Telecom Sector Security Assessment Overview

The unprecedented growth of Telecom sector in emerging economies like Asia, Africa and South America has resulted in rapid expansion of the network, addition of value-added services, and resultant increase in complexity of the entire setup.

In the hurry to increase the market share through innovative network services, often security threats are ignored. However, cyber-criminals have begun to increasingly target telecom infrastructure, especially as it becomes IP-based with the arrival of LTE. Also, the increasing regulations towards telecom security have created quite a challenge that telecom companies are seeking to address.

Telecom Threats

Major threats to Telecom Security usually fall into the following categories:

- Phone Fraud -Toll Fraud, Cramming, Telemarketing fraud, War dialling and so on
- Theft - Data theft, network abuse, illegal data interception, unauthorized data modification (in billing or routing based processes)
- Malware - Viruses, trojan horse
- Spam - Sending Spam messages via SMS, MMS
- Denial of Service attacks - Request flooding, DoS attacks against network infrastructure.
- Data leakage - Penetrating billing and CRM systems to extract customer data

Types of Telecom Security Testing

⑩LTE Equipment security testing

⑩GSM Internet Data Access Penetration testing

⑩GPRS Internet Data Pen-testing

⑩SMS Spoofing and POC

⑩Lawful Interception System/Gateway Security Audits

⑩IVR Security Testing

⑩X.25 Security Audit

⑩SS7 Gateways & Process Security Review

⑩ Sigtran Security Assessment

⑩Diameter Security Assessment

⑩GRX Security Assessment

Types of Telecom Security Testing

⑩Signalling Firewall Rules Testing

⑩Air Interface Assessment

⑩IPTV Penetration Testing

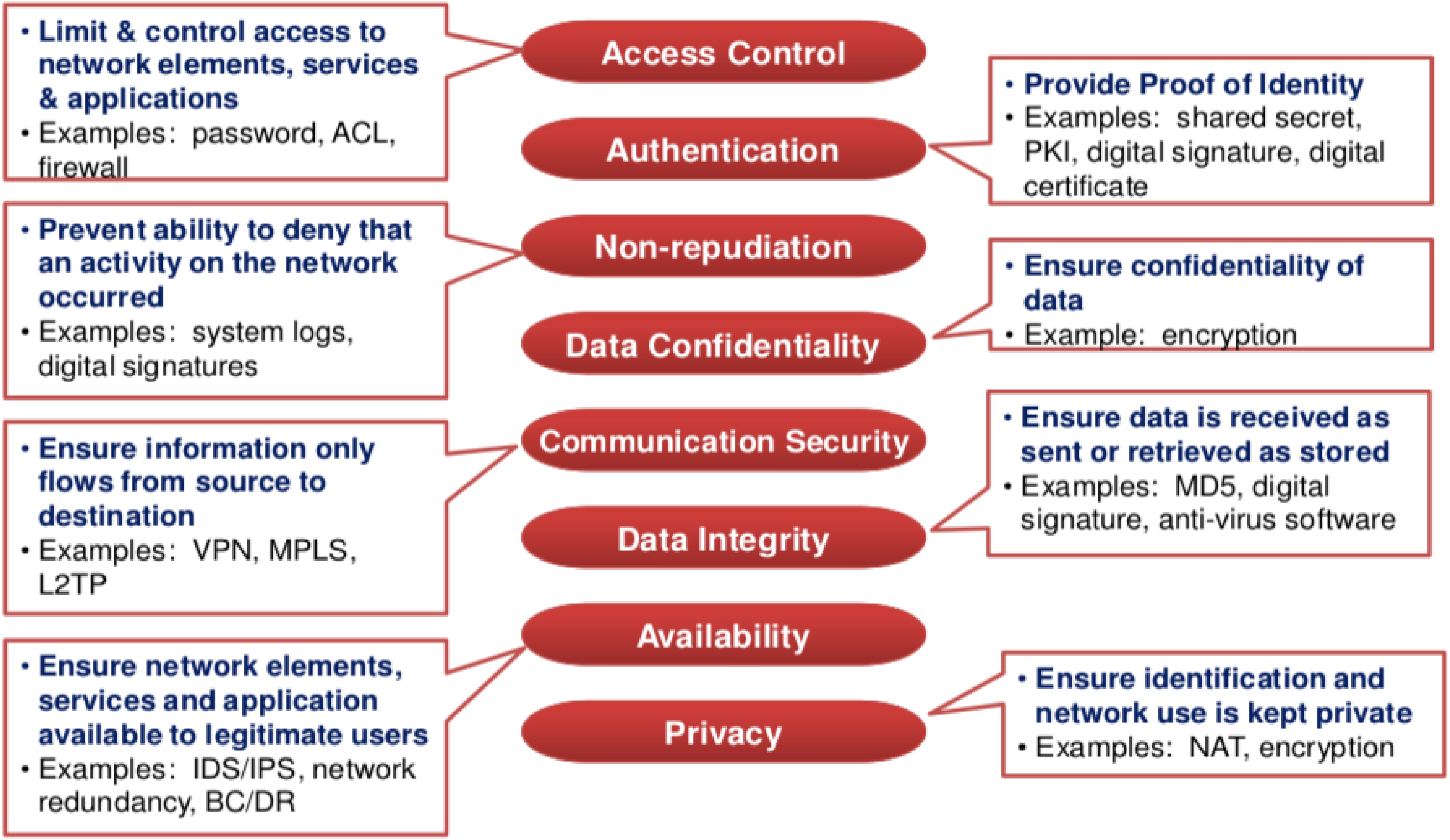
⑩VoLTE and Fixed IMS Penetration Testing

