

Codenomicon whitepaper:

Unknown Vulnerability Management for Telecommunications

- Anna-Maija Juuso and Ari Takanen -



Unknown Vulnerability Management (UVM) tools such as fuzzing enable operators to proactively eliminate unknown vulnerabilities. Complexity of 3G/4G-LTE networks, legacy technologies and Triple-Play services make security and reliability the number one priority. Being proactive also allows operators more control over their integration and deployment processes and reduces reactive operational costs.

CODENOMICON Ltd. | info@codenomicon.com | www.codenomicon.com

Tutkijantie 4E | FIN-90590 OULU | FINLAND | +358 424 7431
10670 North Tantau Avenue | Cupertino, CA 95014 | UNITED STATES | +1 408 252 4000

1 Telecom Threat Landscape

Telecommunication networks used to be very hard to attack, but the introduction of all-IP Next Generation Networks (NGNs) and new more powerful access technologies open the previously closed Telco networks to the risks of the internet. The transition from the matured IPv4 to the new standard, IPv6, only increases this risk. Together with other new technologies, like IPTV and VoIP, it increases the likelihood of new and unique vulnerabilities in software. These unknown vulnerabilities expose Telecom networks and services to security, quality and robustness issues, reducing their operational reliability.

2 Software Minefield: Unknown Vulnerabilities

Vulnerabilities are unpatched software flaws. Without vulnerabilities there would not be attacks, because hackers need to find vulnerabilities in a system, in order to devise an attack against it. However, vulnerabilities can also be triggered by simple unexpected inputs in events like heavier than normal use or system maintenance. Unknown vulnerabilities differ from known vulnerabilities in that their existence is unknown, thus there are no ready patches and updates and attacks against them can go unnoticed.

3 Catching Unknown Vulnerabilities

Traditional security solutions, like heuristics and signature based analysis, cannot catch unknown vulnerabilities, because they focus on scanning for known bugs or variations of them. The best way to discover unknown vulnerabilities is Fuzzing, a form of attack simulation, in which vulnerabilities are triggered with abnormal inputs. Fuzzing is also the core technology behind Codenomicon's UVM process, which helps organizations discover unknown vulnerabilities, before they are publicly exposed.

Model-based Fuzzing

The most thorough and systemic way to test software is model based stateful Fuzzing. Model-based fuzzers use protocol specifications to target tests at protocol areas most susceptible to vulnerabilities, thus reducing the amount test cases without compromising test coverage. They can genuinely interoperate with the tested devices or system, thus they can find more hard-to-reach vulnerabilities and test interoperability.

Traffic Capture Fuzzing

With new technologies the specifications needed to create model based tests are not always available. In such cases, traffic captures can be used to create fuzzers. These fuzzers are quick to create and execute. However, they only cover a limited selection of the implementation. But, traffic capture fuzzers can find problems earlier, when they are easier and cheaper to fix them.

4 Threats from NGN

Next Generation Networks introduce a number of new IP-based technologies. New technologies and proprietary code extensions are frequently infested with unknown vulnerabilities, but being IP-based creates additional security problems. For example, Voice over IP (VoIP) introduces previously inconceivable Denial of Service (DoS) attacks into telecom networks.

Threats from Complexity

The complexity of the new technologies also increases the probability of vulnerabilities. For example, with Triple play and IP Multimedia Subsystem (IMS), the various interfaces, players, protocols and applications are source of such complexity that it already has significant security implications. With such complex technologies vulnerability management is also necessary from an interoperability point-of view.

Improve Quality of Service

Vulnerabilities also affect the Quality of Service (QoS), this is particularly challenging for new IP technologies, like VoIP and Internet Protocol TV (IPTV), which are replacing traditional voice and broadcasting services. Users are used to the high quality transmission of the traditional telecom networks and television broadcasts, thus both VoIP calls and television programs transmitted over an IP network are highly sensitive to packet loss and jitter. If the QoS is not satisfactory, the customers are quick to change the channel, or even the service provider.

Immature IPv6

Additional security, quality and interoperability challenges are created by the transition from IPv4 to IPv6. Industry experts are estimating the remaining IPv4 addresses to run out by early 2011, forcing transition into IPv6. It has taken it a long time to mature into a stable foundation for the Internet, yet people are still reporting critical bugs in IPv4 stacks. It took IPv4 30 years to mature to its current level. Yet, we are expecting IPv6 to be more reliable, more robust and more secure than IPv4 has ever been.

