Wireless security in LTE networks

Monica Paolini
Senza Fili Consulting

Sponsored by

f5®

SENZA FILI CONSULTING

1. Introduction

Mobile security, a top-of-mind concern for operators

When using smartphones to make a call, socialize with friends, check traffic or watch a video, few subscribers are concerned about security – of the device, of the content or of the network. They are more likely to be concerned about having good coverage, a fast connection or sufficient battery life than whether their mobile data traffic is protected.

The mobile security record to date has been quite good. Because voice-dominated networks have been built on proprietary interfaces, mobile networks have been difficult to penetrate, and have provided less incentive for malicious attacks than the more open and data-rich IT networks.

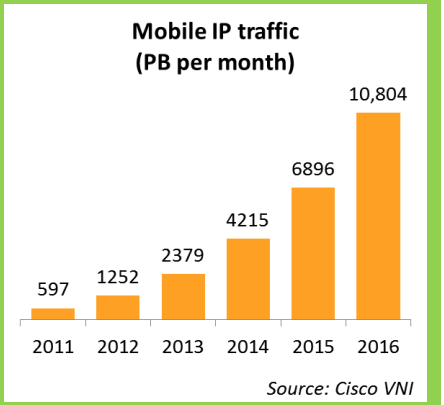
This is rapidly changing. Mobile networks are becoming primarily data networks, moving to a flatter and more open architecture that is inherently more vulnerable to security threats. This transition is gathering momentum both with the adoption of smartphones and the applications they support, and with the transition to a less hierarchical, IP-based architecture in LTE.

The exponential growth in traffic makes it more difficult for operators to protect their networks. Furthermore, most third-party application developers are not directly concerned with (or affected by) security. Hackers and hacktivists have started to shift their attention to mobile networks and are on a steep learning curve, as the sudden spike in malware over the last year shows. Additional threats to network integrity come from non-malicious accidental traffic floods from devices or other network elements.

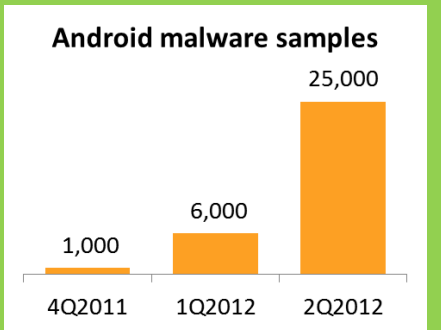
As business subscribers increasingly use mobile devices to connect to their corporate networks, mobile networks become more attractive targets to both hackers and hacktivists[1]. Security is set to become a major source of network disruption, and a top-of-mind concern for both operators and subscribers.

Mobile networks are becoming more attractive targets for security attacks

- There are twice as many mobile-broadband subscribers worldwide as fixed-broadband ones. Their number is growing by 45% per year (ITU).
- According to the Cisco VNI, mobile data traffic is growing by 78% per year and will account for 10% of global IP traffic by 2016 and represent five times the volume of global internet traffic in 2005.
- Trend Micro has reported a rapid growth in Android malware samples.



Source: Cisco VNI



Source: TrendLabs Malware Blog, Trend Micro, 2012

1. "Android Malware Could Infiltrate Corporate Networks", Wall Street Journal, 2012.

2. An evolving landscape
Mobile security in an IP environment

The transition to data-centric, IP-based mobile networks supporting a rapidly growing number of computationally powerful devices such as smartphones and tablets is changing the mobile security landscape and will fundamentally change the way we perceive and deal with mobile security. Mobile networks are becoming more pervasive, more widely used, and more deeply connected to other networks (Table 1).

Devices and the core network are the most heavily targeted parts of the mobile network, while RAN and backhaul have attracted fewer security breaches (Figure 1). Although RAN and backhaul attacks may increase, they are likely to remain more confined. This is because RAN and backhaul have complex deployment configurations that are specific to operator, location and equipment vendor, and attacks require more sophisticated preparation and on-site access.

However, small cells, femto cells and Wi-Fi hotspots integrated with cellular networks will make attacks on mobile networks easier to plan and carry out.

Furthermore, attacks on the RAN and backhaul may attract a different type of threat, aimed at the network infrastructure per se rather than, for instance, access to corporate networks or sending unauthorized premium-rate SMSs. This sort of attack is more likely to be driven by hacktivists with a political or social agenda than by hackers trying to get an economic return.

