FIGHTING FRAUD ON 4G

Neutralising threats in the LTE ecosystem
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>New and Old Vulnerabilities</td>
<td>4</td>
</tr>
<tr>
<td>Identity Management</td>
<td>5</td>
</tr>
<tr>
<td>A Unified Response</td>
<td>6</td>
</tr>
<tr>
<td>Data Mining</td>
<td>7</td>
</tr>
<tr>
<td>An Evolving Challenge</td>
<td>8</td>
</tr>
</tbody>
</table>
LTE adoption is creating new opportunities for criminals to carry out network attacks and commit fraud.

Crime directed against 2G and 3G subscribers and networks – like SIM box, premium rate, IRSF, roaming and dealer fraud – are now being compounded by new types of attacks on next generation services. Crimes like VoIP fraud, viruses and phishing attacks, as well as DDoS and identity theft, are exploiting 4G vulnerabilities.

Much of this new threat is coming to the wireless world from the realm of fixed broadband. The spread of 4G mobile services, and demand for smartphones and tablets, has brought the positive side of the fixed broadband experience to mobile subscribers, along with its security issues.

The LTE environment is convergent by design, increasing the potential for fraud and network attacks to mirror that convergence. It makes sense to look at this new generation of wireless threats from an integrated perspective, encompassing traditional voice fraud as well as malware, intrusions and DDoS attacks.

The arrival of LTE has moved the wireless communications market on from its traditional voice orientation towards a data-oriented environment. The use of soft switching has reduced network complexity while increasing its complexity as an IT platform, with new security vulnerabilities.

LTE also introduces new complexity into the BSS/OSS environment. It introduces new approaches to charging, policy control and policy enforcement functions, as well as new network elements. This creates a need for multiple fraud protection and network security system integration points.

There is new complexity in the fight against fraud and network security but at the same time LTE offers new benefits, including an improved radio interface, a flatter all-IP architecture and the potential to exercise more control over subscriber quality of experience (QoE). The challenges have evolved with new vulnerabilities to network attacks, originating from the nature of the network environment.
NEW AND OLD VULNERABILITIES

In general, fraud attacks and network service abuse result from poorly protected services, so logically if a service is well protected it loses its appeal from the perspective of a hacker or fraudster. This means that a combination of systemised detection and protection, together with best practises must take equal account of both traditional fraud and new security protection measures.

New vulnerabilities include a growing trend towards malware attacks on smartphones and tablet devices. Mobile apps represent a source of such attacks. Infected applications, rather than browser-based downloads, are likely to be the main source of problems. Unauthorized app stores, which may not be monitored properly, are likely to be a common source of mobile malware.

Cybercriminals can post infected applications to less well policed app stores, and attempt to lure trusting users into downloading rogue applications. Cybercriminals can also find ways to get their applications posted into authorized app stores. If the Smartphone is also used for work purposes, then infections can easily spread beyond the smartphone and onto a corporate network. With LTE, it is easier to target mobile app users, given the diversity of applications making use of LTE services.

The list of potential issues is not restricted to malware and identity. VoIP fraud, Wi-Fi offload authentication, phishing attacks, denial of service, M2M and m-commerce service attacks all represent new potential sources of revenue loss attributable to security breaches and fraud attacks. Network optimization and security solutions need to address exponential increases in IP traffic, methods of access, types of activity and volume of content generated. Specifically, VoIP fraud and IP signalling attacks require operators to be investing in Diameter and SIP firewalls.
IDENTITY MANAGEMENT

A fraudster can, for example, create multiple calls without those calls being associated with individual identities, resulting in call inflation. In 2.5G and 3G networks, the bearer channels and the services are integral, whereas in an all-IP/IP Multimedia Subsystem (IMS) environment these are separated so the data bearer will be distinct from the services using it. Fraud and security risks can come from the fact that multiple bearer layers are required for control and monitoring systems in order to provision and manage services.

In LTE, different bearer identities will be used for one service. For example, a customer using Wi-Fi, GSM and wireline services will have different identities for different bearers. Some bearers will be operational at the same time, all of which exposes vulnerabilities and opportunities for fraudulent activities to occur.

The underlying architecture for LTE services is the IMS. Identity management becomes an issue in this architecture, with different ‘identities’ used at different layers in the network model. With a variety of information coming from different layers in the system architecture, there is a need for multi-layer data correlation and new techniques to enable accurate multi-layer identity management.

The IMSI and MSISDN identifiers used in 2G and 3G networks do not necessarily apply to IMS, which introduces the concept of private and public user identities, as follows:

**Private User ID** – A unique and permanently allocated global identity, assigned by the home network operator (equivalent to an IMSI). If a device contains an IMS Subscriber Identity Module (ISIM) then the Private User ID is used to identify a user to the network. So IMSI is not used at all under these circumstances. If a device doesn’t contain ISIM, then a Private User ID is created using the IMSI. This means that the IMSI can be derived from the Private User ID.

**Public User ID** – This identifier is used to communicate with other users (it is equivalent to the MSISDN).

It is possible to share a Public User ID across different phones (for example the case of a single phone number for an entire family), so it doesn’t uniquely identify a user, hence its limitation from a fraud or security management perspective.

