Have you evaluated potential risks before VoLTE launch?

15 November, 2016 at 11:15 AM Posted by: VanillaPlus

New security threats call for a security validation process

Is your organisation up-to-date with the new threat landscape of all-IP networks? Are you aware of the trend in the increase of sophistication of attacks and the counter measures and tools available? Have you evaluated your current threat situation? Have you considered that 4G & VoLTE will also expose your network to new threats due to interconnect, national or international roaming and IoT?

Three years ago, Blue Telecom Consulting (BlueTC®) partnered and started working closely with NextGen Inc., a leading network security vendor in Japan and a pioneer in offering IMS and Voice over IP (VoIP) solutions to telecom operators. As its Service Partner in Europe we have become leaders in the telecom network security area and have held numerous meetings with operators throughout the region. Currently we are capitalizing on this experience by contributing to an industry level initiative that intends to provide a common set of guidelines in this complex area.

Network nodes can have their own vulnerabilities

The fraud aspects of Voice over LTE (VoLTE) Voice over Wi-Fi (VoWiFi) have been highlighted at numerous industry conferences and in telecoms media, but with less attention paid to potential risks against the IMS Core (IP Multimedia Subsystem). The latter, if targeted *and not being properly secured,* could impact the service and cause interruptions or performance degradations. Even if operators have gone to great lengths to secure their networks thoroughly, we have entered a new era where new applications and advanced services are running on their mobile networks and systems. Thus, BlueTC recommends that the full range of security aspects is dealt with in-depth and in a comprehensive way by operators. This implies taking a holistic view and having IT security professionals work side by side with telecom security professionals, and avoiding silo thinking.


Miguel Angel Garcia Matatoros

Also, due to the transition from circuit switched to all-IP networks, we believe mobile operators are facing new and different types of security risks and vulnerabilities for which common solutions like Session Border Controllers (SBCs) and its security functions might not be fully sufficient. The SBC protects the edge of the networks and is resistant to many types of security threats, but by definition the SBC itself is a network node, so it cannot know and monitor its own vulnerabilities, like misconfigurations.

Top management must take ownership

In the course of many customer meetings, we have observed that some operators have still to realise and also recognise that additional security processes and validations could be required. These processes need clear ownership and accountability within the operator organisation.

The Chief Security Officer (CSO) and security department need to ensure that best practice is considered from the design through to the operational phase. The added value of performing security validations upfront is that simulations of various kinds of attacks will reveal potential risks, which is necessary in order to know the level of protection a system really holds.

This means the products and services need to have this built into any deployment schedule already in the planning phase. Early, preventive measures like testing in labs are normally more cost effective than to discover issues during launch phase or in full production with growing volumes.

If this has not been addressed within your company, there is a risk that you are unaware of unidentified threats that your network is exposed to, which could have unintended and unforeseeable consequences.

External security validations

Best practice normally requires engaging specialist, third party consultant organisations that can bring in their expert knowledge, methodologies and tools. To start with, it is imperative to have an updated threat library with an extensive number of theoretical and known threat cases. We also recommend that IMS/VoLTE security validations are performed against such a library.

The ideal validation service should be both time and cost efficient. For security reasons, the validation process must be carried out against a lab configuration which should mirror production. Therefore, reserving time for planning and lab testing is essential. The upside being that for the aggressive, stress testing protocols the lab only needs to be isolated and dedicated for a very limited number of hours.

Apart from having access to up-to-date threat libraries, the most important value to the operator of an external validation service lies in the expert analysis of the results. Interim results will normally be reported daily while conclusions and recommendations for countermeasures are thoroughly prepared in a final report. The threats are classified by severity using the Common Vulnerability Scoring (CVS) system that gives a good overview and permits handling the most pressing issues first.

Such a process provides the management of the operator organisation and the CSO with a powerful, repeatable and tangible framework for understanding the threat and risk landscape of the network.

As the threat landscape changes over time, operator organisations will need to review and revalidate their system configurations, etc. as a continuous improvement process.

An advanced monitoring system for attack prediction