Table 1. How wireless security is changing

	What we were used to	What is coming
Network architecture	Closed, proprietary, hierarchical networks: difficult to penetrate, easier to protect.	Flat networks, more connections among elements: more porous, easier to penetrate.
Equipment	Expensive RAN equipment, large form factor: difficult to buy or operate a rogue base station.	Femto cells, small cells and Wi-Fi hotspots: easier and cheaper to get, they provide an entry point to the mobile network.
Devices	Voice-based network, limited data capabilities: easier for operators to control.	Powerful data-centric devices, visible from the internet: increased vulnerability, more entry points, less control.
Signaling	SS7: closed signaling environment, difficult to penetrate.	Diameter: IP increases mobile networks vulnerability to security threats.
Applications	Few applications available or used: limited entry points to devices.	Applications in a fragmented market that is difficult to control: a source and vehicle for security threats.
M2M	Limited use of cellular networks for M2M applications.	M2M unmonitored devices: difficult to protect, but may have stricter security requirements.
Economic value	Billing fraud as the main concern	Access to corporations and government: mobile networks much more valuable as security targets.

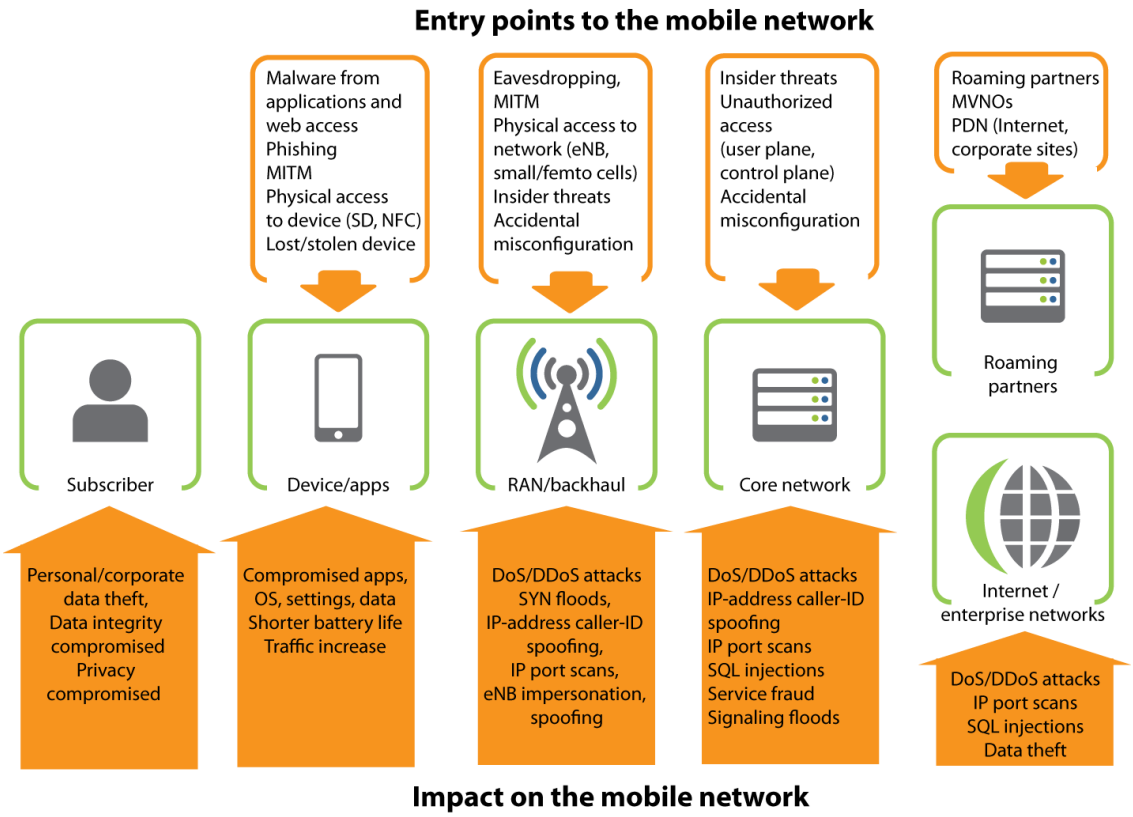


Figure 1. Overview of mobile security: entry points and impact of security threat. Source: Senza Fili

3. Mobile devices
Easier to access, more difficult to protect

From a security perspective, devices play a crucial role within the mobile network and pose difficult challenges to managing them effectively:

- They are the most accessible targets in the end-to-end mobile network, and the most commonly exploited.
- There are a large number of devices in the market, and most lack the tools to manage security.
- Through a mobile device, it is possible to hit both the subscriber (and the linked corporate network, if any) and the mobile core network, as well as to launch attacks on the internet.
- Even if the disruption was caused by unsafe subscriber behavior (e.g., downloading an application from an untrusted source), the subscriber may still hold the mobile operator responsible for the security of the mobile connection.

