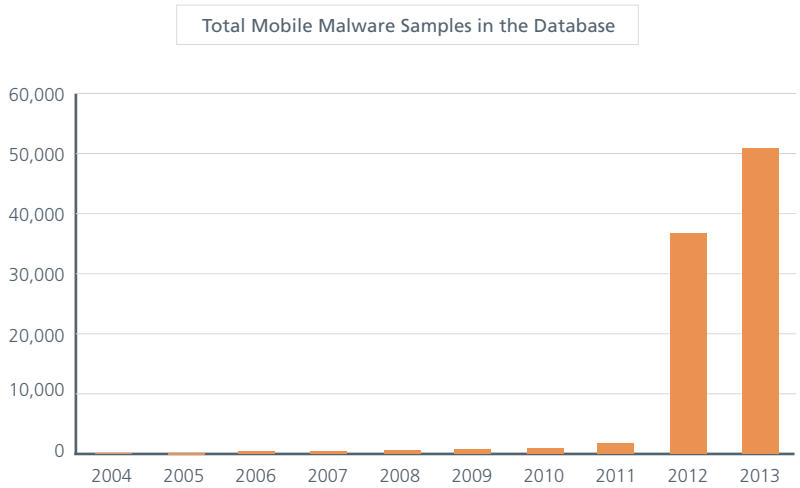

Figure 2. The explosion of Android devices has enabled an explosion in mobile malware.

Beyond mobile malware, "old-fashioned" attacks on more conventional operating systems remain very effective, because many such devices (desktop, laptops) are connecting through wireless broadband through a process of "tethering." Tethering through USB 4G "sticks," or even through phones, places these more conventional (and sometimes not really mobile) devices in the broadband Internet. In places where fixed line broadband is not available, wireless broadband will fill that market gap and introduce this attack opportunity.

Social engineering

Possibly more dangerous even than the spike in mobile malware is the spike in "SMiShing" and "phishing" attacks targeting the social relationships and curiosity of mobile users. These attacks involve malicious messages sent as emails or text messages to be consumed on the small screens and limited viewing areas of many mobile, smart devices. The message dupes a user into clicking a link, installing an app, or going to a website. The result is frequently that identity and credentials are handed over by the user to the attackers willingly but unknowingly; and serious fraud is the outcome.

Unprotected devices

Today, less than 5 percent of "smart," mobile devices run security software, and smart devices represent only a small fraction of mobile devices as a whole. This is in part because basic handsets (or "feature phones") with limited capabilities still make up 82 percent of handsets on mobile networks worldwide.[2] However, this profile is changing fast as smartphone prices drop rapidly. Some places in Asia are transitioning from feature phones to smartphones at rates approaching 25 percent per year[3]—meaning smart devices will be the only type of mobile devices within 4 years.

Another reason for the lack of adoption of security software is user cost sensitivity. Prepaid users account for more than 85 percent of mobile devices worldwide.[4] The perceived value of a monthly premium for security software is limited when the user's typical monthly top-up is just $10.

Smart device customers are the ones driving carriers to invest in LTE. Service providers with saturated markets want to sell mobile apps and data services to smartphone and tablet users. "In 2012, a fourth-generation (4G) connection generated 19 times more traffic on average than a non-4G connection. Although 4G connections represent only 0.9 percent of mobile connections today, they already account for 14 percent of mobile data traffic."[5]

Machine-to-machine (M2M) communications and over-the-top (OTT) content

New apps and services are also connecting new categories of embedded wireless devices to create a rapidly evolving "Internet of Things," providing growth and revenue opportunities for carriers in the face of declining margins in established lines of business. These machine-to-machine systems attach to networks (including the Internet) in many ways, but wireless networks often present an optimal form of connectivity, enabling: remote industrial control systems (ICS); location and tracking of transportation and logistics; broadband delivery of third-party video and gaming content; wireless thermostats; health applications and services; innovative home automation; and much more. Typically built with limited power, processing, and memory resources, these devices require specialized security. Attackers will target such under-protected M2M systems to disrupt critical infrastructure or commit fraud.

Voice goes digital

Already, 3G and 3.5G wireless networks have leapfrogged PSTN/twisted pair networks to service rural communities, especially in the Asia Pacific, Latin American, and African regions. Access points inside the home provide the local network interface, and LTE networks are being deployed to backhaul the data traffic.

