POSITIVE TECHNOLOGIES

UNDERSTANDING CORE TELECOM SECURITY

If you think you're not affected, consider that a 2013 Congressional survey of more than 150 utility companies revealed more than a dozen utilities reported constant, daily, or frequent attempted cyber-attacks including phishing, malware infection and unfriendly probes, and at least one utility was the target of roughly 10,000 attempted cyber-attacks every month.

(Source: Homeland Security News Wire)

Positive Technologies recommends analyzing the whole core Telecom network, with all its interconnections and components, as the best approach to protecting it.

Reliable communications are essential to a nation's health, safety, economy and way of life. To assure availability, telecom operators have historically guarded against service interruptions by considering natural disasters and accidental disturbances as part of their architectures and recovery strategies. But now, due to the convergence of traditional circuit switched networks with broadband and packet-based Internet Protocol (IP) networks, it's imperative that operators consider additional security measures to protect themselves from deliberate and malicious disruptions and disasters resulting from cyber-attack.

A common theme in most cyber-attacks is exploiting vulnerabilities and misconfigured system settings, but where should your network defense begin? Some think that focusing on the signaling network (SS7/SIGTRAN) is best, although doing so leaves your customer management, transmission, switching, access, mobile and intelligent networks open to a wide array of attacks that can be carried out by even novice hackers. Yes, SS7/SIGTRAN is important, but a partial approach that ignores other vulnerabilities leaves opportunities for hackers to break in.

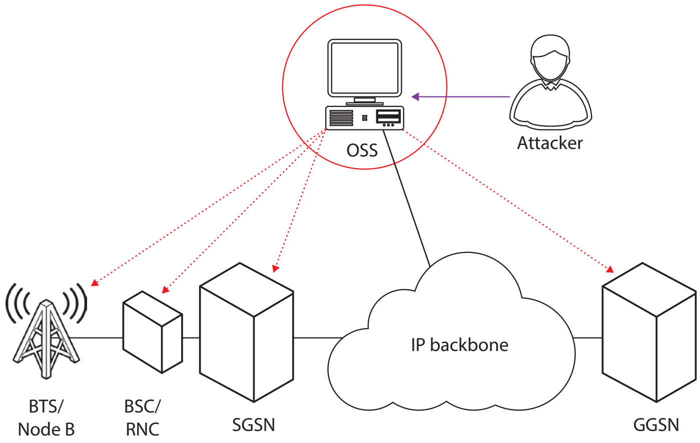

Figure 1: Connected systems are indirectly at risk

Control Your Entire Core

Forward thinking organizations understand that IT security cannot be effectively managed in isolation as separate segments or technologies, but rather it must be considered across all systems. Likewise, Positive Technologies recommends analyzing the whole core Telecom network, with all its interconnections and components, as the best approach to protecting it.

Positive Technologies is a trusted provider of Vulnerability Management (VM), Application Security (AS) and Critical Infrastructure Protection (CIP) solutions to more than 1,000 global enterprise clients. We help you protect your core telecom network from cyber criminals and other bad actors.

Positive Technologies performs an in-depth security assessment across all of your core network layers. We identify all of the cracks that a hacker could crawl through, create a real-world attack model that illustrates where your business is at risk and outline steps you should take to protect it.

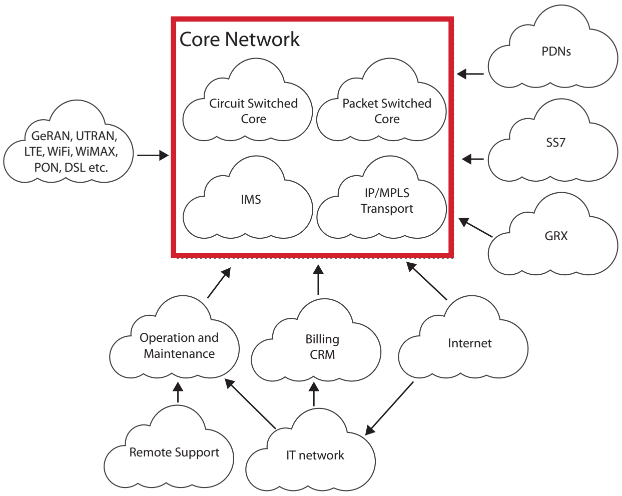

Figure 2: Typical mobile network topology

Our comprehensive approach to core network security for telecom providers includes:

