

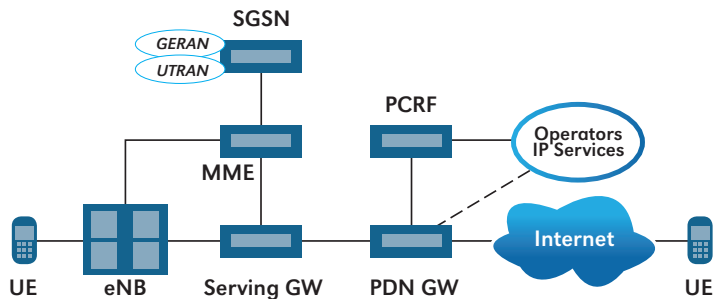
LTE

DEFENSICS for 4G

All new technologies are infested with reliability issues, and IMS, WiMAX and LTE are no different. This is due to increased complexity, fast release cycles and new technology that has not been thoroughly tested yet.

Originally, Fuzzing was introduced as a proactive tool for discovering zero-day security flaws. But especially in telecommunications, it has also been critical in finding and fixing any robustness issues including critical interoperability flaws. Fuzzing can be used in R&D, but also later in verification phase when deploying communication software. Fuzzing is efficient in finding problems in any environment. It has been used in testing of telecommunications network since 1999, with the launch of our WAP tests. Based on our experience, all communication systems will crash when tested with negative testing.

Codonomicon DEFENSICS testing solution is now addressing emerging 4G technologies, such as LTE, and helping customer to harden their systems before deployment.



DEFENSICS Advantage

Codenomicon DEFENSICS preemptive security and robustness testing solutions empower customers to mitigate unknown and published threats in products and services prior to release or deployment - before systems are exposed, outages occur and zero-day attacks strike.

Founded in 2001, the company was spun out of the successful PROTON test tools research of the Oulu University Secure Programming Group. Years later, the world-proven Codenomicon DEFENSICS platform remains unmatched in its ability to quickly find quality, resiliency and security flaws within the broadest array of applications. Thousands of developers and security analysts across telecommunications, networking, manufacturing, financial services and defense industries rely on Codenomicon to reduce costly reputation, quality and compliance risks.

Headquartered in Oulu, Finland, with offices in Silicon Valley and Hong Kong, the company markets its testing software and services directly and through international partners.

The Issue: Greater attack velocity, organized cybercrime, service disruptions and strict SLA agreements between the operator and customer have elevated the need for more extensive security and robustness assessment of devices, applications and systems. Security and quality testing at all levels has become a best practice. However, barriers towards developing and maintaining adequate testing methods that help customers stay ahead of the threat still persists in the market. This is due to:

- Flawed commercial, consumer and corporate applications
- Increased development and deployment release pressures
- Shortage of security resources and expertise
- Increased complexity of systems
- Unpredictable zero-day attacks, patches and
- Inherent fragility of new technologies

Codenomicon's objective is to ensure the security and robustness of any application or service implementation. Development and security personnel in a lab or staged environment use Codenomicon DEFENSICS to fortify quality and security assurance – quickly, easily and reliably. The test software offers a systematic blackbox and negative test methodology uniquely capable of revealing undesired behavior and issues in protocol implementations. Codenomicon teams its Protocol Modeling Engine and Attack Simulation Engine with the industry's broadest protocol support covering network, wireless, and digital media. Tens of thousands of pre-built, highly targeted and well-documented test cases allow users to start seeing results as soon as the platform is connected to the target system, accelerating time-to-value. In short, if a product or service under test passes DEFENSICS inspection – risk management and quality assurance is strong.

DEFENSICS for 4G

DEFENSICS for 4G provides unique value by offering support for core LTE protocols, such as GTPv1, GTPv2 and Diameter. Assuring the security and robustness of underlying IP layers, including Mobile IP, UDP and SCTP are supported. For an all-IP LTE network, Layer 3 tests that cover end-to-end connectivity are important: Network entry, authentication, call setup and security procedures have to be exhaustively tested. Significance of Layer 3 is underlined by the fact that it is the LTE entry vector visible to large amount of consumers. As such, non-compliant client devices and malicious hacking attempts are likely to be encountered.

DEFENSICS for LTE protocol summary:



The most important use scenarios to be tested involve User Access (UA) to LTE/EPC core and an interface between LTE/EPC and open Internet (PDN-GW testing to be more precise). In the User Access case, Serving Gateway (SG) and Mobility Management Entity (MME) are critical components to be tested. These components also play major role in roaming scenarios between operators, creating a trust boundary requiring a high level of robustness. An aspect over which operator has least control in an all-IP network is IP traffic originating from user equipment, and as such, robustness of IP packet handling should be thoroughly tested in an end-to-end configuration. Packet Data Network Gateway (PD-GW), together with the AAA servers create outer boundary of LTE/EPC facing Internet. PDN-GW is also part of the trust boundary in roaming scenarios. This requires high degree of robustness and reliability from these components.