There are multiple entry points in mobile devices.

Application downloads are the most often used method of spreading malware to mobile devices. The malware can be inserted into a legitimate application by a third party, who then promotes the download of the modified version of the software. Software can also be purposely designed to be a vehicle for the malware and then promoted as legitimate.

By granting permission to collect and transmit information from the device, the subscriber may become exposed to data and privacy loss: the malware may transmit information such as GPS coordinates, contact information, email, or credit card information across the network to a destination set by the malware originators. A common type of malware sends premium-rate SMSs without subscriber permission (or knowledge) and charges the subscriber through the mobile operator for them.

Web-based attacks are triggered by the subscriber accessing compromised or malicious websites that remotely install malware, or that access or modify data stored in the device.

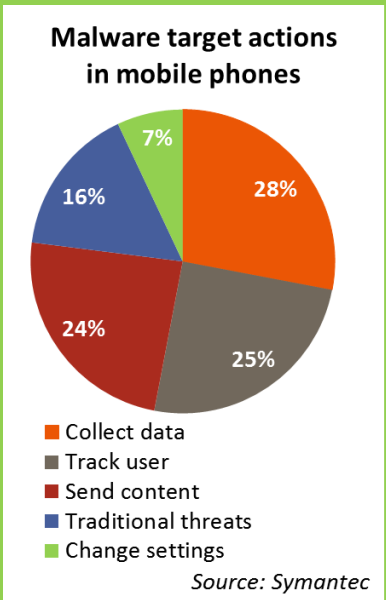
Further security breaches may result from obtaining confidential data through phishing, or through unauthorized physical access to a device (e.g., stealing it or taking a device's SD card long enough to put malware on it). Inappropriate non-malicious data syncing may also lead to data theft. For instance, corporate data may become inadvertently copied in a mobile device that is subsequently infected with malware.

Mobile devices can be used as vehicles for attacks on the subscriber's mobile network, as well as other networks. The mobile operator may not be aware of it or able to contain its effects. Yet there is a potential negative repercussion on the network's reputation when an attack can be traced to originators who are subscribers of one or a few networks, or when the network is used to target the corporate network of an enterprise customer.

Security threats on mobile devices

- Only 4% of French smartphone users are concerned about smartphone viruses, and 22% about online viruses (The Future Laboratory/AVG).
- Only 4% of mobile devices had security software installed in 2011 (Canalys).
- IBM has found a 70% increase in critical mobile OS vulnerabilities in 2011–2010. From 2009 to 20011, mobile OS exploits grew from 2 to 19.
- Trend Micro identified 5,000 new malicious applications in the first quarter of 2012, and another 10,000 in just one month in the following quarter[2]. Among these applications, 17 were able to infiltrate in the Google Play Store and ended up in 700,000 devices before being removed.
- According to Dimensional Research, in 89% of enterprises employees connect to their corporate networks and in 47% they save customer information on mobile devices.

  Mobile devices contributed to an increase in security incidents in 71% of enterprises, with employees representing a more serious security concern than hackers in 72%[3].



2. TrendLabs Malware Blog, Trend Micro, 2012.
3. "The impact of mobile devices on information security: A survey of professionals," Dimensional Research, 2012.

Trends driving increasing security risks in mobile devices

- Rapid increase in adoption of mobile devices, with more users, more devices per user, more syncing and data sharing across devices, and more wireless interfaces (e.g., NFC, Wi-Fi, Bluetooth).
- Fast growth in the number of malicious applications as mobile devices become more attractive revenue-generating targets and because developing a new application requires little time and expertise.
- Wide adoption of Android devices, which are more susceptible to malware than competing OSs because Android has less-strict monitoring processes and allows sideloading (i.e., downloading applications from third parties).
- The enterprise's growing dependence on mobile devices for corporate applications[4]. With BYOD initiatives[5], employee-owned mobile devices connect to corporate networks without direct control by IT managers, who find it difficult to enforce corporate security policies on these devices.
- Low awareness among subscribers about growth in mobile security risks. For instance, permission-based downloads are still one of the major sources of data theft and privacy concerns because most subscribers do not understand or pay attention to the permission requests[6] and end up accepting them all.