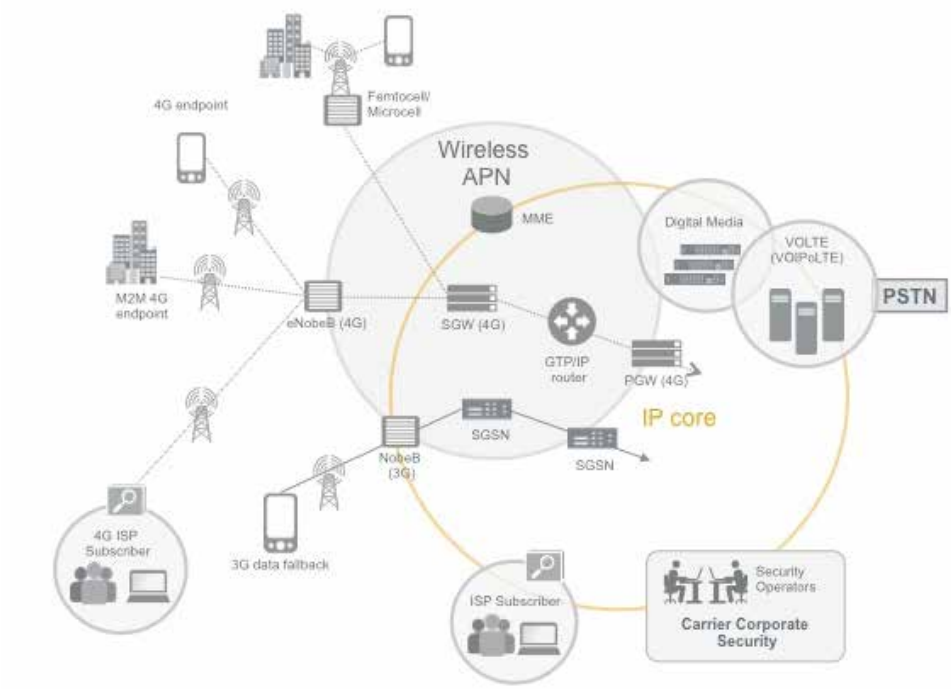

Figure 3. A 4G Reference Design (with 3G fall back).

While initially providing data capacity and leaving voice service to older 3G technologies, LTE won't remain a data-only network for long. It has a planned upgrade and migration path to support voice and data services as one. As voice services transition to all digital VOLTE, the data network will also be the voice network. All assets on the network will be running on top of Internet Protocol. Eventually, there will be no fallback to analog, circuit switched networks for even basic voice services, while many of the applications in the Internet of Things will not ever function on such legacy networks.

The conclusion should be clear. We are facing growth in malware and increased threats targeting poorly-protected devices, increasing device and service diversity and sensitivity, and critical service dependency on 4G availability. These trends all justify the effort and cost of making LTE networks not just highly efficient and available, but also secure.

The 7 Deadly Threats to 4G

The changes specific to 4G permit seven unique variations on older attacks. By understanding the nature of these threats and vulnerabilities, carriers and service providers can act to mitigate them.

Threat 1: Wireless APN flooding

The expanding bandwidth of 4G provides a larger attack surface for cybercriminals. The dribble of data through a 24 kb–256 kb 2G and 3G wireless network becomes a flood of data with 3-150 Mbit 4G networks. In the absence of aggressive countermeasures, criminal activities will consume so much of this new bandwidth that users who have paid to upgrade to 4G service will get 2G speeds, as was illustrated in our earlier example, Figure 1.

Figure 4 illustrates the attackers' automated probing and scanning software and the traffic from "enslaved" devices that can quickly monopolize core bandwidth. These actions can flood the wireless architecturally private network (APN) that connects the mobile devices of the 4G network to the Internet. The attacks can consume the "last mile" of scarce, wireless capacity (radio frequencies are physically limited assets—you cannot add more to get more capacity as with fiber or copper wire) and degrade service levels.

