NGN Security

Next Generation Nightmare?

Emmanuel Gadaix
Telecom Security Task Force

Dubai, HITB 2007
Agenda

- Evolution of mobile security issues
- NGN, 3G, IMS, 4G: what is what?
- The NGN architecture
- NGN threats and security controls
- VoIP issues in the IMS model
- Decentralisation of telcos
- Conclusions
The Early Days
History of mobile networks

- Pre-mobile: the PSTN
- 1G: NMT, AMPS, RC2000
- 2G: GSM, CSD
- 2.5G: GPRS, EDGE
- 3G: UMTS, CDMA1x, CDMA-2000, WCDMA
- 4G: IMS, NGN
- 5G: no operator required?
PSTN security issues

- Blue boxing with CCITT #5
- Other boxing techniques
- Out-of-band SS7 stopped in-band signalling
- PSTN generally considered “secure” (closed garden model)
Early mobile systems

First car mounted radio telephone (1921)
First cellular network

In 1978 Bahrain was the first country to operate a commercial cellular system…
Security issues in 1G systems

- **Eavesdropping** (no over the air encryption, easy to listen in to frequencies with a simple radio scanner)
- **Cloning** of phones by intercepting the serial number (ESN)
Lessons from 1G systems

- Designers of early telephony systems had **no considerations for security** – just for functionality.
- Phreakers were quick to learn how to **abuse the system**
- Countermeasures to limit the increasingly large fraud were only “band aid” that **never really eradicated the problem**
2G... the GSM world
2G: GSM “closed” garden
SIM Hacking tools
Bluetooth Security

- Bluejacking allows phone users to send business cards anonymously using Bluetooth.

- Bluesnarfing allows hackers to gain access to data stored on a Bluetooth enabled phone without alerting the phone’s user of the connection made to the device: phonebook and associated images, calendar, and IMEI.

- Bluebugging allows access the mobile phone commands using Bluetooth without notifying or alerting the phone’s user. This vulnerability allows the hacker to initiate phone calls, send and receive text messages, read and write phonebook contacts, eavesdrop on phone conversations, and connect to the Internet.
Encryption in 2G

Mobile Stations

Base Station Subsystem

Network Management

Subscriber and terminal equipment databases

OMC

Exchange System

BTS

BTS

BTS

A5 Encryption

MSC

VLR

HLR

AUC

EIR
Mixed attacks on SIM crypto

Side Channel Attacks

Side Channels
- Power Consumption
- Electromagnetic radiation
- Timing
- Errors
- Etc.

Smart Card

Crypto Processing

Sensitive Information

Input

Output
Security issues in 2G

- Eavesdropping and cloning foiled by use of encryption (no more scanners) and authentication (no more cloning).
- SIM cloning demonstrated due to weaknesses in crypto algorithms. Attacks on COMP128, A5/1 A5/2, A5/3.
- Attackers can tap conversations and decrypt them either in real-time, or at any later time.
- Active attacks such as call hijacking, altering of data messages and call theft.
- Non-technical subscription fraud still a major issue, mitigated by the growth of Prepaid services and Fraud Management Systems.
2.5G

AUC=Authentication Center
BSC=Base Station Controller
BSS=Base Station Subsystem
Gs, Gr, Gb, Gi=interfaces
GGSN=Gateway GPRS Support Node
HLR=Home Location Register
MSC=Mobile Switching Center
PCU=Packet Control Unit
PLMN=Public Land Mobile Network
SGSN=Serving GPRS Support Node
VLR=Visitor Location Register
CG=Charging Gateway

TCP/IP or X.25
The Evolution Continues
3G Security

Network access security (I)
Network domain security (II)
User domain security (III)
Application domain security (IV)
Visibility and configurability of security (V)
SIP / IMS Evolution
Still growing

MOBILE SUBSCRIBER GROWTH IS SLOWING WORLDWIDE

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>South America</td>
<td>117%</td>
<td>49%</td>
</tr>
<tr>
<td>Africa/Mideast</td>
<td>76%</td>
<td>35%</td>
</tr>
<tr>
<td>Eastern Europe</td>
<td>81%</td>
<td>21%</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>72%</td>
<td>16%</td>
</tr>
<tr>
<td>North America</td>
<td>52%</td>
<td>9%</td>
</tr>
<tr>
<td>Western Europe</td>
<td>39%</td>
<td>4%</td>
</tr>
</tbody>
</table>

Source: EMC World Cellular Database: GSM Subscribers by Region
Price war

PRICE COMPETITION IS DRIVING DOWN REVENUE PER MINUTE

Source: CTIA, Merrill Lynch, TIA, Wilkowsky Gruen Assoc.
The VoIP Threat

Anyone can become a VoIP provider
Thousands of VoIP companies
Low investment
Flexible
Fast Time-to-Market
Easy to introduce new services
Low cost international calls
Flat rate plans
VoIP business growing very fast
IMS overview
IMS Model

1. Alice calls Bob, who has a find-me-follow-me service in IMS.
2. Call is routed to the IMS network via a PSTN to IP gateway.
3. Application server forks the call to Bob’s find-me numbers.
4. Call is routed back to the PSTN through the gateway.
5. Bob receives the call just like any other, except, but with added features.

