Securing Mobile Targets

While 4G and LTE networks deliver unprecedented bandwidth and performance, they lack the inherent security of previous-generation networks. Below, John Vestberg, CEO of Clavister shows how operators can secure their LTE networks, and protect subscribers' data.

Next generation 4G and LTE (fourth generation and long term evolution) mobile networks have rung changes for European businesses. These new superfast mobile broadband networks are allowing organizations to deploy more bandwidth-hungry applications that make business on the move entirely possible using a handheld device. Mobile Network Operators (MNOs) also benefit from being able to offer new, revenue-generating services.

But with the increased performance that next-generation networks bring, there has been a trade-off in security. Unlike previous-generation mobile networks – the 2G and 3G services that a majority of people and businesses still use – 4G and LTE architectures do not have built-in security to protect the network or subscribers' voice calls, texts or data.

The majority of current 2G and 3G services provide inbuilt encryption of voice and data from the subscriber's handset, right through to the core mobile network. But in LTE networks, while traffic may be encrypted from the mobile device to the cell site, the link from the cell site into the core of the mobile network is unencrypted, leaving the traffic (and the network itself) vulnerable to interception and attack.

Small Cells, Big Security Problems

This security problem is compounded by the rapid, widespread deployment of microcell base stations that provide extra call and data capacity in public spaces, such as shopping centres and shared office complexes. The analyst Heavy Reading expects that the global number of cellular sites will grow by around 50% by the end of 2015, to approximately 4 million. Many of these new sites will be micro- and small cells, driven by the demand to deliver extra bandwidth to subscribers at lower cost.

Why is this? Simply put, mobile operators are facing a data crunch. Sales of bandwidth-hungry mobile broadband devices continue to rise, and the smartphone has become as much of a business tool as it is a personal device. For example, users are able to take photos and videos and upload the content instantly to social networking sites or the corporate network. This, combined with consumer-led, all-you-can-eat data tariffs mean that there is increasing congestion on networks.

So these small base stations are placed in publicly-accessible areas, where bandwidth is needed most. But these stations typically have only a minimum of physical security when compared to conventional base station sites, which are in remote locations, often with perimeter security and tamper-proof containers. This creates the risk of malicious parties tampering with small cell sites to try and exploit the LTE mobile network, to probe for weaknesses from which to gain access and launch attacks on the mobile core network. These attacks could involve access to end-user data traffic, denial-of-service on the mobile network, and more. Furthermore, mounting attacks is made easier because 4G and LTE networks use Internet Protocol (IP), the basis for the public Internet – so proven, established attack techniques can be transferred relatively easily from the 'net to next-generation mobile networks.

Also, mobile operators are looking to expand their networks with the lowest overall cost of deployment and ownership. This can mean sharing cell sites and network links with other operators, which can also impact on security: after all, who should take ownership of ensuring the shared network resources are secure?

So with operators starting to experience pressure to deliver strong security for subscribers' data – because of competitive pressure from rivals, and the need to assure both current and future customers that their mobile traffic is fully protected against interception and theft – how should they protect their networks against security risks, to protect their reputation and their revenues?

"Mobile operators are looking to expand their networks with the lowest overall cost of deployment and ownership. This can mean sharing cell sites and network links with other operators, which can also impact on security."

Scalable Security

The 3rd Generation Partnership Project (3GPP) which sets standards for mobile networks, has made recommendations on security for LTE networks. However, there are concerns about the deployment of those security solutions, based on factors such as the operator's market position and customer profile; the cost and complexities of deployment; and how the security solutions deployed might impact on overall network performance.

Network operators need to be confident that their security deployments are highly scalable, and offer high availability to cater for the expected explosive growth in LTE traffic and bandwidth demands. This in turn means using security solutions that offer true carrier-grade throughput capabilities as well as compliance with 3GPP standards, while being flexible enough to adapt to the operator's needs, and competitive pressures, as these evolve. At the same time, the solution should be as cost-effective as possible, to minimise impact on budgets.

To address these concerns, the mobile network security solution should run virtualized, on commercial off-the-shelf computing platforms. This avoids the costs and complexity of installing new hardware, while also enabling rapid deployment and easier management. A virtualized solution also gives excellent scalability to support operators' future requirements.

Using a flexible security platform that offers advanced encryption and authentication capabilities, and supports other advanced security applications, MNOs can protect their subscribers' data and the network core against the risks of interception and attack, and easily manage the security deployment. This in turn helps them to secure their subscribers' loyalty and ongoing revenues, while giving the best possible experience to users, where all they have to do is enjoy the bandwidth.

More From Clavister

For more though leader articles and information about Clavister products, visit **www.clavister.com**.

About Clavister
Clavister is a leading security provider for fixed, mobile and virtual network environments. Its award-winning solutions give enterprises, cloud service providers and telecoms operators the highest levels of protection against current and new threats, with unmatched reliability. Clavister's performance in the security sector was recognized with the 2012 Product Quality Leadership Award from Frost & Sullivan. The company was founded in Sweden in 1997, with its solutions available globally through its network of channel partners. To learn more, visit www.clavister.com.

Where to Buy
www.clavister.com/partners

Contact
www.clavister.com/contact

CLAVISTER®
WE ARE NETWORK SECURITY

Clavister AB, Sjögatan 6 J, SE-891 60 Örnsköldsvik, Sweden
Phone: +46 (0)660 29 92 00 | Fax: +46 (0)660 122 50 | Web: www.clavister.com