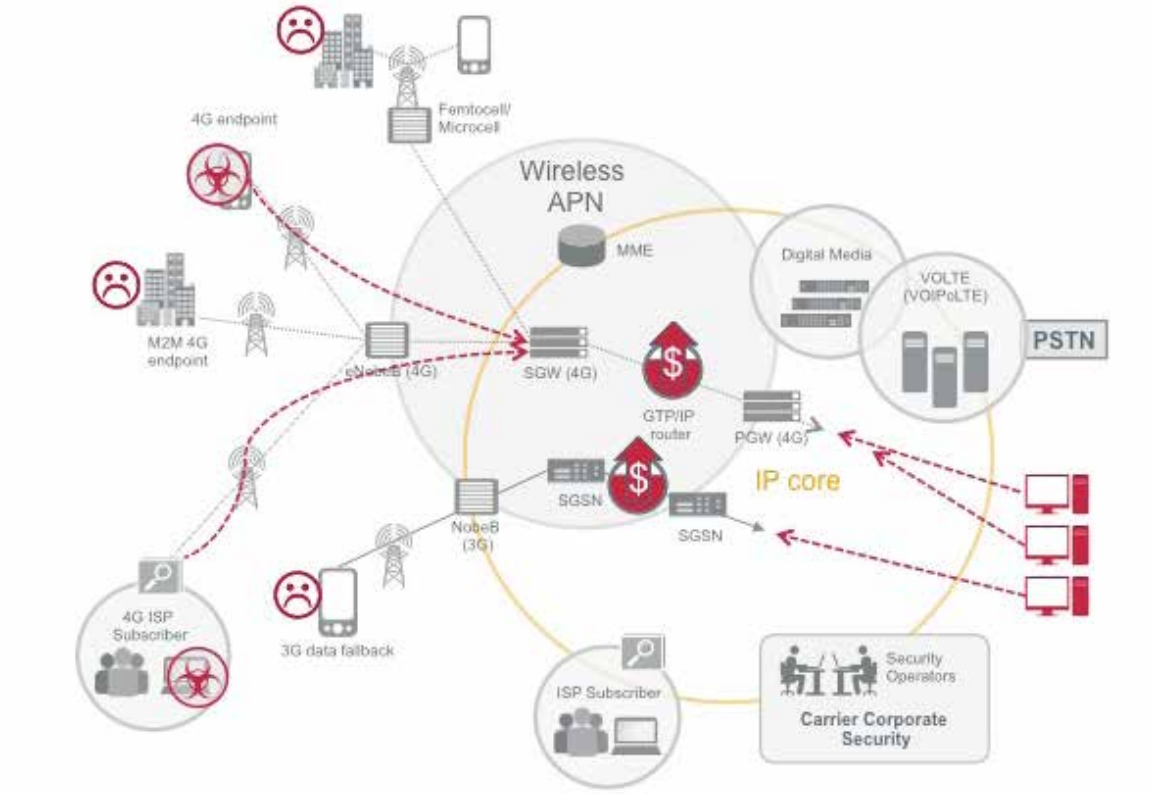

Figure 4. Attacks into a mobile network.

Threat 2: Mobile to mobile attacks

Unlike 3G traffic that tunnels directly into the core IP network from the mobile device, 4G traffic is all IP-based and can travel directly from mobile device to mobile device inside the wireless APN. This "peer to peer" (P2P) communication reduces backhaul traffic. However, it also permits mobile-to-mobile (Mob2Mob) attacks.

A compromised mobile device can target and scan large numbers of other, locally adjacent, mobile devices at once, consuming huge amounts of spectrum. This activity frequently goes unseen by the carrier because the wireless APN to which the device connects has limited instrumentation and few internal security capabilities. In addition to siphoning off spectrum, a mobile to mobile attack drains the battery on the victim's device by maintaining a network connection. The attack can also cause a denial-of-service (DoS) situation due to signaling congestion.

In an attack, the traffic may enter the network from one mobile device, perform an automated scan to look for devices with similar IP numbers (indicating that the devices are on the same subnet), and then reach back out over the 4G network to contact those devices. Once an attacker has exhausted one range of IP addresses, the attack moves to the next range and begins to attack and infect the new devices. Unfortunately, the mere act of scanning for responding IP addresses of other mobile devices can cause severe DoS due to the previously mentioned signaling congestion.

To avoid users being denied a connection, the operator would need to invest in better security or: more spectrum, more LTE base stations (eNodes), and more backhaul network—which lead to more capital expense, more operating expense, and more management complexity. The user may experience degraded service and also shoulder the burden of these incremental costs over time. Inevitably, unhappy users lead to account churn.

Threat 3: eNodeB/Femtocell/Microcell compromise

As part of a cost containment strategy, many carriers are adopting virtualization technology at the radio edge, in the mobility management infrastructure, and even in the networks.[6] These commodity hardware platforms and commercial, off-the-shelf software components have the ability to increase equipment utilization and drive down capital and operating costs.

However, virtualization in mobile networks may also introduce vulnerabilities that attackers can exploit. For example, a common eNodeB (4G basestation) may use a virtualized Linux operating system instead of a custom OS that has been explicitly hardened—made secure—during development. If a virtualized eNodeB in the 4G network is successfully attacked through a security flaw in the commercial hypervisor or operating system of application (radio) software, it may fail. Or, worse, it may become a launching pad for attacks against the overall network management infrastructure behind it. Each lost Femtocell hurts service availability for multiple users.

With its position in the IP core, loss or compromise of the management infrastructure takes down a much higher number of users. It is the critical control point for the 4G network, accessible from Femtocells, Microcells, and eNodeB as a matter of design.

It's true that the management infrastructure generally shelters within the protection of the network, but this infrastructure still needs to maintain open connections to service its users. If an attacker can get into a trusted device like an eNodeB, the attacker can navigate to many other internal devices (such as the management infrastructure). Once they have penetrated the network infrastructure, attackers have many ways to disrupt services or cause outages—outcomes that hurt revenue and customer retention.

Specialized security optimized for hypervisors and other virtualization technology can mitigate the risks of attack. This security adds comparatively minor costs relative to the costs of service degradation, as measured in lost usage revenues, customer churn, service level breaches, and regulator audit and inquiry.

Threat 4: Machine to machine fragility

The Internet of Things (IOT) includes not only devices managed by people, such as desktops and smartphones, but semi-automated and fully automated devices that control physical outcomes, such as traffic lights, pipeline pressure sensors, electrical grids, and water utilities. These devices are sometimes referred to as engaging in "machine-to-machine" (M2M) networking. Traditionally, these fixed-function devices were built without much concern for security, since they used limited, dedicated networks that were not connected to a public network.

Simple probing of the network (performed by vulnerability scanners as well as would-be attackers) can have adverse effects by destabilizing controllers. Hindering potential mitigations, field-based sensors are resource-constrained, with minimal memory and CPU to spare: there is no "room" to install firewalls or even basic security capabilities.