4. RAN and backhaul
Increase in flexibility calls for stronger security

The introduction of LTE fundamentally changes the approach to security in the RAN and in the backhaul. In 3G networks, the traffic is encrypted from the mobile device, through the NodeB, and all the way to the RNC, so both the RAN and the backhaul portions of the network are protected (Figure 2). In LTE networks, mandated encryption from the UE stops at the eNB, leaving the IP traffic in the backhaul unprotected. The flatter LTE architecture also exposes backhaul traffic to more entry points, because each eNB can connect through multiple links to other eNBs and network elements.

4. "Mobile lifecycle management," AT&T, 2012.
5. According to Dimensional Research ("The impact of mobile devices on information security: A survey of professionals," 2012), 65% of companies allow employees to use their personal devices for work.
6. A. Felt et al. in "Android permissions: User attention, comprehension and behavior," EECS University of California at Berkeley, 2012, showed that only 17% of participants paid attention to permission requests and only 3% answered correctly to comprehension questions after the download.

Most attacks will be directed at the mobile core network, external sites, and subscriber data and devices, but they can also be more limited in scope and target a single eNB or a group of nearby eNBs (eNB identity spoofing and impersonation). Tampering, traffic hijacking, eavesdropping, DoS, compromised control data, unauthorized access, and loss of accountability of the control plane are the biggest threats to the core network.

Even if the backhaul traffic is encrypted, this architecture creates further vulnerabilities in the eNB. Unauthorized access from external parties or from employees at the cell site has always been a concern in mobile networks, but in LTE it poses a more significant threat because the traffic within the eNB is not encrypted in the transition from PDCP to IPsec.

Furthermore, the higher density and diversity among eNBs lowers the barriers to physical access. In particular, residential femto cells – effectively eNBs that can be purchased for $100 – are an ideal target. Small-cell deployments may also pose increased security threats, because they have the same functionality as macro cells but are installed closer to subscribers, on light/utility posts or other nontelecom infrastructure, where they are difficult to hide and protect physically.

Wi-Fi offload, both in public locations (i.e., hotspots) and in home/office locations, may also introduce new security concerns that go beyond simply offering a new wireless interface through which a mobile device can be accessed. If the Wi-Fi network is integrated with the LTE network, the Wi-Fi access point may have access to some of the elements of the LTE core network, depending on the level of integration. As in the case of femto cells, it is easy to gain physical access to an access point that is part of the mobile operator infrastructure.

As a result, RAN and backhaul traffic has to be treated as untrusted. To secure traffic, an IPsec tunnel has to be established between the eNB, and the MME, SGW and O&M in the core network over the user, control and management plane, and terminated at a SEG that sits at the border of the trusted area.