IMS supports two types of identity - for the bearer and service layers, so different identities might be combined into one account. Additionally, there will be a number of other identities used internally in the network and many of the identities are dynamic and can change in session:

**Service ID:** IPMU, IPMI, SIP URI, Tel URI, E.164

**Bearer ID:** Account_ID, Radius_ID, IMSI, Terminal_ID, MSISDN, IMEI

There is a need to be able to reconcile these identities, and questions remain about how to create the linkage and also over where dynamic identities are going to be stored. This creates new issues for fraud detection and also for tracing malicious activity in the network.
So much concern over identity management would seem to dictate the need for a separate identity management
database and correlation engine. An option might be to define the fraud management system as the preferred location
for this. There might be also be a requirement to manage other forms of verification in the fraud management system, to
authenticate user identity. This is now a common feature in online commerce sites and search engines.

Under this approach, the fraud management system might perform some form of identity look-up capability, such that
customer IDs and third party interaction histories can be analysed, to establish association. This is useful, particularly when
dealing with organised crime.

With LTE expected to facilitate an increase in online transactions and commerce, using the fraud management system to
reference customer transactions with third parties, particularly with content providers, allows an expanded role for fraud
protection and security systems.

A UNIFIED RESPONSE

There is a need for more accurate knowledge about network security and related fraud potential in LTE. This should include
specifics about potential points of attack, an understanding about what information is available from key network points,
the necessary information correlation and the types of new detection techniques that are needed to stay one step ahead of
the fraudsters. Fraud protection and network security system touch points multiply with network elements, with in-house
IT security policies and systems and of course with third party partner systems.

Securing the network, detecting and preventing attacks requires a mapping of security and fraud system touch points, to
assure process integrity. These touch points typically include:

• **BSS/OSS** - provisioning, charging, billing, network, mediation, CRM, ERP
• **Network Elements** - SS7, IP flow, nodes, IP routers, Radius servers, Diameter signalling, border gateways
• **Security** - unified threat management, firewalls, web filtering, virus scanners, CA and key check servers
• **Third party partners** - external partners, third party networks, resellers and service providers

The advent of LTE services has multiple implications from a network security and fraud protection systems analysis
perspective.

There is a need to identify and map out security system and fraud management touch points as comprehensively as
possible. This means understanding the sort of information that needs to be located and retrieved, to be used for
correlation, reconciliation and analysis. With the potential for multiple events in each user session and multiple identities
associated with a single session, there is a need for very complex event correlation, with appropriate systems for Big Data
analysis.

LTE requires more effective security and fraud rules management. This does not just mean the definition and application
of rules, but also how to manage flexibility, thresholds and exceptions in a way that is appropriate for the LTE service
environment. Rules should also take usage context into account, to assist with more accurate user profiling as well as
helping to avoid potential false alarms.

LTE service deployment and the next generation service mix may result in evolving organizational structure. If this is the
case it is important to consider the way you want to protect your services, not just the tools themselves, to manage LTE
security, and also to be able to adapt to new approaches and new services.
DATA MINING

As with rules management, system flexibility is only one component of this and functions that enhance data analysis, automation and data visualization all help fraud and security analysts to manage significantly larger data volumes and pro-actively identify and resolve potential fraud issues and network threats.

With so much complexity to manage, does it make sense to invest in in-house tools at all? The availability of comprehensive managed security services and fraud protection hosted in the cloud provides new options for virtual and managed solutions or combinations of in-house and managed service options. A significant advantage of a third party managed approach is the 24-hour nature of the protection being provided, as well as removal of the need to try and keep up with new systems, new techniques and new technology updates.

The application of disciplines including context-based usage checking, user profiling, rules definition and management, machine learning and data analysis are continuously evolving. With LTE, from the security or fraud analyst perspective, there is an increasing need to be able to manage complex event correlation, involving data from multiple sources, including bearer/IMS session data; session/event analysis; content/merchant information; tracking of online payment streams and tracking of a variety of user identifiers.

The techniques associated with this sort of analysis moves security protection and fraud detection into the area of Big Data analytics, beyond the capability of existing relational database structures. New techniques including advanced data visualisation, are required to help determine and pro-actively identify complex patterns of security attacks and attempted fraud activity. More than ever in the fight to protect your network will be a requirement for speed of analysis and detection, as data sessions increasingly mean that higher value activities are occurring on the network, beyond simple voice traffic activity.

From the perspective of a network operators’ security and fraud teams, there is a requirement for constant training and re-training in securing the network, a need to review task automation, in order to relieve excessive workloads and the need to ensure effective workflow management and division of tasks across the team, separating analysis and detection on the one hand from post-detection case management for example.
AN EVOLVING CHALLENGE

Security attacks and attempted fraud activity are evolving problems which don’t stay still for long. With the arrival of LTE, new opportunities present themselves for criminals to attack and breach the communications network, in order to disrupt services and profit from potential vulnerabilities in LTE architecture.

A new world of cyber-crime, previously the domain of the fixed broadband environment is making its way into the wireless communications environment and with the rise of demand for smartphones and tablet devices and the services these devices support, the wireless communications network is taking on more of the characteristics of the fixed broadband world. It is hardly surprising that security breaches and methods of fraud associated more with the broadband enabled web environment are being introduced into the world of wireless communications.

As the wireless communications industry adopts LTE and moves from a voice-centric towards a data-centric focus, then the nature of the value of transactions also changes, thus presenting even more incentive for criminals and hackers to attack higher value services and m-commerce transactions. All of this requires a disciplined response towards network security and fraud detection, to ensure that analysis can be performed quickly and accurately on the relevant data, to minimize risk and make the LTE wireless network a less attractive target for criminals.

For more information, visit us at www.tatacommunications.com