Telecom

- Security Testing and Research on a range of telecom equipment from 3G/LTE modems and femto, pico and micro cells to HLR/STP/VAS, including architecture analysis, fuzz testing and reverse engineering
- Audit of IT and telecom networks for known and 0-day vulnerabilities and to assess security policies, processes and controls implemented
- Radio Access Path Security Testing for mobile and wireless communications standards GSM, UMTS, LTE, WiMax and WiFi, including authentication, encryption, fraud calls, flash SMS, HLR call request tests and GSMA security testing
- Penetration Tests to gauge resistance to network and data link layer attacks, execute traffic and log analysis, measure the effects of exploiting vulnerabilities and check the likelihood of unauthorized access
- GPRS, IP & Packet Core Domain Security Audits and GTP Testing
- SMS Service and Signaling Security:
    - USSD Service
    - Signaling Security Assessment (e.g., SS7, SIGTRAN, MAP, CAP, ISUP) and SS7 external information gathering
    - SS7/SIGTRAN Interconnection and Architecture Audits
    - Fraud Analysis
- Operational Management, OAM Interface Security Testing
- Core Network Services Provisioning Security:
    - Web/Vas/IN/ Femto, VoIP, etc.
    - Configuration Hardening Guides and Checklists developed for a wide range of core equipment

Because malware and bad actors can spread between interconnected networks, Positive Technologies also examines and analyzes GRX, UTRAN, LTE, DSL and Internet and IT network connections.

Uncover Your Core Weaknesses

The security specialists at Positive Technologies actively employ common and advanced attack techniques to provide a hacker's perspective on:

- Subscribers/From Subscribers/VAS/Backhaul: PON, FTTx, xDSL, WiFi and GPRS
- Circuit Switched Core Networks: HLR/AuC, VLR/MSC, STP and SMSC
- Packet Switched Core Networks: SGSN, GGSN and DNS
- Evolved Packet Core: PGW, HSS/PCRF and MME
- IMS, OSS, BSS, IP/MPLS and GRX/IPX

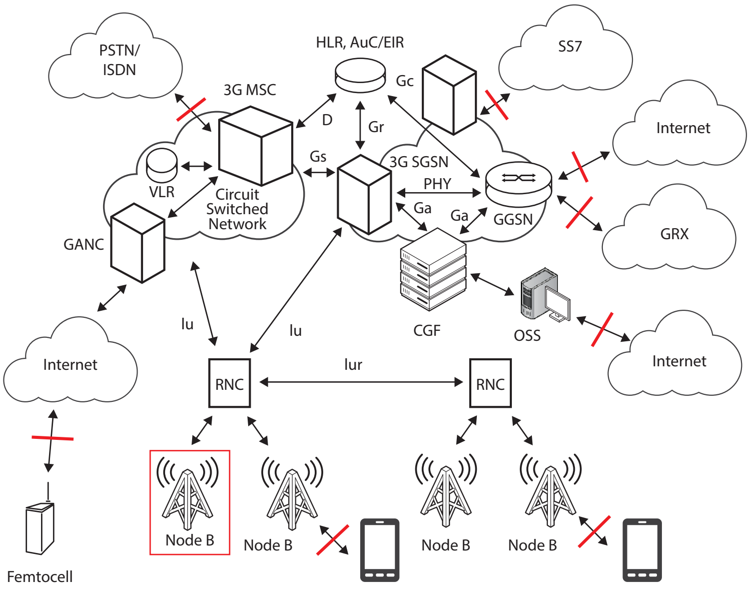

Figure 3: Many attack vector options

Our experts have demonstrated their deep and broad knowledge of core telecom security by successfully exposing hundreds of weaknesses including bypassing service charges, spoofing calls and SMS messages, unauthorized access to voicemail, call and user account interceptions, gaining access to OSS/BSS/HLR, compromising VAS/Web/self-service portals, acquiring confidential data (IMSI, IMEI) and substituting the subscriber profile in VLR, just to name a few.

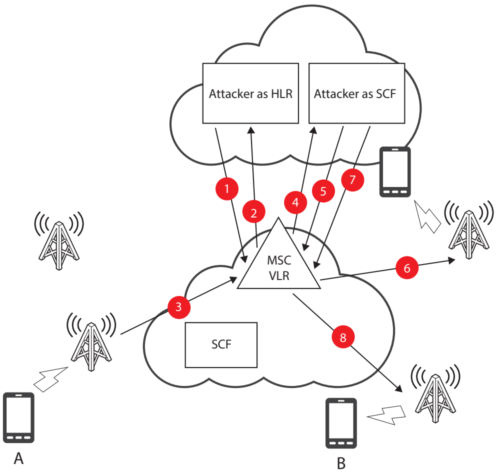

Figure 4: Example attack sequence

Gain Visibility Into Your Core Network

Positive Technologies has extensive hands-on experience analyzing equipment from leading telecom suppliers such as Broadcom, Cisco, Ericsson, F5, Huawei, Juniper and NSN, across a wide range of systems including:

- BTS/NODEB/BSC/RNC
- MSS(VLR)/MGW/HLR(AuC)/SGSN/GGSN/STP(SS7)
- SMSC/MMSC/USSD Gateway
- VAS IVRs
- IP Core elements and transport (routers, switches, FWs, DNSs)
- GRX/Internet/Core Network Charging Elements
- eNodeB/MME/S-GW/PDN-GW/P-GW/HSS/IMS