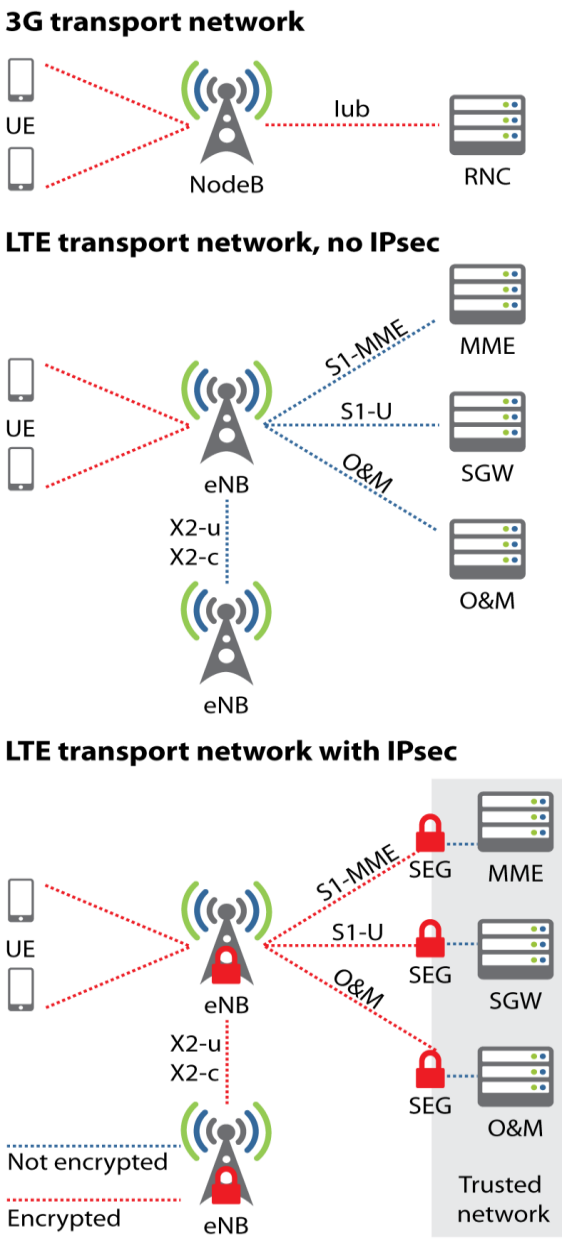


Figure 2. 3G and LTE security: RAN and backhaul. Source: Senza Fili

5. Core network
A new target for mobile attacks

The effects of mobile security breaches targeted at mobile networks are felt first in the core network and, from there, they spread out through the entire network and its subscribers. While attacks directed at mobile devices may have a debilitating effect on the target device and subscriber, their impact remains confined. Attacks targeting the core and transport network have a wider impact, and may affect a restricted area or the entire network.

DoS attacks flood the victim network with a massive volume of requests or messages that the network lacks the resources to address[7]. As a result service may be halted or slowed down. Other types of attack include port scans and SQL injection (Table 2). Unintentional traffic surges due to configuration errors or network updates may have a comparable impact on the network.

The core network is easier to protect from direct external attacks than the RAN and backhaul are, because it is part of the trusted network, where the operator has exclusive control over physical access to the core elements. The challenge in protecting the core network lies in the interfaces to the RAN and backhaul on one side, and to the internet, corporate networks and mobile partners, on the other side.

Table 2. Types of attacks

Attack type	Trigger and impact
DDoS	The target network is flooded by traffic from multiple sources.
Ping flood	A large volume of ping packets causes a network to crash. In a "ping of death," malformed ping requests are used.
SYN flood	The attacker sends a high number of TCP/SYN packets, which the network accepts as connection requests and which overwhelm the network.
Replay attack	The attacker intercepts legitimate signaling traffic and retransmits it until the network is overwhelmed.
SQL injection	The attacker sends malicious commands in statements to a SQL database to make unauthorized changes to the database or to get a copy of the data.
DNS hijacking	The attacker redirects DNS queries to a rogue DNS server.
IP port scans	The attacker scans network elements for active ports and exploits their vulnerabilities.

The trend toward virtualization and software-defined networks will create new vulnerability sources as both the user- and control-plane traffic becomes more distributed across network elements and has to cross untrusted portions of the network.

Firewalls, NAT and DPI gateways, and IPSs will continue to be the main elements to protect mobile networks. To manage signaling traffic and to protect it from security threats, operators will need to add Diameter core network elements such as the Diameter Signaling Controller, the Diameter Routing Agent, and the Diameter Edge Agent. With the increase in traffic volume, both in the user and the control plane, scalability and flexibility have become crucial to effectively managing security threats and preventing the network from becoming paralyzed by sudden traffic spikes, and to adapting to a rapidly evolving environment in which the source, scope, frequency and impact of security threats constantly change.

7. In the US, AT&T recently suffered a DNS outage caused by a DDoS attack that interrupted service for enterprise customers ("AT&T hit by DDoS attack, suffers DNS outage," PC World, 2012).

6. Diameter signaling
What's different about mobile security

Mobile IP networks are vulnerable to the same type of attacks that can be directed to fixed IP networks. But they also are subject to security and network disruption threats that are linked to Diameter signaling and that uniquely affect IP-based mobile networks. Managing device mobility, roaming, complex policy-based billing models, QoS and new services (e.g., IMS-based services, including RCS and VoLTE) generates high levels of signaling traffic directed at different core network elements.

In 3G networks, SS7, a difficult–to-penetrate protocol, is used for signaling. In LTE, 3GPP mandates the use of Diameter, an IP-based open protocol that scales better than SS7 with the increase in signaling traffic volume. Diameter is used for signaling across all core network elements and is crucial to billing, traffic and subscriber management, subscriber authentication, roaming, and mobility management. As a result, security of Diameter traffic is highly sensitive, because the traffic includes user passwords, location data, network addresses and cryptographic keys. IPsec or TLS are used to secure Diameter traffic, especially when it is used to share information with partners, for instance for roaming, or, more generally, when traversing unsecure parts of the network.

While IPsec provides traffic encryption, operators need to take further actions to protect themselves from signaling flood threats, which may be caused either by malicious activity explicitly directed at the mobile network, or accidentally, for instance as an unintended and indirect effect of upgrades or through applications that generate large amounts of signaling when they are widely adopted. Regardless of the cause, signaling floods block or limit subscriber access, and they may also compromise the overall security of the network as some of the core elements' functionality is lost.