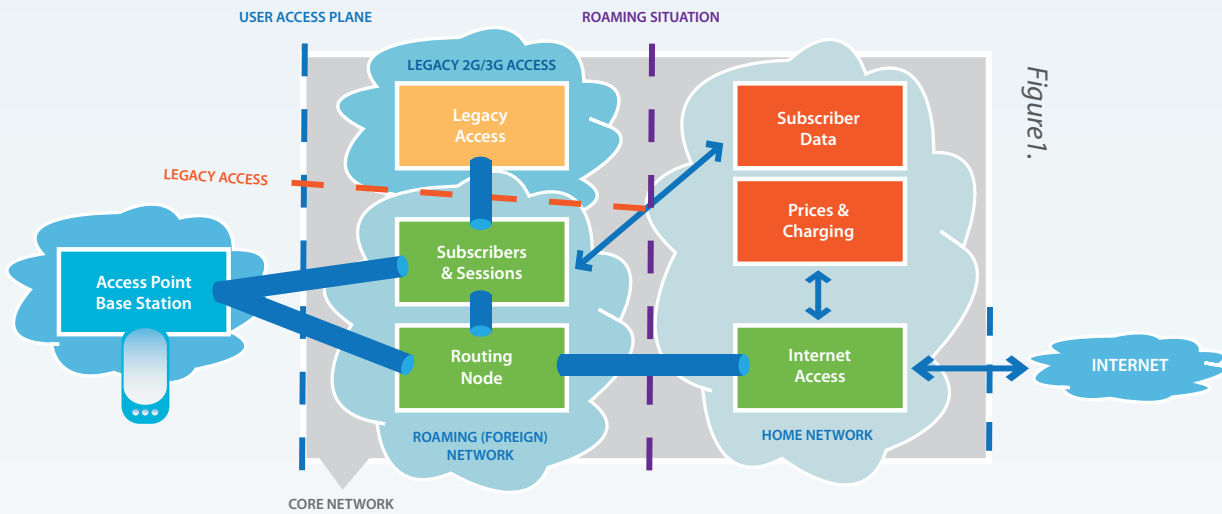


Figure 1.

5 Attack Vectors in All-IP Telecoms

All-IP networks contain fewer network elements than traditional 2G/3G networks, but even though the network core itself is simpler, the technical changes create a number of critical interfaces, as shown in Figure 1.

Roaming Problems

Roaming situations create a trust boundary between these two carriers within their core networks. Before a user is able to access any services in a foreign roaming network, the foreign access network has to talk to home routing, which then calls the home billing system. Until now operators have used their own backbone connections between each other. But with the arrival of all-IP networks, this transaction will also take place over the Internet meaning that even more robustness is required from network equipment involved in roaming scenarios.

Legacy Burden

Legacy technologies contain rarely used features, which are not subjected to rigorous everyday use and, thus, probably contain unknown vulnerabilities. These vulnerabilities can be exploited by hackers or they can affect the operability of the network. Faulty legacy equipment, for example, in a roaming partner's network, can send invalid data, which in turn triggers vulnerabilities in the operators own network.

Wireless Threats

An important difference between Next Generation and legacy networks is the amount of control given to modern access

point base stations, such as FemtoCells and Home eNodeBs. Traditionally, these base stations have had limited functionality, but with NGN some logic, like transmission, are handled on new access point base stations. This will achieve shorter response times, but, at the same time, it enables easier outside access into the carrier's core network. New types of home routers also allow users to program the handset radio features.

Threats from Users and Internet

The most critical interfaces in all IP networks are the interface between user access plane and the core network, and the interface between the core network and the Internet. These are the two interfaces carriers with least control. The problem in the off-site connections is not the wireless connection in itself, but potential vulnerabilities in the higher level protocols. In particular IPv4 and IPv6, because they can directly access components in the operator's core network. As an entry vector, the IP layer is visible to most users. It is also the easiest one to attack, due to the large number of ready tools used for Internet hacking.

6 Unknown Vulnerability Management for Telecommunications

The Codenomicon Unknown Vulnerability Management Lifecycle is a security and quality assurance process. The aim of the process is to ensure the security, quality and interoperability of both in-house and third party software productions by finding and fixing unknown vulnerabilities. Through Unknown Vulnerabilities Management operators

can anticipate future challenges and gain more control over their systems and devices. The process consists of four phases: Analyze, Test, Report and Mitigate, as shown in Figure 2.



Figure 2.

ANALYZE

Analyze real network traffic and reveal vulnerable interfaces in enterprise and core networks. Networks nowadays are a mixture of applications and components from various suppliers; nobody has an overall picture of the tested system.

TEST

Test the protocol implementation in the vulnerable interfaces to discover critical vulnerabilities. Codenomicon's Defensics Fuzzers allow you to run multiple test suites simultaneously and discover both known and previously unknown vulnerabilities with unparalleled efficiency.

REPORT

Codenomicon test suites generate different reports for different audiences from high-level managerial overviews to detailed technical reports augmented with PCAP traffic recordings for easy technical analysis of individual tests. Remediation Packages can be used sent test case data to third parties for automated reproduction.

MITIGATE

Codenomicon Defensics report contain CVSS and CWE values, which help testers decide what should be fixed first, and direct links to help reproduce vulnerabilities and verify patches. The test case documentation can be used to create tailored IDS rules to block possible zero-day attacks.

COLLABORATE

Manage tests carried out in multiple locations, process test results and coordinate the repair process in the Collab environment. The Codenomicon Collab enables users to remotely access the same system, thus they can execute the same tests, share results and other documentation, and reproduce the same vulnerabilities.

SERVICES

Codenomicon also provides a number of security services ranging from creating custom tools to trial tests and coordinating the process of fixing the found vulnerabilities.

7 USE CASE: Using UVM to Select Vendors

A major US operator uses fuzz tests as acceptance criteria for selecting vendors. In their tests, they have found significant differences in security and robustness between different vendor equipment. The operator in question performs the tests itself. This is possible, because Defensics is a black-box testing method. Defensics can also be used to outsource testing to suppliers. Often enterprises have no visibility over the tests done by vendors. Codenomicon's collaboration environment allows operators and vendors to share test case environments and documentation. Regardless of who does the testing, the vulnerabilities can be easily reproduced by the vendor.

8 Conclusion

The deployment of new technologies always involves a high risk of unpredictable security, quality and interoperability issues. The source of this unpredictability is unknown vulnerabilities in the software. Codenomicon's Unknown Vulnerability Management Tools help operators to gain more control over the deployment process and avoid any undesirable shortcomings that might affect the customer experience. Codenomicon's customers have already got good results from testing third party developments, before integration, but even better results could be achieved by insisting that vendors utilize Codenomicon tools during development. The earlier software is fuzzed the cheaper and easier it is to fix it and the more thorough the fixes are.