In some cases, these devices run legacy, unpatched, and unpatchable operating systems. In most cases, even modern M2M systems and devices are not intended to operate within the hostile and unhygienic environment of the Internet—yet that is what 4G will become without adequate security.

When attacked, devices may just shut down—without warning, and sometimes without an easy or fast recovery. Disruption of ICS devices can lead to costly civil emergencies or loss of life. This feared scenario is driving critical infrastructure operators and the governments that regulate them to invest heavily in understanding and implementing more rigorous security controls. For service providers looking to provide the networks for these burgeoning new M2M applications, a degree of security and awareness related to mobile-on-mobile attacks will be a business enabler.

Threat 5: Lawful intercept compliance

National regulations and licensing rules typically obligate carriers to intercept many different types of traffic when they receive a judicial order. In 4G networks, full interception for a given endpoint requires data collection at up to three different places in the IP network, as seen in Figure 5:

- *Edge cache traffic*—Create a system for managing copies of frequently requested content that is stored at the edge of the network, so one copy can serve many endpoints without multiple downloads through the backhaul network.
- *Voice calls*—Track and intercept voice over IP and voice over LTE traffic.
- *Internet traffic*—Intercept "long haul" email and web interactions headed to and from the Internet directly (versus the edge cache).

Government regulators expect carriers to solve this problem before LTE services go live. Actually, regulators don't necessarily possess any awareness of LTE or 4G network improvements. They simply require that judicial orders are fulfilled. The problem of "how" is largely left to the service provider to figure out.

Additionally, lawful access requests typically come with precious little compensation for service providers, so the more efficient and elegant the solutions, the better! Designing this interception, monitoring, and collection capability into the relevant points of the network will allow you to preserve your network compliance with lawful access requests and judicial orders.

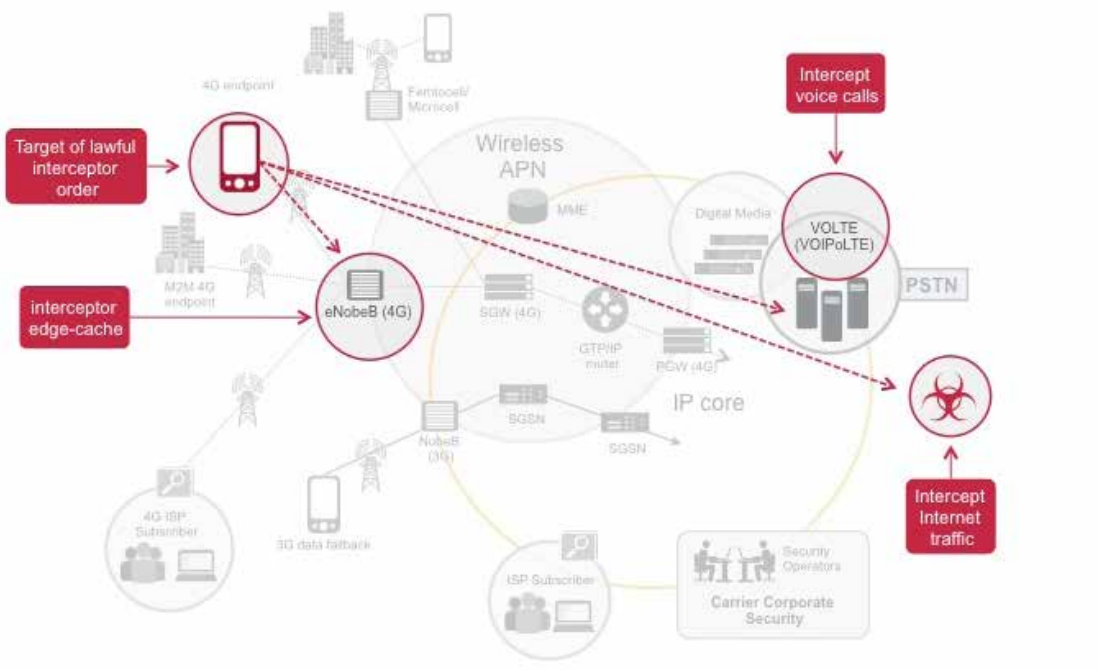

Figure 5. Compliance requires support for multiple lawful access intercept points.

Threat 6: VOLTE service assurance

So far, we have looked at the weaknesses of different devices that participate in the "data" side of the 4G network, which leads to the open Internet and the wealth of data and services to be found there. However, there are other services that will reside entirely inside the 4G network. These services represent substantial value to device users: namely, the voice services and media services.

VOIP attack tactics that have evolved on the Internet can be used just as effectively against VOLTE, even if the VOLTE infrastructure is not accessible from the Internet. Why? Because VOLTE infrastructure must be accessible from any mobile device subscribing to voice services from the service provider. In this age of pre-paid accounts and phones purchased and topped-up from automated kiosks, restricting only "friendly" and recognized subscribers to the VOLTE infrastructure is difficult.

