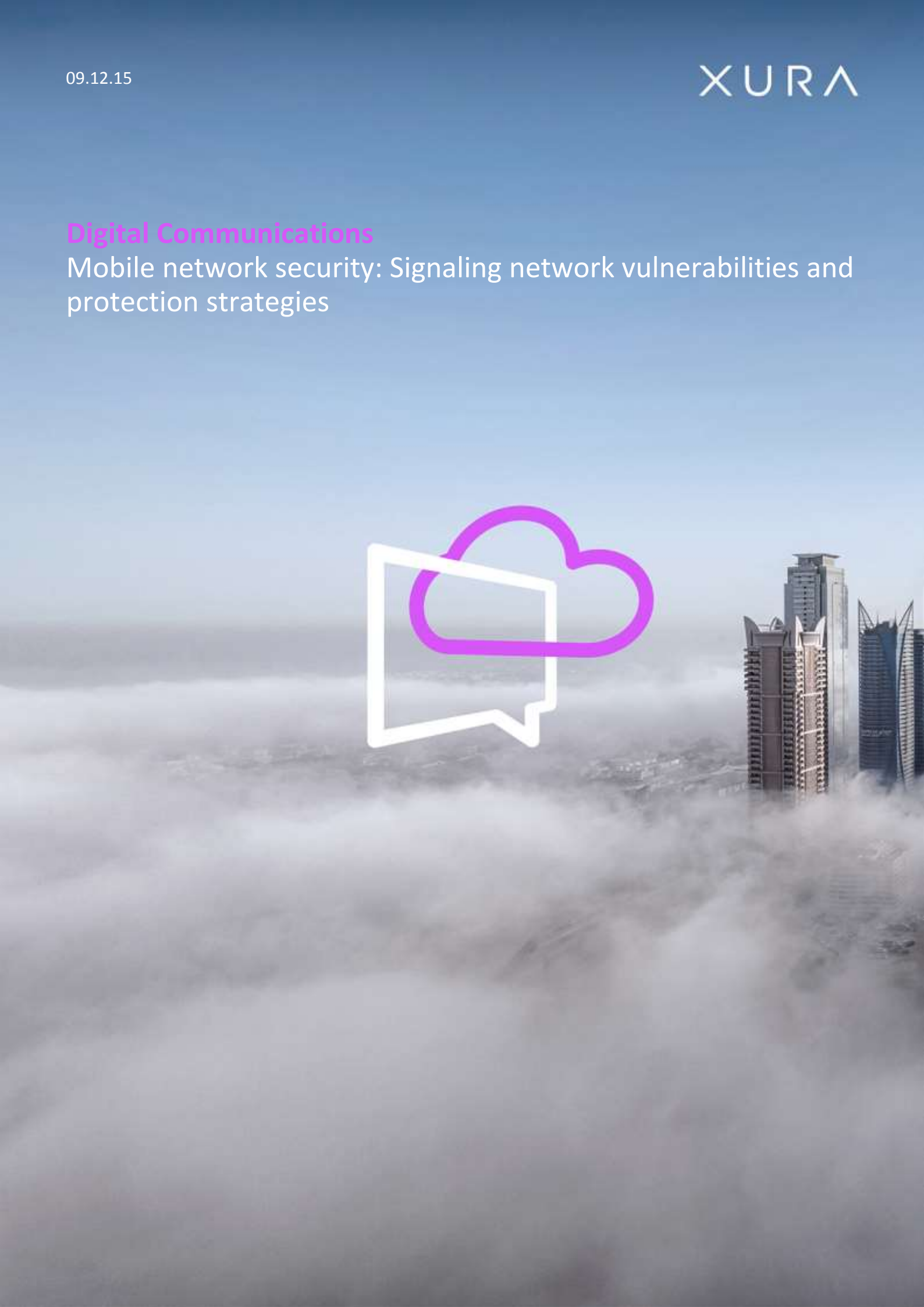
09.12.15

XURA

Digital Communications

Mobile network security: Signaling network vulnerabilities and protection strategies



Mobile network security: Signaling network vulnerabilities and protection strategies

Access to personal subscriber information and using it at the right time can be incredibly valuable if used in acceptable ways or very risky if used by the wrong people.

Introduction

The mobile communication world has experienced a wide range of changes over the last decade. Innovations in handsets, applications and services required shifts in how the mobile operator runs the business. While attention was focused on addressing new business models, services, data monetization etc. underlying industry technology was unknowingly vulnerable to security and privacy attacks.

Gaining access to mobile networks has always been an interest for the various groups of attackers, but due to equipment complexity and specialization of the physical layer connectivity, mobile network infrastructure was essentially a closed environment. However, with the evolution of network infrastructure towards an IP based architecture, networks have become much more accessible and hackers' interest has surged.

The evolution enables much more accessibility which improves network manageability and introduces possibilities of launching new services for end users. However, along with this accessibility, the IP based networks have become subject of attention by various groups of fraudsters exploring the exploitation possibilities.

Motivation behind attacks

Information is one of the most valuable assets in the modern world. Gaining access to personal subscriber information and using it rightfully can be incredibly valuable in certain contexts and very risky in others. This is the primary motivation behind armies of hackers who continually develop exploits for computers and mobile devices. They are looking for novel ways to get into the secure networks and gain access to information.