⑩FTTH Service Assessment

⑩Compromised Assessment

⑩Telecom SAP Implementation Security Assessment

Eight Security Dimensions Address the Breadth of Network Vulnerabilities



- **Limit & control access to network elements, services & applications**
- Examples: password, ACL, firewall

Access Control

Authentication

- **Provide Proof of Identity**
- Examples: shared secret, PKI, digital signature, digital certificate

- **Prevent ability to deny that an activity on the network occurred**
- Examples: system logs, digital signatures

Non-repudiation

Data Confidentiality

- **Ensure confidentiality of data**
- Example: encryption

- **Ensure information only flows from source to destination**
- Examples: VPN, MPLS, L2TP

Communication Security

Data Integrity

- **Ensure data is received as sent or retrieved as stored**
- Examples: MD5, digital signature, anti-virus software

- **Ensure network elements, services and application available to legitimate users**
- Examples: IDS/IPS, network redundancy, BC/DR

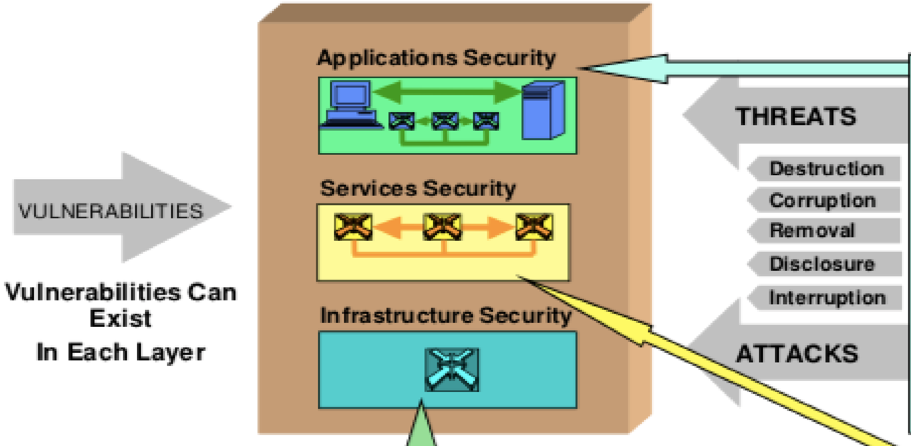
Availability

Privacy

- **Ensure identification and network use is kept private**
- Examples: NAT, encryption

Eight Security Dimensions applied to each Security Perspective (layer and plane)

Three Security Layers



3 - Applications Security Layer:

- Network-based applications accessed by end-users
- Examples:
  - Web browsing
  - Directory assistance
  - Email
  - E-commerce

1 - Infrastructure Security Layer:

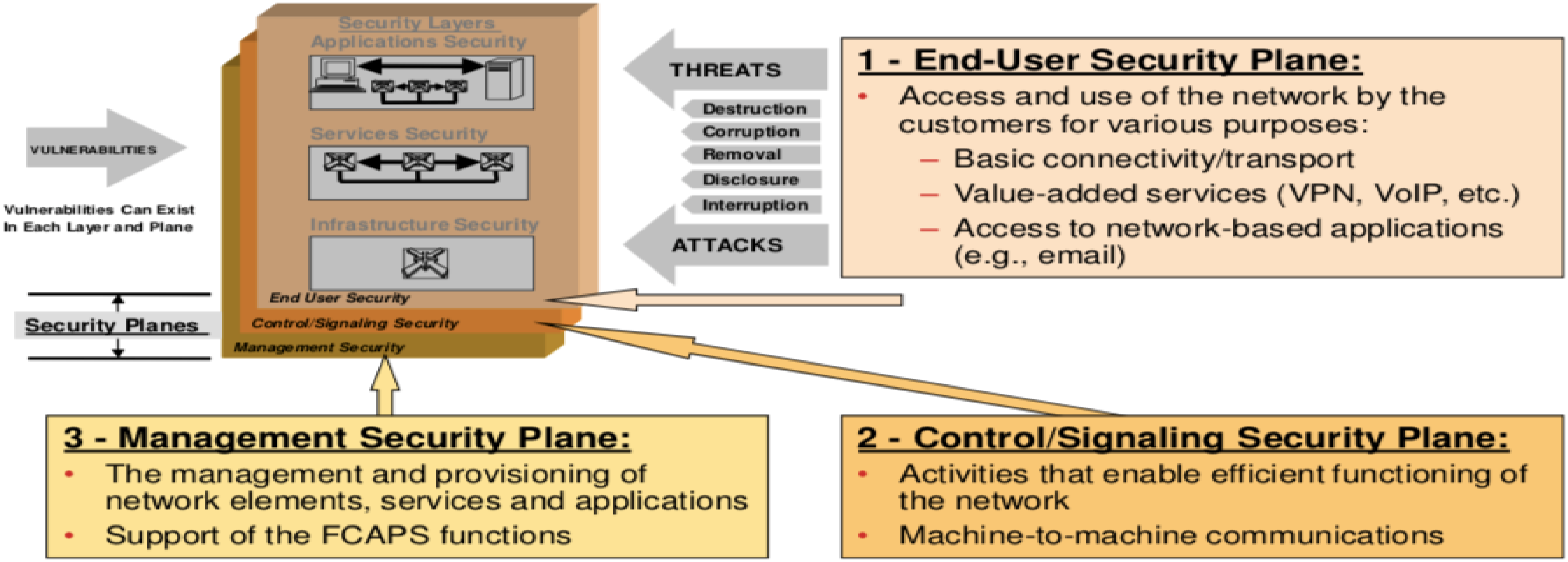
- Fundamental building blocks of networks services and applications
- Examples:
  - Individual routers, switches, servers
  - Point-to-point WAN links
  - Ethernet links