There are several thousand known attacks against VOIP protocols that range in outcome from capturing administrative privileges to denial-of-service attacks. The impact on voice services to consumer and business users, as well as emergency services that support police, fire, and medical resources, can be highly disruptive and dangerous and result in regulatory issues. Because VOLTE traffic remains largely within the wireless APN, carriers need different monitoring equipment to detect attacks as they move through the 4G infrastructure to the VOLTE service infrastructure.

Threat 7: Content and media delivery

Paid-for content and media, such as movies or music-on-demand, are another element of the 4G broadband ecosystem. They present the potentiality of significant additional revenues to service providers, especially since up to 50 percent or more of the data travelling over the Internet is already video, according to Cisco.[7] Making video and music available from localized portals connected directly to the wireless APN can offer performance and variety (due to formalized licensing and digital rights management) that cannot be had from "over the top" services accessed via the Internet.

As was the case with VOLTE, unauthorized access and denial-of-service attacks can jeopardize expected revenue from broadband media services, degrade services, and erode subscription and adoption rates. Carriers should expect attackers to attempt to disrupt content delivery systems during peak times. Internet criminals, hacktivists, and other malicious parties are adept at unleashing their attacks during major events—World Cup matches, elections, or royal weddings, for example.

Additionally, wholesale disruption of a broadcast service will be much more visible than a large number of usually unrelated dropped calls. Subscribers who have paid a premium to watch a major sporting event will quickly share their anger through social media. This damages your organization's reputation and can dampen subscriptions and long-term adoption of new services.

4G Security Reference Design

With this understanding of the threats facing 4G networks, we can now explore some appropriate countermeasures and mitigations. We start by assuming that the 4G network endpoints—mobile devices and remote sensors—cannot be fully "trusted." Three issues make trust impossible: software control, physical control, and accountability of users.

- *Software control*. Carriers can't guarantee the presence of security software on these devices. Many devices can have software removed or disabled by the user, while fixed-function devices don't have the capacity to run traditional software.
- *Physical control*. Criminals can get physical access to ports, memory, and interfaces on these devices, which make all manner of tampering much easier to accomplish, including the introduction of malware.
- *Accountability of users*. Most mobile devices on the network that are operated by people (smartphones, tablets, and laptops) are pre-paid or pay-as-you-go. Many prepaid devices don't require personal or account identification, so they foster the anonymity of criminals.

While these factors could change over time, for now we must build the security necessary to counter the seven 4G threats into the IP core and wireless networks, not the devices.

Perimeter security for broadband wireless networks

Today's "first generation" protections for the broadband wireless network typically include firewalls or intrusion prevention systems (IPS) that inspect traffic at the perimeter of the wireless APN: the border of the Internet and the wireless infrastructure. The first threat, APN flooding, can be partially mitigated by upgrading these network gateways to include reputation-based blocking and packet inspection.

IP reputation-based blocking can provide effective, real-time protection against attacks to mitigate the deluge of unwanted traffic at the network's edge. The accuracy of this approach greatly depends on access to reliable, community-based reputation databases and how frequently the feeds are updated.

Packet inspection is an equally important approach to filtering malicious broadband traffic. It examines the header and data components of a packet as it passes the gateway inspection point, searching for protocol non-compliance, viruses, spam, intrusions, or other defined criteria.

McAfee network security solutions

Reputation-based blocking is a simple option to deploy with McAfee products. McAfee network protections do a lookup of source and destination reputation through the McAfee Global Threat Intelligence (GTI) network. Based on the previous activities of that source or destination, McAfee provides a risk assessment that guides the firewall or IPS to drop or allow the network traffic according to the policy or tolerance configured by the administrator.

In wireless APN flooding, when an Internet-attacker transmits high volumes of traffic to and from high volumes of devices, the attacker's IP address may be flagged as potentially risky in the McAfee reputation database, or a rule-set within the firewall or IPS may simply flag such behavior as illicit and "treat" traffic from that source. "Treating" may include anything from slowing the rate of flow to dropping the packets outright.

You can easily define rules to tell a McAfee IPS to block this sort of traffic, including rules for geolocation (which can let you block traffic with countries known to host malicious traffic). A template generates alerts and reports the APNs in the attack, and this data stream can feed the McAfee security information and event management system (SIEM) as well. McAfee threat intelligence feeds also include message reputation and file reputation to facilitate advanced network security functions and value-added services.

The choice of IPS versus firewall on the perimeter will depend on the use of network address translation (NAT). If you do not use NAT or routing, then the McAfee IPS will deliver better performance for this purpose, whereas firewalls will support NAT.

McAfee IPS sensors can be placed as needed at the perimeter and within the APN and roll up data and monitoring processes in a common management and reporting environment.