Mobile networks are no exception. While mobile handsets are generally secure when used carefully, the network itself is a treasure trove for attackers and an obvious target for exploitation. With proper access, information may be gained on the subscriber's identity or location, voice calls or texts may be blocked, intercepted or eavesdropped, funds requested to be transferred between accounts, billing systems bypassed or even network level denial of service attacks launched.

One may ask about the rationale behind Denial of Service attacks. In the IT space, the intention is to bring down a service or a web-site. In the network signaling world, the intended result may very well be temporarily eliminating communications in a specific geographical area which would severely impact law enforcement, public services or key high value targets in the area.

Another aspect of Denial of Service attacks is related to end-users. In these cases, targeted mobile subscribers can become victims while not even noticing that certain services on their handsets are not functioning.

Mobile network security: Signaling network vulnerabilities and protection strategies

As a result it becomes obvious that gaining access to the signaling network does justify the effort and investment for an attacker to be able to gain information on locations, conversations and messaging data exchanges.

Publicity/The press

During the last days of 2014, at the Chaos Communication Congress, signaling network attack vectors where presented on how to gain location and track mobile users, launch denial of service attacks, perform eavesdropping, divert traffic, de-anonymize interactions and perform various types of network level fraud. The industry reaction was generally muted as network operators quietly evaluated the exposed vulnerabilities and their possible countermeasures.

Although the concerns of information security and privacy were made public back in 2013 currently known as Snowden effect, the latest major news development came in mid-August 2015 when the Australian TV news show '60 minutes' demonstrated the security issues showing German hackers working from Berlin intercepting and recording a mobile phone conversation between the reporter speaking from Germany to an Australian Senator. The segment went on demonstration that they were able to intercept and read the Senator's SMS' and geo-track the Senator as he travelled around the streets of his home suburb.

Since then, security in signaling networks has been hot news in practically all technology publications and even covered by main stream consumer news sources such as the BBC, Forbes, the Guardian and the Washington Post. The subject of network signaling security will go down as the defining topic of 2015 and will be the subject of intense scrutiny for mobile network operators in the coming years.

Mobile network security: Signaling network vulnerabilities and protection strategies

Anatomy of the signaling attacks

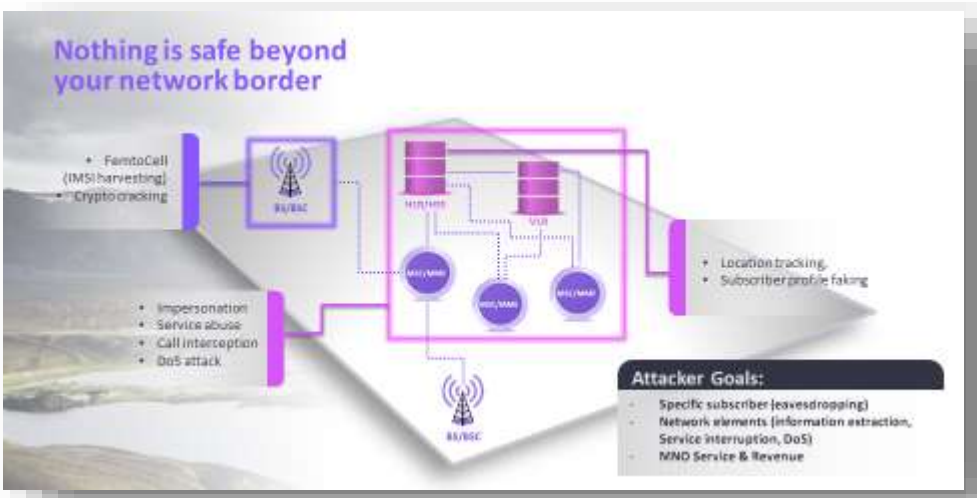
The primary focus of the design of signaling protocols (SS7, Diameter, SIP) is to provide high quality of service to mobile subscribers by enabling mobility and allowing service providers to enable different charging mechanisms and manage optional qualities of service.

For example the structure of SS7 protocol caters for addressing on multiple protocol levels. This protocol feature on one hand offers routing optimizations that take advantage of the high speed capabilities of differing network equipment while on the other hand is often misused by the attackers. Moreover, at the application layer the SS7 signals enable a defined level of service for mobile users such as roaming procedures, call setup, SMS messaging, data connectivity and other supplementary services. However, when signaling is misapplied or used in a wrong way, it can lead to unexpected outcome for either the signaling network equipment or for other mobile subscribers.

As example, one of the attacks that has been successfully demonstrated in several mobile networks is voice call interception using a fake charging system. The steps executed by the attacker are as follows:

1. Obtain unique subscriber identity called IMSI, which is used in other signaling operations. This number is not available on the mobile equipment and can be obtained from the mobile network only.
2. Identify the system that is currently serving targeted mobile user (MSC/VLR) and is holding subscriber profile. This profile might have an identification of the charging system.
3. Update subscriber profile in such a way that the charging system identification is modified pointing to the system belonging to the attacker
4. Through spoofing the charging system an attacker can redirect an incoming call to another platform
5. Redirected call can be looped back towards the attacked subscriber without the victim knowing that.