2 - Services Security Layer:

- Services Provided to End-Users
- Examples:
  - Frame Relay, ATM, IP
  - Cellular, Wi-Fi,
  - VoIP, QoS, IM, Location services
  - Toll free call services

- **Each Security Layer has unique vulnerabilities, threats**
- **Infrastructure security enables services security enables applications security**

Three Security Planes



1 - End-User Security Plane:

- Access and use of the network by the customers for various purposes:
  - Basic connectivity/transport
  - Value-added services (VPN, VoIP, etc.)
  - Access to network-based applications (e.g., email)

2 - Control/Signaling Security Plane:

- Activities that enable efficient functioning of the network
- Machine-to-machine communications

3 - Management Security Plane:

- The management and provisioning of network elements, services and applications
- Support of the FCAPS functions

- **Security Planes represent the types of activities that occur on a network.**
- **Each Security Plane is applied to every Security Layer to yield nine security Perspectives (3 x 3)**
- **Each security perspective has unique vulnerabilities and threats**

FCAPS is the ISO **Telecommunications** Management Network model and framework for network management. **FCAPS** is an acronym for fault, configuration, accounting, performance, security, the management categories into which the ISO model defines network management tasks.

Security Assessment Methodology

⑩Our team members work dedicatedly to review analyze and recommend robust solutions. Every penetration test follows ***GIS Cyber Security Solutions (GCSS)*** proprietary process on clients systems and applications and we also offer to report as per the client’s desired format for enhanced security.

⑩Our aim is to reveal hidden threats, vulnerabilities and conduct necessary actions to eliminate or reduce threats.

Planning and execution

Our professional team designs and conducts penetration tests and run a full series of hand-crafted simulated attacks against your systems and applications.

Penetration tests are designed to eliminate or reduce cyber intruders from an amateur teenage hacker or malicious assaults by highly veterans. Our dedicated team can identify the most likely vectors for attacks and eliminate the same.

Hand-crafted penetration attempts

Based on the research and results of the prior tests, our team of experts would devise and conduct hand-crafted penetration attempts to determine areas of weakness. Based on the results our team would analyze the area of exploitation and reverse engineering for robust security systems.

Reporting and recommendations

⑩We provide detailed documentation for the entire penetration attempt vectors, detailing the types of tests that were attempted, the status of their success or failure, any discovered issues and the resultant risks (sorted by priority), and suggested remediation efforts.

⑩In order to address your comments and feedback, we may provide draft and final versions of the report.

⑩**We follow guidelines from external organizations such as**

- GSMA
- ENISA(European Network and Information Security Agency) ,
- CIS (Center for Internet Security) Guidelines
- OWASP (Open Web Applications Security Project),
- National Institute of Standards and Technology (NIST)
- Open Source Security Testing Methodology Manual (OSSTMM).
- PCI DSS (Wherever Applicable)

Vulnerabilties to be Checked

Some of the key Vulnerabilities Assessed are as under :-

- Dictionary & Brute force Attack
- Sniffing Attack
- SQL Injection Vulnerability
- XSS Script Vulnerability
- CSRF Script Vulnerability
- Shell Shock Vulnerability
- Dos Attack Vulnerability
- Backdoor Vulnerability
- Software Backdoor Testing
- Social Attack Testing
- OWASP TOP 10 Vulnerabilities
- MITM Attack Vulnerability etc

Tools Used

Depending upon the scenario we use below tools to assess the vulnerabilities :-

- Nessus (With OWASP Plugins)
- OWASP Zed Proxy
- Acunetix
- Nmap
- Metasploit
- Burpsuite
- Internal tools
- Hydra
- Nikto
- Vega
- W3af
- GISC Internal Stack of penetration tools
- Scenario based VAPT Strategies & Manual Scripts & Scan Methodologies.