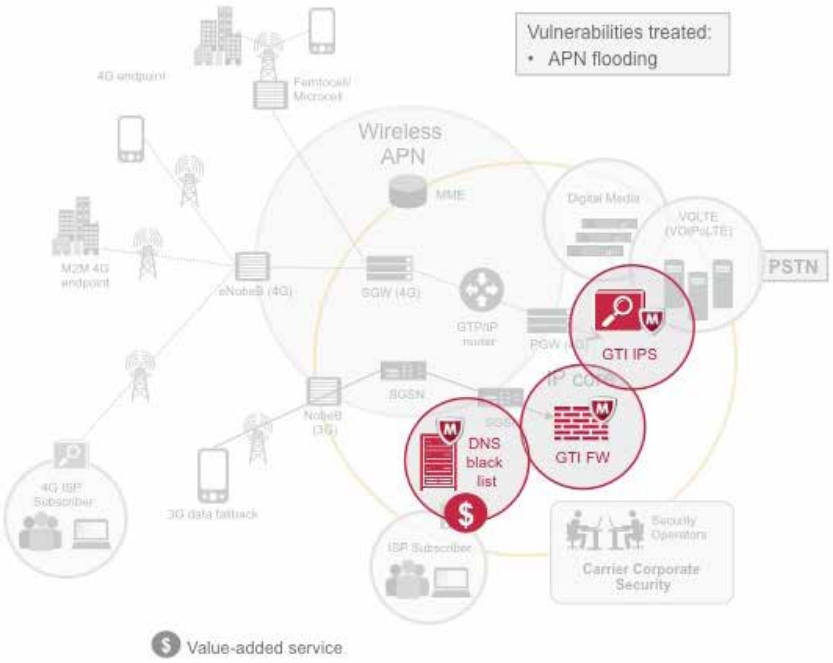

Figure 6. Network security protecting the core combats APN flooding.

An IPS on the perimeter can only see attacks crossing the perimeter, to or from the wireless APN. It does not inspect traffic within the APN (see Figure 6). "Second generation" wireless security adds instrumentation inside the APN to supplement perimeter security and combat attacks that target and occur within the APN.

DNS blacklisting service

Reputation intelligence also enables another valuable—and potentially profitable—security control tactic called Domain Name Server (DNS) blacklisting. When a user contacts a risky address (for instance www.bad.com), either directly or in response to a phishing email, Domain Name Server (DNS) blacklisting rules can apply reputation to block or redirect the request to a warning page or apply whatever treatment is considered appropriate by the service provider. DNS converts a text stream (www.bad.com) to an Internet Protocol address (10.10.10.10) that enables networks connections on the Internet: DNS blacklisting allows providers to interrupt the text-to-IP address conversion by injecting a new IP address (like a security warning web site) when a known bad IP address is about to be returned to a user who looked up www.bad.com.

Some carriers are deploying DNS blacklisting at no extra charge as a basic service that reduces risky traffic. If you add analytics and usage data, you can offer a value-added service that helps businesses reduce illicit traffic in the network and support Internet usage rules and laws—such as family safety laws. Although determined and smart users can work around DNS blacklisting, this service helps honest people avoid accidents, cons, and malice. DNS blacklisting also represents a highly effective first line of cybersecurity for enterprises and a simple, cost-effective way to show due care.

The recommended security architecture places an IPS sensor with active threat intelligence between the serving gateway (SGW) and packet data network gateway (PGW) (see Figure 7). This IPS sensor can decode the GPRS Tunneling Protocol (GTP) unique to wireless networks. The IPS will identify infected or malicious devices that can roam onto the network and mobile-to-mobile attacks that might otherwise not be identified. It can monitor and filter the traffic to help mitigate five of the seven threats we have described:

- Mobile to mobile attacks
- eNodeB/Femtocell/Microcell attacks
- Machine to machine (M2M) fragility
- VOLTE service assurance
- Content and media delivery

Preventing these attacks will help you avoid service degradation and outages that drive away customers and drive up costs. As part of your service design, consider the ability to include automated reporting and alerting as a value-added service to enterprise subscribers of wireless broadband (for instance, those buying large numbers of wireless identities to support machine-to-machine systems).

