Network Infrastructure Security in Cellular Data Networks: An Initial Investigation

Kavita Barapatre, Nirlesh Koshta, Vishal Sharma
IIT Bombay, Mumbai, India
and
Fabio Ricciato
Forschungszentrum Telekommunikation Wien (FTW), Vienna, Austria

© Copyright 2005-06
All Rights Reserved
Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, ...
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security
Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM/GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security
Why Infrastructure Security?

Network Security

Information Security
- Keeping user’s info. protected
- Subject of cryptography
- Not subject of this talk

Infrastructure Security
- Sustaining ability of network elements to provide connectivity between communicating entities
- Subject of this talk

Cellular GSM/CDMA networks moving to an IP core …

- Network increasingly open
- Control/data segregation inherently less stringent
- Increased threats! … Exposure to wireline-like security risks
Motivation (contd)

- Interplay of IP and complex structure of cellular networks
  - Gives rise to subtle phenomena ...
  - ... that may not be easily conceived
  - Need to be found empirically via intelligent experimentation

- Provider *infrastructure* security becomes *key*, imperative to ...
  - Investigate susceptibilities and risks
  - Evaluate options, fixes, and solutions
  - Propose techniques and tools for proactive/reactive action
Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security
Vulnerabilities in GSM

Flaws in authentication and encryption

- No subscriber auth. in initial part of mobile originated call
- Radio interface well protected, fixed infrastructure vulnerable
- Access to AuC allows attacker to obtain auth. key
  - Encrypted MS ↔ BS traffic can be captured & deciphered
- GSM encryption has been broken!
  - Large scale attacks can be launched with relatively small traffic vols.
A Signaling Channel DoS Attack in GSM

Malicious MS now repeats exercise

Signaling channels end up assigned & “lockout” genuine MSs
GPRS Network Architecture
Vulnerabilities and Criticalities in GPRS

Critical Interfaces

Gi: Exposed to Internet and corporate networks

Gp: Primary interconnection pt. between operator’s n/w and untrusted external n/ws

Gc: Allows access (via HLR) to key user info. from remote network during roaming

Vulnerable Interfaces

Gi: Exposed to all threats from Internet: viruses, DoS, and malicious network traffic

Gp: Connection hijacking, over-billing from a roaming network during handover

Gn: Not encrypted by default
A DCH “Lockout” Attack in GPRS

T = DCH release/dynamic reassignment timeout

GSM/GPRS RAN

MS with open PDP context & IP address

DCH never released!

2.5G/3G Provider’s Core Network

Small IP pkt. at rate $R > 1/T$

External Agent

With multiple DCHs occupied, logical radio resources wasted

- Congestion in cell
- Lockout of genuine MSs

UMTS RAN

Other 2.5G/3G CN

©Copyright 2005-06
All Rights Reserved

SANOG 7, Mumbai, India, 23-24 Jan. 2006
Impact of Unwanted Traffic: Viruses, worms, trojans, ...

- Attacker can be inside your n/w!
- Consider effect of large infections!
- Viruses/worms from Internet detected in 3G core networks
Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, ...
- **Testbed setup and testing scenarios**
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security
Experimental Test-bed Setup & Testing Scenarios

Testing can be:
- Intra-provider
- Inter-provider (CDMA-GSM)
- Wireless-wireline
Outline of the Talk

- Motivation – why worry about *infrastructure security*?
- GSM /GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, ...
- Testbed setup and testing scenarios

  **Methodology:** nature of tests possible, what else is needed

- Tools for investigating network security
Testing Methodology

**Taxonomy of Tests**

- **Active Probing**
  - Direct malicious generated traffic to SP’s network or to a remote m/c on network. E.g.
    - SYN attack
    - Tear-drop attack
    - Smurf attack
  - Exploit various types of commun.
    - Port-to-port
    - IP address spoofing
  - Infer network parameters: RTT, buffers

- **Passive Listening**
  - Provoke remote attacker(s) to attack m/c under observation
    - Invoke attacks, HoneyD as “bait”
    - Run intrusion detection systems on attacked m/c
    - Apply intelligent algorithms for proactive threat inference
Outline of the Talk

- Motivation – why worry about infrastructure security?
- GSM/GPRS network architecture & critical interfaces
- Attacks exploiting security loopholes in GSM/GPRS
- Impact of unwanted traffic: viruses, worms, trojans, …
- Testbed setup and testing scenarios
- Methodology: nature of tests possible, what else is needed
- Tools for investigating network security
Network Security Investigation