PSTN Technology = slow development
SIP Technology = fast, flexible development
IMS: “Open Garden”
Security in IMS networks
IMS: Inherit VoIP problems

Security assessment concerns several layers, from the terminal (mobile phones) to the SIP application servers.
Protocol Attacks

- **SIP attacks**: interception, impersonation, denial or degradation of service, toll bypass, voice phishing
- **Access Network**: localized denial of service, interception
- **SS7 Network**: SIGTRAN-based attacks could compromise the signaling infrastructure
- **IP Backbone**: routing protocols could compromise operator’s network integrity, cause overload
- **Perimeter**: morphing DMZ with numerous vendors, service providers, content providers, API
# IMS-related Attack Tools

<table>
<thead>
<tr>
<th>Scanning</th>
<th>Enumeration</th>
<th>Denial of Service</th>
<th>Eavesdropping</th>
<th>Others</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCTPscan</td>
<td>netcat</td>
<td>DNS Auditing tool</td>
<td>Angst</td>
<td>RedirectPoison</td>
</tr>
<tr>
<td>SIPping</td>
<td>SiVuS</td>
<td>Internetwork Routing</td>
<td>Cain and Abel</td>
<td>Sipproxy</td>
</tr>
<tr>
<td>fping</td>
<td>sipsak</td>
<td>Protocol Attack Suite</td>
<td>DTMF Decoder</td>
<td>MTPflood</td>
</tr>
<tr>
<td>Nessus</td>
<td>SIPSCAN</td>
<td>UDP Flooder</td>
<td>dsniff</td>
<td>Registration Hijacker</td>
</tr>
<tr>
<td>nmap</td>
<td>smap</td>
<td>Wireshark</td>
<td>NetStumbler</td>
<td>siprogue</td>
</tr>
<tr>
<td>snmpwalk</td>
<td>TFTP BruteForcer</td>
<td>TCAPflood</td>
<td>Oreka</td>
<td>Ravage</td>
</tr>
<tr>
<td>SNSscan</td>
<td>SS7auditor</td>
<td>MTPsequencer</td>
<td>VoIPong</td>
<td>ohrwurm</td>
</tr>
<tr>
<td>VLANping</td>
<td></td>
<td>INVITE Flooder</td>
<td>vomit</td>
<td>RTP fuzzer</td>
</tr>
<tr>
<td>SuperScan</td>
<td></td>
<td>RTP Flooder</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Scanning**
  - SCTPscan
  - SIPping
  - fping
  - Nessus
  - nmap
  - snmpwalk
  - SNSscan
  - VLANping
  - SuperScan

- **Enumeration**
  - netcat
  - SiVuS
  - sipsak
  - SIPSCAN
  - smap
  - TFTP BruteForcer
  - SS7auditor

- **Denial of Service**
  - DNS Auditing tool
  - Internetwork Routing
  - Protocol Attack Suite
  - UDP Flooder
  - Wireshark
  - TCAPflood
  - MTPsequencer
  - INVITE Flooder
  - RTP Flooder

- **Eavesdropping**
  - Angst
  - Cain and Abel
  - DTMF Decoder
  - dsniff
  - NetStumbler
  - Oreka
  - VoIPong
  - vomit

- **Others**
  - RedirectPoison
  - Sipproxy
  - MTPflood
  - Registration Hijacker
  - siprogue
  - Ravage
  - ohrwurm
  - RTP fuzzer
Session Border Controller

The “SIP Firewall” concept
Insider Attacks

- **NMS**: Controls the whole network and every single Network Element
- **OSS**: Customer data, billing records
- **IN**: Prepaid database, Vouchers, CDR
- **Core**: IB backbone, SS7 network
- **VAS**: Services data, billing data
SS7

- Mobile networks use Signalling System no. 7 (SS7) for communication between networks for such activities as authentication, location update, and supplementary services and call control.

- The messages unique to mobile communications are MAP messages. Other protocols include MTP, ISUP, SCCP, TCAP, INAP, CAP.

- The security of the global SS7 network is based on trust relationships between operators and is assuming a closed network architecture.