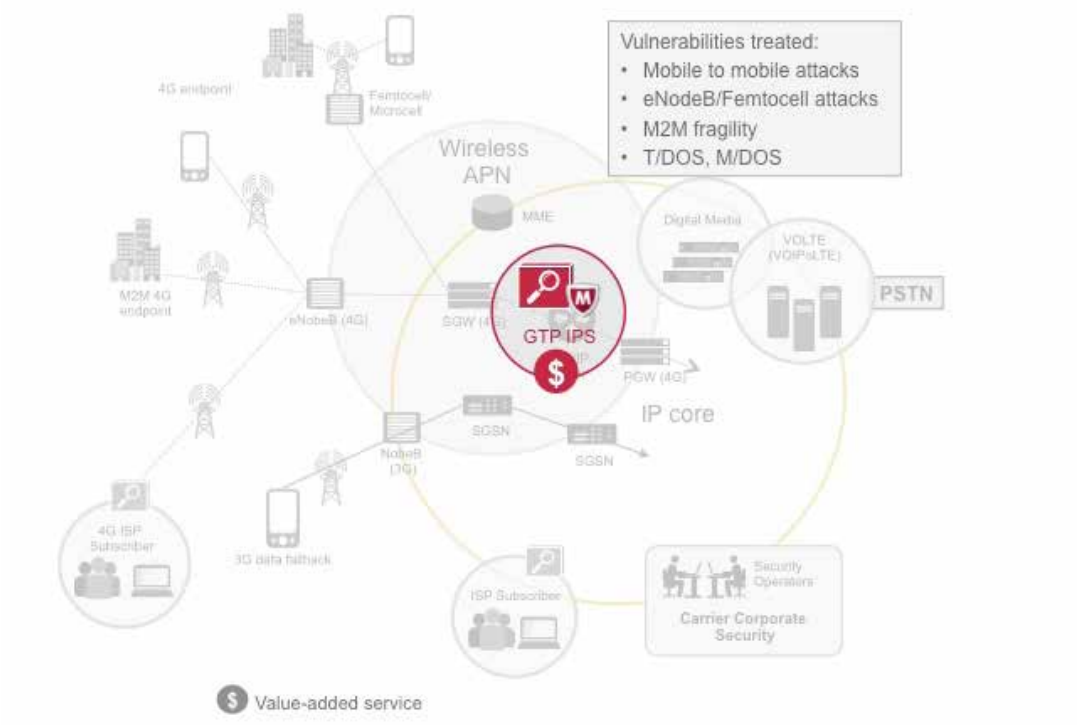

Figure 7. Network security within the APN combats several 4G threats.

Value-added services

As with the DNS blacklisting service mentioned earlier, carriers and integrators also have the option of offering a menu of tiered services related to IPS: basic service that uses built-in filtering malware, an upsell that includes reporting of where and when traffic is headed from mobile devices, or premium policy management and security monitoring helpdesk services. By deploying a multi-tenanted IPS sensor within the network, you can spread costs over multiple clients to achieve economy of scale.

For instance, M2M applications riding on the network depend on service quality. You can help M2M application owners monitor and pinpoint issues associated with devices in their M2M network. And an appliance that can monitor for unusual traffic coming or going through the M2M network creates tangible evidence of due care associated with security controls, in order to mitigate liability.

Virtualized infrastructure security

While the IPS sensor can provide inspection to block malicious traffic in the wireless APN, you also need to protect the network components at the edge of the evolved and virtualized 4G network:[8] for instance eNodeB basestations, Femtocells, and microcells (small coverage basestations). By protecting against attacks starting at the radio edge, you help preserve backhaul (up to 25 percent of wireless network operating cost) and implement controls supporting lawful intercept compliance.

Femtocells and microcells will often be located in premises not controlled by the carrier. These devices will require additional logical security to mitigate potential physical attacks on the terminal, in addition to attacks from malicious users on the network.

For devices built with commercial hypervisors and running commercial operating systems like the Linux OS, mitigating vulnerabilities associated with counterfeit, rogue, or "gray market" devices is another security challenge. This problem must be addressed through a combination of hardware- and software-based security controls.

Active images

Application whitelisting permits you to lock down the applications running on the radio-edge devices (such as eNodes and Femtocells) so that only the desired, trusted applications can execute. This whitelisting, as well as file system encryption and change monitoring, can help you prevent changes to the software on the edge, whether introduced by someone with physical access to the device or by an attacker connecting over the network.

Application whitelisting is an appropriate security control on the network edge, because the images will change infrequently (unlike, for instance, a personal PC, which changes constantly). Additionally, whitelisting does not rely on the ability to constantly download new signature files, which loads the backhaul network with update traffic from potentially hundreds of thousands or millions of edge devices.