In Japan, NTT DoCoMo experienced a signaling flood of this type that disrupted network access in January 2012, caused by a VoIP OTT application running on Android phones[8]. Signaling flood attacks cause congestion in the network and may slow down or even block network access for subscribers.

Diameter signaling floods are an emerging threat to mobile networks, and the industry – mobile operators and vendors alike – does not yet fully understand their causes, forms and impact. Understanding the sources of signaling floods and preventing them is the first priority. This requires better network intelligence and visibility into the dynamics of network traffic, to identify the network's vulnerable entry points and how malicious threats are evolving with time. Tools like topology hiding can be used to prevent or contain attacks directed at the core network. In the event of a signaling flood attempt, operators also have to be able to rely on effective traffic management, including load balancing, policy enforcement, and validation of legitimate signaling traffic to minimize disruption.

8 . "DoCoMo to ask for changes in Android," Reuters, 2012.

7. External networks
Sharing resources, sharing risks

Security threats to mobile networks also come from outside the mobile network. In an environment where networks are connected not only to the internet but to other networks – roaming partners, MVNOs, enterprise networks, infrastructure partners – entry points for security threats multiply.

To enable the same services that are available on the home network on the partners' networks or to provide partners with the functionality they need, operators and their partners need to mutually provide access to some of their core network's elements.

If these partners do not adhere to mobile security's best practices, they put the mobile operator and its subscribers at risk for attacks that may result in network disruption, data theft or corruption, or fraud. But, of course, operators cannot enforce best practices on their partners and typically do not even have visibility into them.

Operators can limit the exposure to threats from external networks with tools like topology hiding that limit the visibility of network elements and thus restrict access. In addition, operators can deploy Diameter edge agents, or DEAs, where their core network interfaces with third-party networks, to protect their core network from both unauthorized access and traffic overload.

Potential third-party threat sources

- **Roaming partners.** Security has always been a concern in roaming because roaming requires home and visited networks to be connected with each other and to share information. Traditionally the set of operators that had a mutual roaming agreement was wide but well-defined, and limited to operators or MVNOs with a license to deliver mobile voice services. With the increasing availability and use of VoIP and data roaming, the range of service providers that are involved in roaming or that have access to signaling interfaces has grown to include OTT players and other service providers. This makes it more difficult to establish partners' trustworthiness and security practices. Security weaknesses on their side may affect the networks of operators that are their roaming partners and may lead to an increase in fraud and, hence, revenue loss.
- **MVNOs.** Mobile operators have to be connected with their MVNO networks and exchange data for subscriber management, policy and billing.
- **Infrastructure-sharing and wholesale infrastructure partners.** Mobile operators have started to adopt infrastructure-sharing and wholesale arrangements to slash costs and increase network utilization. While these agreements affect different elements of the network, the partners have to share access to some network elements (especially eNBs and backhaul), and coordinate network management (which is likely to involve core elements as well).
- **Enterprise networks.** In some cases, mobile operators provide preferential access to corporate networks or operate some infrastructure at enterprise sites that requires a degree of infrastructure sharing (e.g., using the corporate network for backhaul).

8. Conclusions

Keeping mobile networks secure in the face of escalating threat levels

Subscribers and mobile operators have become accustomed to a mobile environment rarely threatened by malicious activities, so they have assumed that security can be guaranteed and it is not a looming concern. The increasing exposure of mobile networks to security threats and the ensuing network disruption is changing this perception, among both operators and subscribers.

Awareness among subscribers is growing as they realize that mobile devices expose them to security and privacy threats. According to the Pew Research Center[9], 54% of application users have declined to install an application and 30% have uninstalled an application due to privacy considerations. In response to subscriber concerns, in the US AT&T, Sprint and Verizon have recently introduced security-protection services to their subscribers.

Security is rapidly gaining high-priority status among mobile operators. The transition to LTE and, more generally, to IP-based mobile networks exposes mobile networks to new and rapidly evolving security threats that can hit the network through devices, the RAN, backhaul, and external, third-party networks.

What to do about wireless security?

- **Use network intelligence and visibility of real-time traffic patterns** to improve detection of malicious attacks and accidental traffic floods, and to understand how they impact the mobile network.
- **Adopt scalable, distributed, and flexible security solutions** to smoothly manage the transition to more porous IP-based LTE networks, keep up with the increase in user and signaling traffic volume, and cope with advanced policy, QoS and charging tools.
- **Strengthen protection of corporate networks,** which are increasingly accessed by mobile devices that are often outside the control of IT managers.