- One of the problem with the current SS7 system is that messages can be altered, injected or deleted into the global SS7 networks in an uncontrolled manner.
SS7 attacks
Examples of SS7 attacks

- Theft of service, interception of calling cards numbers, privacy concerns
- Introduce harmful packets into the national and global SS7 networks
- Get control of call processing, get control of accounting reports
- Obtain credit card numbers, non-listed numbers, etc.
- Messages can be read, altered, injected or deleted
- Denial of service, security triplet replay to compromise authentication
- Annoyance calls, free calls, disruption of emergency services
- Capture of gateways, rerouting of call traffic
- Disruption of service to large parts of the network
- Call processing exposed through Signaling Control Protocol
- Announcement service exposed to IP through RTP
- Disclosure of bearer channel traffic
NGN Security
NGN: Not a garden any more…
Managing Security

- To be able to make sound security judgments, both the particular business context and the networking environment must be fully understood.
- To support the whole telecom system life cycle, from end-to-end, the following operations have to be undertaken:
  - Business Continuity Management
  - Network Security Design
  - Network Configuration / Integration
  - Network Security Audits
  - Network Security Implementation
  - Fraud Management
Security Operations

- **Risk Management**: all network operation implies a certain risk that must be accepted, avoided, reduced or transferred.
- **Business Continuity**: the operator’s critical processes and information should be protected from disclosure and/or disruption.
- **Lowering operator costs**: well thought-out security solutions provide a payback in terms of
  - Reduced operating costs
  - Reduced risk of fraud
  - Reduced risk of critical security-related network outages and potentially less churn
Security Wheel

- Nw Security Analysis (incl. penetration tests)
- Nw Security Assessment
- Nw Security Design
- Nw Configuration/Integration
- Nw Management
- Fraud Management
- Nw Security Assessment/Analysis
Security Architecture Model

Separated Security Planes
- End User Security Plane
  - Application Security Layer
  - Netw. Services Security Layer
  - Infrastructure Security Layer
- Signaling and Control Security Plane
  - Application Security Layer
  - Netw. Services Security Layer
  - Infrastructure Security Layer
- O&M Security Plane
  - Application Security Layer
  - Netw. Services Security Layer
  - Infrastructure Security Layer

Security Dimensions
- Accountability
- Authentication
- Authorization
- Availability
- Confidentiality
- Integrity
- Non-Repudiation
- Privacy

Threats
- Disclosure
- Modification
- Destruction/loss
- Interruption
- Unauthorized access

Attacks

Security Policies & Principles: Defense in Depth, Least Privilege, Fail Safe Stance, Choke Point, Diversity in Defence...
## ITU-T X.800 Threat Model

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Destruction</strong> (an attack on <strong>availability</strong>):</td>
<td>![Diagram of network with X symbol]</td>
</tr>
<tr>
<td></td>
<td>– Destruction of information and/or network resources</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Corruption</strong> (an attack on <strong>integrity</strong>):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Unauthorized tampering with an asset</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td><strong>Removal</strong> (an attack on <strong>availability</strong>):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Theft, removal or loss of information and/or other resources</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td><strong>Disclosure</strong> (an attack on <strong>confidentiality</strong>):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Unauthorized access to an asset</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td><strong>Interruption</strong> (an attack on <strong>availability</strong>):</td>
<td></td>
</tr>
<tr>
<td></td>
<td>– Interruption of services. Network becomes unavailable or unusable</td>
<td></td>
</tr>
</tbody>
</table>
X.805 Security Domains

- Access Network Security Domain
- Visited NGN Network Security Domain
- Home NGN Network Security Domain

IPsec ESP tunnel

Security Gateway Function (SEGF)
Threats

Relative threats of NGN networks: insiders still #1 problem
NGN Security Summary

- Divided into Security domains
- Authentication is performed on service and transport layer
- Authentication for NGN IMS is based on identity and keys stored on smart card (UICC)
- The S-CSCF authenticates users during registration
- Full IMS security as defined by 3GPP is the preferred solution
- Domains are considered to be trusted
- Inter-domain security is provided by IPsec
- Media data security relies on transport network
Conclusions

- The IMS paradigm introduces several new attack vectors.
- Critical Infrastructure such as SS7 is more exposed and will be targeted.
- NGN Security is well defined and properly documented – at least in theory.
- NGN implementations will likely suffer from interoperability problems leading to security exposure.
- The complexity of emergent network architectures will present a serious challenge to their security.
- Operators and Regulatory Bodies must embrace security as part of the design process of their networks.
Questions?

Contact: eg@tstf.net
Thanks

- H.E. Mr. Mohamed Nasser Al Ghanim
- The HITB Crew
- The TSTF OOB Research Group

Some illustrations on slides copyright from RCS Labs, Data Connection Limited, Aqsacom, 3GPP, Ericsson, ETSI, EMC, ITU, Merrill Lynch, Newport Networks