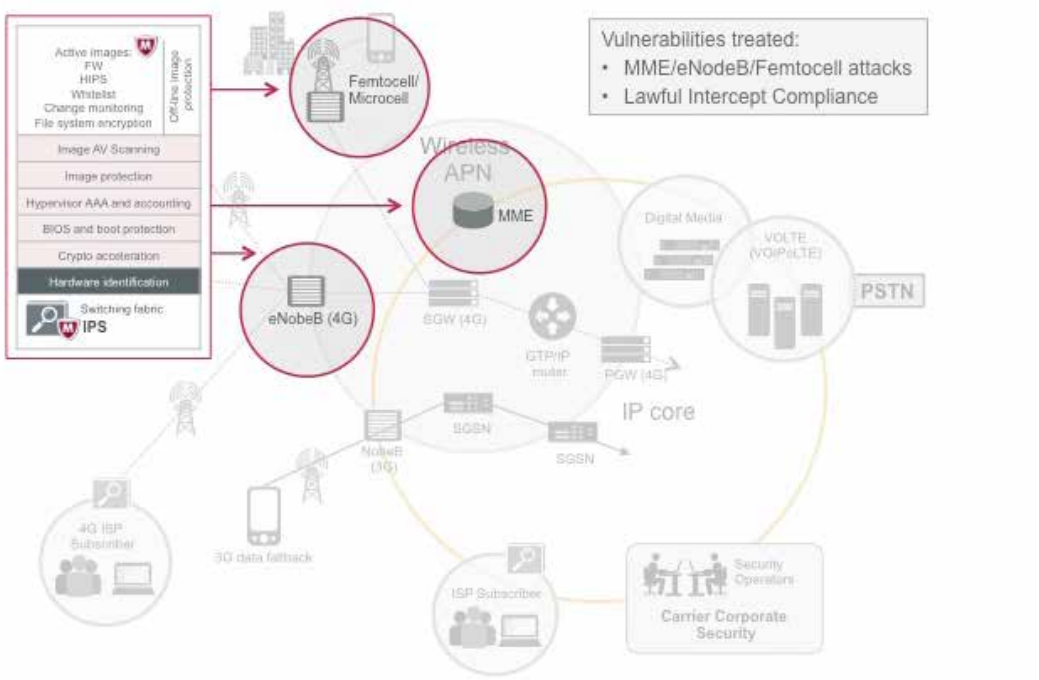

Figure 8. New security software such as whitelisting can help protect virtualized equipment.

Through integration with event correlation and analysis engines, the edge IPS could be coordinated with the core network IPS. By advising of new attack signatures and behaviors, discovery of an attack at either point (edge host or core network sensor) can allow all protective devices to recognize, intercept, and drop traffic.

The concern about lawful intercept compliance can be met with controls that can intercept and report out traffic from these different places on the network, as well as the VOLTE network. Data from IPS sensors positioned in these traffic flows can be rolled up to a central location for monitoring. Carriers using a 3G fallback solution can collect this traffic at the radio edge as before.

McAfee solutions for virtualization

The McAfee approach to virtualization security helps service providers optimize virtualized resources and ease management of the virtualized systems that are becoming a core part of carrier infrastructure. McAfee solutions overcome the unique concerns that arrive with virtualized infrastructure:

- Performance of shared platforms and resources
- Exploitation of shared platforms and resources
- Integrity of active and offline virtual machines
- Hypervisor security
- Security of the virtualized networking within the hypervisor
- Server imaging standards and patch levels
- Physical platform authentication

McAfee solutions include virtualized appliance versions of proven security products such as the McAfee® Network Security Platform and McAfee Firewall Enterprise, as well as innovations like McAfee Optimized for Virtualized Environments (MOVE AV) and McAfee VirusScan® Enterprise for Offline Virtual Images. These specialized technologies make our best traditional antivirus and host intrusion prevention capabilities work efficiently within virtualized deployments, with both hypervisor-aware and hypervisor-agnostic options to preserve flexibility. In addition, McAfee products extend key controls such as application whitelisting and change control into the virtual environment.

Conclusion

From a security perspective, the race to build and introduce 4G can be a headlong dash into the unknown. A proactive implementation of security can help you win by stabilizing operational costs, maximizing infrastructure utilization, and improving customer satisfaction. By understanding and mitigating the seven primary threats that come with the bandwidth and Internet-oriented technologies of 4G, carriers and service providers can win the allegiance of customers while supporting a healthy value-added service revenue stream.

The McAfee telecommunications service provider program has resources to help you design security into your 4G wireless infrastructure. To learn more, visit McAfee Telecommunications Service Providers and mcafee.com/securityconnected.

About the Author

Tyson Macaulay is the Vice President–Global Telecommunications Strategy for McAfee. Mr. Macaulay is accountable for the definition of value-added solutions, business models and thought-leadership specifically for the global telecommunications industry. Previously, Tyson served as the Security Liaison Officer at Bell Canada for eight years where he was responsible for technical and operational risk management solutions for Bell's largest enterprise clients. Prior to that he was Director of Risk Management for a U.S. defense contractor in Ottawa–Electronic Warfare Associates (EWA 2001–2005), and founded General Network Services (GNS 1996–2001). Tyson's career began as research consultant for the Canadian Federal Department of Communications (DoC) on information networking, where he helped develop the first generation of Internet Services for the DoC in the early 1990's.

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ: INTC), empowers service providers, businesses, the public sector, and home users to safely experience the benefits of the Internet. The company delivers proactive and proven security solutions and services for systems, networks, and mobile devices around the world. With its visionary Security Connected strategy, innovative approach to hardware-enhanced security, and unique global threat intelligence network, McAfee is relentlessly focused on keeping its customers safe. http://www.mcafee.com

[1] McAfee Threats Report First Quarter 2013.

[2] Source: Cisco Visual Network Index Global Mobile Data Traffic Forecast.

[3] Sharma Consulting, 2012.

[4] International Telecommunications Union (ITU).

[5] Source: Cisco Visual Network Index Global Mobile Data Traffic Forecast.

[6] See IDF 2011–The Future, http://download.intel.com/newsroom/kits/idf/2011_fall/pdfs/IDF_2011_Rattner_Presentation.pdf, and see Implementing SDN and NFV with Intel® Architecture, http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/sdn-part-2-secured.pdf

[7] http://www.cisco.com/en/us/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-481360_ns827_networking_solutions_white_paper.html

[8] Note: Current 3G and current 4G infrastructure is not virtualized. These infrastructures are based on highly customized equipment. In the immediate future, this infrastructure will be converted to run on commercial platforms (virtualized systems of hypervisors and operation systems) to achieve better performance and flexibility.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

60437wp_4g-threats_0813_fnl_ETMG