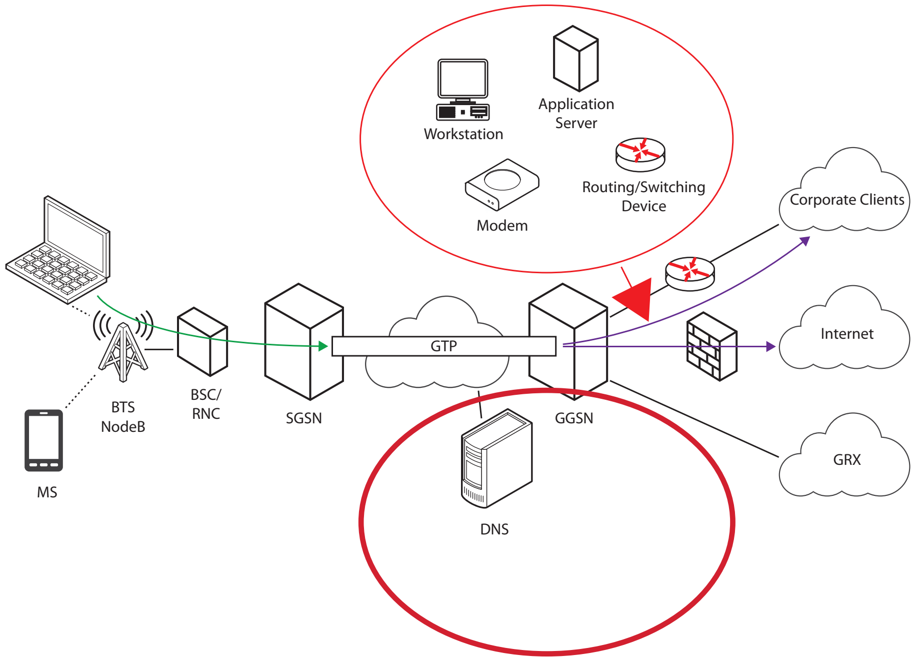

Figure 5: Visibility into actual systems on the network

Our insights provide telecom clients with crucial intelligence and visibility to see where their core network is locked down, where it has holes and what must be done to resolve vulnerabilities.

Translate Security Standards Into Action

Security and data privacy standards provide high-level guidance, but that's it. They lack any technical details that explain what should be monitored and checked to ensure security and compliance. Positive Technologies allows you to turn high-level guidelines into operational security controls through our deep understanding of digital security standards including:

- ISO 27001:2005, ISO 27002, ISO 27011:2008
- ITU-T X805, ITU-T X1051, ITU-T E408, ITU-T E409
- 3GPP 33-Series, 3GPP2 S.S0086 , ENISA Guidelines, DoT TRAI Regulations and others

Converge IT & Critical Infrastructure Protection

To keep your communications network secure and online, you must proactively identify vulnerabilities and potential attack vectors, assess and prioritize threats, and remediate weaknesses. But doing this across only your core telecom systems will not keep you safe. IT and core networks face complementary security risks that cannot be effectively managed in isolation. Rather, they must be viewed together as part of a unified enterprise security strategy.

Consequently, in addition to solutions for protecting your core telecom systems, Positive Technologies also provides powerful vulnerability management products and services aimed at traditional IT systems, including:

- External IP Networks Vulnerability Assessment and Penetration Testing (black-box methodology)
- Internal Network Vulnerability Assessment and Penetration Testing (white-box or gray-box methodology)

- Application Security Assessment (corporate website, self-service and provisioning portals, VAS, etc. (black-box, white-box, or gray-box methodologies and tools for dynamic and static code analysis)
- Vulnerability Research, Application, OS, Networks, DB, ERP Systems Analysis and the development of Configuration Hardening Guides
- SOC External Perimeter Continuous Monitoring Services
- Security Assessment and Compliance Automation in MaxPatrol http://www.ptsecurity.com/what_we_do/maxpatrol/

Why Choose Positive Technologies?

At Positive Technologies, our people are among the world's most advanced specialist researchers, renowned security experts and highly-skilled programmers.

With one of the largest and most dynamic research facilities in the world, Positive Technologies carries out research, penetration testing and threat and vulnerability analysis on dozens of large-scale networks every year. As a result, we discover over 100 Core Telecom and IT 0-day vulnerabilities annually and have earned our reputation as one of the foremost authorities on Telecom Security anywhere.

With our hands-on experience assessing real-world systems, our deep understanding of telecom security and our more than 150 researchers keeping you ahead of the bad guys, why wouldn't you choose Positive Technologies?

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

TELECOM_SB_A4.ENG.0011.01.DEC.29.2014