Mobile operators have been very successful at driving mobile broadband adoption among their subscribers. Their success has the side effect of creating more powerful and more extensively used mobile networks, with a deeper reach in our personal (and financial) life and in corporate networks. This makes mobile networks a more attractive target for malicious activity, aimed at either acquiring or compromising data, or at creating disruption to gain a financial benefit, or to pursue a political or social agenda. As mobile data traffic continues to follow its explosive growth trajectory, we expect mobile security breaches to become more prominent, with an escalation in the frequency and severity of attacks, and a corresponding increased awareness among both operators and subscribers. The higher traffic volume as well as the most sophisticated traffic and service management will also increase the incidence and impact of accidental signaling and data floods, which have the same potential impact as malicious attacks.

As they move to LTE, mobile operators need to develop a robust and comprehensive end-to-end security strategy that encompasses the entire network (including device, RAN, backhaul, core and interfaces to other networks) and all traffic (user, control and management planes) to protect their networks and provide a safe environment for their subscribers.

9. Pew Research Center, "Privacy and data management on mobile devices," 2012.

9. Acronyms

3G	Third generation
3GPP	Third Generation Partnership Project
BYOD	bring your own device
DDoS	Distributed denial of service
DEA	Diameter edge agent
DNS	Domain name system
DoS	Denial of service
DoS	Denial of service
DPI	Deep packet inspection
eNB	eNodeB
eNodeB	Evolved NodeB
GPS	Global positioning system
iOS	iPhone operating system
IP	Internet Protocol
IPS	Intrusion prevention systems
IPsec	Internet Protocol security
IT	Information technology
ITU	International Telecommunication Union
Iub	3G interface between the NodeB and the RNC
LTE	Long term evolution
M2M	Machine to machine
MITM	Man in the middle
MME	Mobility management entity
MVNO	Mobile virtual network operator
NAT	Network address translation
NFC	Near field communications
O&M	Operations and management
OS	Operating system
OTT	Over the top
PB	Petabyte
PDCP	Packet data convergence protocol
PDN	Packet data network
PGW	Packet gateway
PKI	Public key infrastructure
QoS	Quality of service
RAN	Radio access network
RCS	Rich communication services
RNC	Radio network controller
S1	LTE interface between an eNode, and an MME (S1-MME, control plane) or an SGW (S1-U, user plane)
SD	Secure Digital
SEG	Security gateway
SGi	LTE interface between the PGW and the PDN
SGW	Serving gateway
SIP	Session initiation protocol
SMS	Short message service
SON	Self-organizing network
SQL	Structured query language
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UE	User equipment
VoIP	Voice over IP
VoLTE	Voice over LTE
X2	LTE interface between two eNodeBs, including X2-C (control plane) and X2-U (user plane)

About Senza Fili

Senza Fili provides advisory support on wireless data technologies and services. At Senza Fili we have in-depth expertise in financial modeling, market forecasts and research, white paper preparation, business plan support, RFP preparation and management, due diligence, and training. Our client base is international and spans the entire value chain: clients include wireline, fixed wireless and mobile operators, enterprises and other vertical players, vendors, system integrators, investors, regulators, and industry associations.

We provide a bridge between technologies and services, helping our clients assess established and emerging technologies, leverage these technologies to support new or existing services, and build solid, profitable business models. Independent advice, a strong quantitative orientation, and an international perspective are the hallmarks of our work. For additional information, visit www.senzafiliconsulting.com or contact us at info@senzafiliconsulting.com or +1 425 657 4991.

About the author

Monica Paolini is the founder and president of Senza Fili. Monica writes extensively on the trends, technological innovation, and financial drivers in the wireless industry in reports, white papers, blogs, and articles. At Senza Fili, she assists vendors in gaining a better understanding of the service provider and end user markets. She works alongside service providers in developing wireless data strategies, and in assessing the demand for wireless services. Independent advice, a strong quantitative approach, and an international perspective are the hallmarks of her work.

Monica has a PhD in Cognitive Science from the University of California, San Diego, an MBA from the University of Oxford, and a BA/MA in Philosophy from the University of Bologna (Italy). She can be contacted at monica.paolini@senzafiliconsulting.com.

Securing Networks with BIG-IP® Firewall

F5's native, high-performance BIG-IP® firewall solutions for communications service providers protect the entire infrastructure and scale to perform under the most demanding conditions. CSPs get the intelligence and flexibility needed to enhance network security in the ever-changing and increasingly threatening landscape, and a common platform to deliver applications and improve responsiveness.

