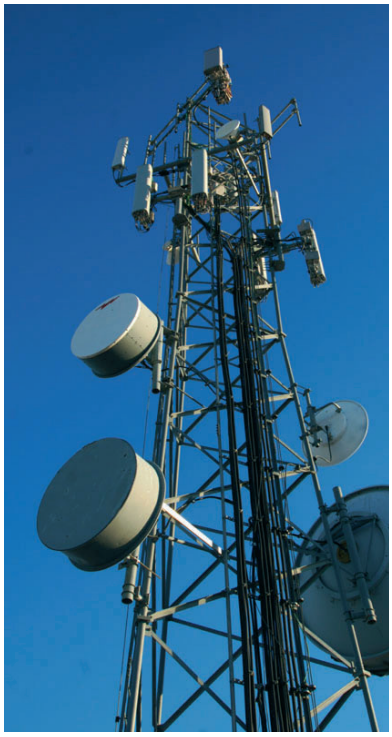

HIGHLIGHTS

- Test and audit your entire infrastructure including your Radio Access Network, (U)SIM, IP & Packet Core Domain, SS7 interconnections and CS Core, OSS/BSS and integrated IT systems.
- Receive attack model to illustrate where your business is at risk and what steps you should take to protect it.
- Gain visibility into mobile systems from Ericsson, Huawei, NSN, ALU and more.
- Gain insight from our experts who have carried out dozens of Mobile network audits and security assessments uncovering over 150 Telecom and IT 0-day vulnerabilities annually.

HOW MOBILE SECURITY ENSURES RELIABLE COMMUNICATIONS

Mobile operators typically consider accidents and natural phenomenon when trying to mitigate service disruption and plan their architecture and recovery strategies. But the convergence of traditional circuit-switched networks with broadband and packet-based Internet Protocol (IP) networks leaves mobile communications vulnerable to deliberate and malicious disruption from cyber-attack.

There are also many alternative ways to hack the network: hackers can carry out attacks on OSS/BSS systems, Internet facing web applications, SS7, transport and access networks to steal confidential data, provoke service interruptions or create a new line of attack.

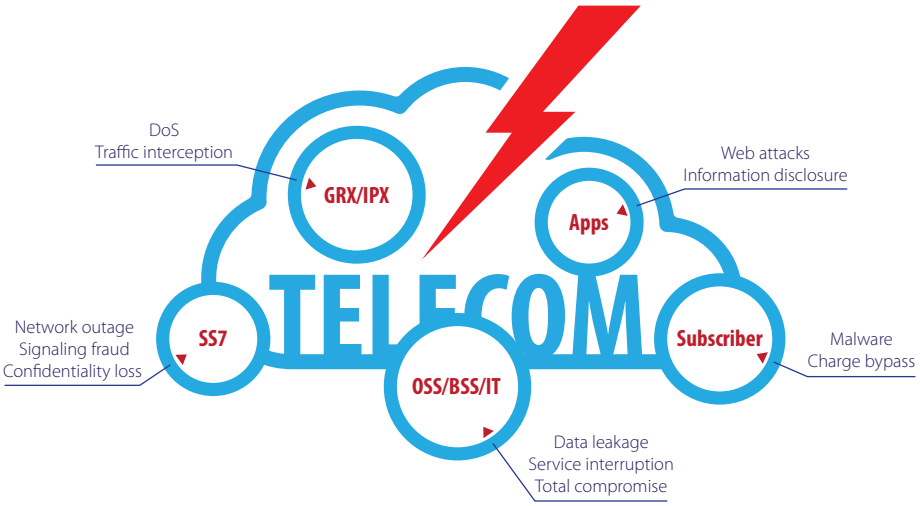

Diagram of Telecom Threat Vectors

It is important to consider what mobile operators need to do to ensure a secure experience for users. They need a robust and complete security strategy that protects their networks and services as an integrated whole.

A Comprehensive Security Approach

For over a decade, Positive Technologies has been conducting penetration testing, and vulnerability and compliance assessments for leading mobile operators around the world, giving unique insights into the practical challenges involved in securing mobile networks and services. Our experience tells us that a network provider must analyze the entire mobile network, with all its interconnections and components, to determine the best approach to protecting it.

VimpelCom

"VimpelCom depends heavily on the stability and safety of its Information Systems. That's why it is so important for us to have a common set of tools providing robust information security for all of our subdivisions. It's also important for us to have full control of security compliance for all our IT systems. MaxPatrol provides us with the complete solution to these challenges."

Dmitry Ustyuzhanin
Head of Information Security
VimpelCom

MEGAFON

"With Application Firewall we can now detect and track attacks as they happen. We can see what is going on with our web services and in case of an alert we can change the system configurations to improve our security levels."

Sergey Khimanych
Information Security Expert
MegaFon

du

"We found that MaxPatrol worked with more of our systems and produced better quality results than other solutions on the market. Not only did MaxPatrol find vulnerabilities in our network that others failed to find, it also gives us more detailed information on each weakness, letting us tackle issues more quickly."

Ahmad Hassan
Director of Risk Management and Compliance
du

Our industry-specific approach to mobile security includes:

- Security testing and vulnerability research on a range of telecom equipment including 3G/LTE modems and femto cells, and to HLR/STP/VAS including architecture analysis, fuzz testing and reverse engineering.
- SS7 vulnerability testing including MAP/CAP attack simulation, assessment of impact on CS Core (MSC/VLR/HLR/AuC) and analysis of possible fraud.
- (U)SIM security checks for weak encryption algorithms, exposure of encryption keys and signatures, and Java application vulnerabilities.
- Radio Access Network security testing (GSM, UMTS, LTE, WiMax and WiFi) including authentication, encryption, network isolation and firewall verification.
- Mobile application security testing and security analysis of both client- and server-side applications.
- Custom application security testing including OSS/Billing/CRM/ERP systems.
- External and internal penetration testing including technical and information security social engineering methods.
- Forensic investigation of security incidents.
- Security and compliance audits of IT and telecom networks

Our extensive knowledge of how to strengthen networks in the face of exposed weaknesses can help to avoid serious security issues. These issues include, but are not limited to, users bypassing service charges, fraudulent calls and SMS interception, leakage of subscriber database, and mobile network outage leading to huge financial and reputational damage.

Because attacks and malware can spread between interconnected networks, Positive Technologies also analyzes GRX, Internet and IT network connections.

Positive Technologies helps world leading mobile operators and telecom companies meet their security challenges head-on. With our hands-on experience assessing the latest communication technology, our deep understanding of mobile security and our 150-person strong researcher team, we are able create the latest innovation in the field. Positive Technologies is the ideal partner to help you secure your mobile networks and services and ensure reliable communications.

About Positive Technologies

Positive Technologies is a leading provider of vulnerability assessment, compliance management and threat analysis solutions to more than 1,000 global enterprise clients. Our solutions work seamlessly across your entire business: securing applications in development; assessing your network and application vulnerabilities; assuring compliance with regulatory requirements; and blocking real-time attacks. Our commitment to clients and research has earned Positive Technologies a reputation as one of the foremost authorities on SCADA, Banking, Telecom, Web Application and ERP security, and distinction as the #1 fastest growing Security and Vulnerability Management firm in 2012, as shown in an IDC report*. To learn more about Positive Technologies please visit www.ptsecurity.com.

*Source: IDC Worldwide Security and Vulnerability Management 2013-2017 Forecast and 2012 Vendor Shares, doc #242465, August 2013. Based on year-over-year revenue growth in 2012 for vendors with revenues of $20M+.

POSITIVE TECHNOLOGIES