Mobile network security: Signaling network vulnerabilities and protection strategies



Multiple variants of this type of attack exist misusing the capabilities of the IN charging system to redirect the call or other actions. However this is not the only option to do that. All of these activities can be performed from outside of the network and may be categorized in three major steps:

a. Obtaining mobile subscriber identity
b. Using this identity and fake a portion of subscriber related operational data
c. Ensure that the service compromised can be used through an attacker system

Therefore the actual attack is actually contains of two actions (a, and b) that should be detected and prevented.

Mobile network security: Signaling network vulnerabilities and protection strategies

Industry approach to the protection

Mobile network security: Signaling network vulnerabilities and protection strategies

The majority of the mobile operators have reacted to the SS7 security issues in a straight-forward way supported by the network equipment vendors (NEPs), applying simple filtering policies on the edges of the network. These policies can be generally configured on the interconnect STPs by simply black-listing originating SCCP-layer addresses or limiting their access to certain services by means of blocking appropriate MAP operations. In such a way some of the subscriber phishing attempts (described in step (a) above) can be prevented. However this approach helps to prevent rudimentary IMSI phishing attempts, difficult to configure and maintain. One should also take into account that traditional equipment, where these filters are suggested to be defined, primarily is optimised for routing on the low level of SS7 protocol ensuring for the speed and stability of the service. Somewhat more advanced techniques have been applied by operators who have introduced Home Routing solutions for SMS. This has been triggered by the deficiency of filtering out IMSI requests from foreign SMSCs. However either of these approaches has been missing the major component, which is detection. Therefore a number of vendors have proposed complex big data solutions bundled with the network equipment that are intended to provide the operator insights on the incoming singling traffic. These solutions, although powerful in data analysis, still lack the capability of on-line prevention and incur the additional costs associated the big data framework.

Further on, as demonstrated in recent security conferences (Black Hat 2015 Europe), interconnect protection from IMSI harvesting does not provide a real solution. A simple femtocell approach can expose all subscribers in a given area and provide their data to an attacker.

Exposure of the IMSI information is not the primary venerability for a mobile user. The attack uses this identifier as a component in the faking step (stage (b) above) that truly makes the subscriber and the operator vulnerable. Therefore an effective signaling fraud prevention solution should include comprehensive attack detection and prevention instead of simple intermediate steps such as IMSI and location (VLR/MSC ID) harvesting prevention.

XURA Signaling Fraud Management solution

With more than 15 years of experiencing protecting signaling value added services such SMS, XURA signaling fraud management solution has been designed to detect and prevent all stages of the signaling attacks as well as providing the operator with detailed insight into the signaling network behaviour.

Mobile network security: Signaling network vulnerabilities and protection strategies

The Xura solution was developed taking best practices from the IP security world combined with our carrier grade components and experience in mobile networks. This unique combination enables us to deliver one of the most comprehensive signaling fraud management solution available on the market today. Unique signaling network integration experience and understanding of mobile network architecture enables us to deliver the product that naturally integrates into the mobile network ensuring reliable failover principles built into each signaling network design. This clearly distinguishes this product from the comparable attempts suggested by the security vendors originating from the IP world.

XURA Signaling Fraud management solution contains of two major elements: Signaling Firewall module and Analytics module working in conjunction with each other.

Signaling Firewall

This module integrates into the signaling network attaching to the interconnect STPs. It supports two integration modes: fully passive traffic monitoring enabled through the IP port mirroring on the IP equipment or active, attaching using SIGTRAN protocol to the STP allowing to block suspect traffic.

Mobile network security: Signaling network vulnerabilities and protection strategies

This module has high speed signaling stack processor that is tightly integrated with rule engine and correlation engine. These components allow to define screening policies, detect fake and spoof attempts through the correlation rules and adapt signaling primitives passing through the system. Real-time visual configuration capability enables mobile operators for a quick reaction to the new threats. When attached to all interconnect signaling transfer points, the system can also off-load existing traffic screening rules centralising their management what can significantly reduce TCO for the signaling transport network of mobile operator.

Analytics & Monitoring module

This module provides detailed analysis and real-time insight for the mobile operator on the detected threats, rules violated, blocked traffic, attack sources and attack targets. Advanced search and query capabilities enable operator in a user friendly manner to generate any kind of report required either to identify new threats or their sources matching security team KPIs.

We are Xura

We offer our customers a pathway to next generation digital technology. Our thinking unlocks the possibilities of no boundaries communications.

For over 20 years, we have been working with Communications Service Providers (CSPs), operators and enterprises all over the world, helping them to meet the needs of tomorrow's multi-device, multi-services consumers.

We offer clever ways to financially realize opportunities from existing technology, while guiding customers to richer communications solutions by creating innovative products and services to disrupt digital.

We help 8 out of the top 10 global operators reach over 3 billion endpoints.

We are the enabler making the future of digital communications services happen.

Xura. We think beyond.

For more information
Please visit our website xura.com
or email contactxura@xura.com