BIG-IP firewall solutions for communications service providers provide:

- Defense against more than 30 DDoS attack types, SQL injections, and SYN flood and IP port scan attacks across both the network and application layers.
- Unparalleled capacity and scalability in throughput, simultaneous connections, and transactions per second.
- Unmatched flexibility and control of network traffic with F5®iRules® —a scripting language that enables you to create incremental security policies in a matter of hours, and to dynamically configure BIG-IP products to filter out unwanted traffic and protect against newly uncovered threats.
- Integration with leading web application scanning tools for comprehensive vulnerability assessments and automated security policy development.
- Reduced hardware and operating costs by as much as 50 percent.

Key features:

- Unmatched capacity and scalability—Better protection of networks against high-volume attacks
- Protection against multi-varied attacks—Broad defense against DDoS, SQL injection, SYN flood, and IP port scan threats
- Visibility, analysis, and compliance—Granular view of violations, attacks, and incident correlation
- Integrated security capabilities—Integrated with leading vulnerability assessment and automated security policy solutions for discovery and remediation in minutes
- Layer 4–7 application layer security—Application layer security and attack protection wherever applications live

Key benefits:

- Stateful firewall—ICSA Labs certified firewall offers unified security solutions
- Carrier-grade—Provides unmatched capacity and scalability to offer better protection
- Unified platform—Reduces exposure to a variety of attacks
- Greater flexibility—Offers customizable scripting language, iRules, for control over security policies and rapid responses to new threats

Security Solutions for LTE Networks with the F5 Traffix Signaling Delivery Controller™ (SDC):

The Traffix SDC is a 3rd generation Diameter signaling solution that has unmatched product maturity in its three years as a commercial router and numerous deployments worldwide. As the market's only full Diameter routing solution combining 3GPP DRA, GSMA DEA and 3GPP IWF, the SDC platform goes far beyond industry standards' requirements including support for more than 50 Diameter interfaces, offering an Active/Active deployment model, an advanced Diameter load balancer, a Diameter gateway to legacy protocols (like RADIUS, LDAP, HTTP, JMS, etc.) and the basis for advanced applications like Billing Proxy, Policy Proxy and much more. With unbeaten performance and ROI ratios of value/cost and capacity/footprint, it benefits operators' balance sheets as well as fulfilling operational requirements for top network performance.

The SDC's Diameter Edge Agent (DEA) offers an advanced Edge Router for secure roaming and interconnecting. These capabilities support the realization of LTE enabling service providers to work freely with third party roaming partners and share resources securely.

Part of the SDC, the Traffix Diameter Edge Agent (DEA) offers operators secure roaming and interconnecting through the following functionality:

- Normalization engine ensuring that only supported AVPs (attribute-value pair) and content enter the network
- High security and failover protection by masquerading the network to prevent unauthorized access, by ensuring that external sessions are routed according to policies set by the service provider
- Guaranteed accuracy of incoming and outgoing messages with mechanisms to either fix or reject the message if the message presents a problem
- Network protection from both overload and draining the network's resources
- Prevention of outgoing messages from content that exposes the network
- Improved Diameter policy rule engine that makes decisions on an unlimited number of AVPs based on destination, origin, location, QoS, rating, vendor, interface or any other information or any combination thereof

Full compliance with GSMA's IR.88 requirements for LTE roaming guidelines:

- Support of IPsec and/or TLS security
- Key KPIs based on unique visibility of all Diameter signaling information entering or leaving the network

About F5

F5 Networks, Inc., the global leader in Application Delivery Networking (ADN), helps the world's largest enterprises and communications service providers realize the full value of virtualization, cloud computing, on-demand IT and network resources. F5® solutions help integrate disparate technologies to provide greater control of the infrastructure, improve application delivery and data management, and give users seamless, secure, and accelerated access to applications from their corporate desktops and mobile devices. An open architectural framework enables F5 customers to apply business policies at "strategic points of control" from the IT infrastructure to an operator's core network and into the public cloud. F5 products give customers the agility they need to align IT and network resources with changing business conditions, deploy scalable solutions on demand, and optimize data and signaling traffic. F5 enables communications service providers (CSPs) to optimize and monetize their networks by leveraging contextual subscriber and network information to provide the ultimate customer experience, maximize network efficiency, and deliver services more cost-effectively.

For more information, go to www.f5.com or www.traffixsystems.com