Investigative Tools

Detect
- NMAP
- Netcat

Exploit
- Honeyd
- PackEth

Analyze
- Snort
- NTOP
Tools for Detecting Vulnerabilities

- **Network MAPper (NMAP)**
  - Determines running apps. on target m/c
  - Identifies open ports, OS, firewalls used by remote host(s)

- **Netcat**
  - Utility used to read/write across network connections using TCP/UDP protocol(s)
  - Feature-rich, network debugging and exploration tool
Tools for Exploiting Vulnerabilities

● HoneyD:
  ● Creates virtual machines (VMs)
  ● VMs have unique IP addresses
  ● Lure attackers to themselves
  ● Can be Windows or Linux

● PackETH
  ● Packet generator
  ● Generates packets of any protocol - ARP, TCP, UDP, ...
  ● User configurable pkt. profiles
Tools for Analyzing Vulnerabilities

- **Snort**
  - Real-time traffic analysis & packet logging
  - Usable in multiple modes:
    - Packet sniffer
    - Data logger
    - Intrusion detection
  - Generates variety of alerts – usable for proactive detection

- **NTOP**
  - Traffic usage monitor & packet analyzer
  - Supports mgt. activities: planning, opt., detection
  - Tracks ongoing attacks, generates alarms
### NTOP at Work

#### Traffic breakdown by hosts seen

<table>
<thead>
<tr>
<th>Host</th>
<th>Domain</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Other Name(s)</th>
<th>Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>dnscache.iitb.ac.in</td>
<td></td>
<td>10.200.1.11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.1.99</td>
<td></td>
<td>10.11.1.99</td>
<td>00:03:0D:32:1B:85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.201.89</td>
<td></td>
<td>10.11.201.89</td>
<td>00:13:20:2A:25:85</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.100.70</td>
<td></td>
<td>10.11.100.70</td>
<td>00:11:11:8C:3E:CA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.201.54</td>
<td></td>
<td>10.11.201.54</td>
<td>00:50:BF:F0:FE:7B</td>
<td></td>
<td></td>
</tr>
<tr>
<td>bridge sp. tree/osi route:00:00:00</td>
<td></td>
<td>01:80:C2:00:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>d-link systems, inc.:00:00:00</td>
<td></td>
<td>00:80:C8:00:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.11.16</td>
<td></td>
<td>10.11.11.16</td>
<td>00:03:47:6B:AA:98</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.11.200.65</td>
<td></td>
<td>10.11.200.65</td>
<td>00:08:A1:7B:AD:81</td>
<td></td>
<td></td>
</tr>
<tr>
<td>router.hostet1.iitb.ac.in</td>
<td></td>
<td>10.11.250.1</td>
<td>00:04:96:10:4A:00</td>
<td></td>
<td></td>
</tr>
<tr>
<td>extreme networks:00:00:00</td>
<td></td>
<td>00:EC:2B:00:00:00</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Packet size distribution

- < 64 bytes: 38.0%, 2.62M packets
- 64 to 127 bytes: 42.4%, 2.60M packets
- 128 to 255 bytes: 14.0%, 1.00M packets
- 256 to 511 bytes: 1.2%, 90 packets
- 512 to 1023 bytes: 1.2%, 70 packets
- 1024 to 1518 bytes: 1.5%, 98 packets
- > 1518 bytes: 0.0%, 0 packets

#### TCP/UDP distribution by major protocols
Attacking m/c: scans using NMAP

Exposed m/c: performs analysis via Snort
What More is Needed

Radio Access Network (RAN) | Core Network (CN)

BSS | CS-CN
BTS | Information Servers
BSC | PS-CN
Gb | Application Servers & Proxies

GSM/GPRS RAN

UTRAN

GGSN

SGSN

Gn

Gi

Internet

BG

PS-CN of other carrier

Monitoring points

©Copyright 2005-06
All Rights Reserved

SANOG 7, Mumbai, India, 23-24 Jan. 2006
Summary

- Cellular infrastructure security ... critically important in future
- Analyzed GSM /GPRS from a vulnerability standpoint
- Highlighted key aspects, such as
  - Critical interfaces
  - Sample attacks
  - Effects of unwanted traffic!
- Presented our testbed setup and testing scenarios
- Focused on nature and types of test portfolio
- Reviewed tools and techniques to assess security