Taming Mr Hayes: Mitigating Signaling Based Attacks on Smartphones

Dependable Systems and Networks (DSN) 2012

Collin Mulliner, Steffen Liebergeld, Matthias Lange, Jean-Pierre Seifert
{collin,steffen,mlange,jpseifert}@sec.t-labs.tu-berlin.de
Researchers can attack mobile phones via spoofed SMS messages

Science News

Stealth Attack Drains Cell Phone Batteries

Malicious Android apps double in six months

Creepy Android malware records your phone calls

Mobile Trojan horse tries to send premium rate SMS messages

Windows Phone 7.5 SMS Vulnerability Can Disable Messaging

Security Alert: DroidDream Malware in Official Android Market
Attacks against smartphones
Attacks against cellular network infrastructure
Attacks against Smartphones

- Malware: trojans & botnets
  - Premium SMS fraud (this is common today!)
  - Data theft
  - Denial-of-Service ... phone stops working

- Targets
  - End user
  - The actual smartphone
Rooted & Jailbroken Smartphones

- **Disable major security features of smartphone OS**

- **User driven (voluntarily)**
  - Gain full control over phone – access all “features”
  - Install “unauthorized” applications

- **Rooting malware**
  - Gain system privileges to access users data etc..
  - Abuse known root exploits
    (observed in the wild, e.g. DroidDream)
Attacks against Cellular Network Infrastructure

- Denial-of-Service attacks – reliability is their business!
  - Extortion
  - Cyber warfare

- Targets
  - Mobile Network Operators (MNOs)
  - Cellular infrastructure components
Previous Work tried to protect the Phone!

We aim to protect the network!
Signaling Attacks

- **Denial-of-Service (DoS) attack against cellular network**

  - Targets: cellular infrastructure components
    - Home Location Register (HLR)
    - Packet-Data Infrastructure
    - ...

- Attacks executed by hijacked smartphones
  - Malware: trojans and botnets

- Accidental misuse or misconfiguration by the user

  GSMA Network Efficiency Threats v0.4, May 2010
Prevent Signaling Attacks

- **Cellular network side**
  - Very expensive
  - Slow adoption

- **Cellular modem “baseband” side**
  - No access to sources
  - Modification → re-certification (slow)
Prevent Signaling Attacks

- **Cellular network side**
  - Very expensive
  - Slow adoption

- **Cellular modem “baseband” side**
  - No access to sources
  - Modification → re-certification (slow)

- **Our solution: Smartphone side**
  - New smartphone released every 6 month
  - Fast adoption possible!
Contributions

- **Categorization of Signaling Issues**
  - We investigated different types of signaling issues

- **Cellular Signaling Filter**
  - Designed, implemented, and evaluated a signaling filter
  - The filter is deployed and executed on the smartphone

- **Safe-to-root virtualized Android**
  - Our system works even when the smartphone OS is rooted!
Signaling Attacks

- DoS attack against cell network
  - Hijacked smartphones

- “Knockout” HLR (user DB)
  - Massively issue “insert call forwarding” command

On Cellular Botnets (CCS 2009 Traynor et al)

- Overload Packet-data network
  - Massively create / destroy PDP context
Signaling Attacks

- DoS attack against cell network
  - Hijacked smartphones

- “Knockout” HLR (user DB)
  - Massively issue “insert call forwarding” command

On Cellular Botnets (CCS 2009 Traynor et al)

- Overload Packet-data network
  - Massively create / destroy PDP context
A Signaling Attack: HLR DoS
A Signaling Attack: HLR DoS

Communication breaks down
Signaling Attacks work because...

- Permission just deny/grant access to cellular modem
  - Users always say “yes”

- “Rooted” devices
  - Permissions are worthless

- Cellular modem is not protected
Stop “Malware” from abusing the Modem
Our solution: The Virtual Modem

- Connects to real modem
- Provides modem interface to virtualized Android phone
- Resilient against rooting
  - Android VM cannot access modem directly
System Architecture

- L4 Fiasco.OC micro kernel
  - Hypervisor

- Virtual Modem
  - L4Linux with minimal userland
  - Contains modem driver

- Android VM
  - Android + L4Linux = L4Android*
  - Custom RIL for virtual modem

*http://www.L4Android.org
Development Target

- AAVA dev phone
  - x86 moorestown CPU

- Modem interface
  - GSM AT commands
    (this is common!)
Inside the Virtual Modem

Virtual Modem

- Virtual Serial Interface
- Virtual Network Interface
- AT Command Filter
- IP Filter
- Baseband Driver
The AT Command Filter
The AT Command Filter

Attacks rely on capability to issue commands at high rate
Filter → rate limiter
Commands to filter

- Command → Signal → Attack

- Signaling relevant commands

  Packet-Data : AT+CFUN, AT+CDGMNT, AT*EPPSD

  HLR : AT+CCFC

  SMS : AT+CMGS
Commands to filter

- Command → Signal → Attack

- Signaling relevant commands
  
  Packet-Data : AT+CFUN, AT+CDGMNT, AT*EPPSD
  
  HLR : AT+CCFC
  
  SMS : AT+CMGS
AT Command Usage under “normal” Conditions

<table>
<thead>
<tr>
<th>Command</th>
<th>#</th>
<th>When</th>
<th>Why</th>
</tr>
</thead>
<tbody>
<tr>
<td>AT+CFUN</td>
<td>2</td>
<td>Boot</td>
<td>Flight mode. Normal mode.</td>
</tr>
<tr>
<td>AT+CFUN</td>
<td>1</td>
<td>Use</td>
<td>Switch to GSM-only.</td>
</tr>
<tr>
<td>AT+CDGMNT</td>
<td>1</td>
<td>Boot</td>
<td>Set PDP configuration.</td>
</tr>
<tr>
<td>AT*EPPSD</td>
<td>1</td>
<td>Boot</td>
<td>Activate PDP context.</td>
</tr>
<tr>
<td>AT+CMGS</td>
<td>1</td>
<td>Use</td>
<td>Send a SMS message.</td>
</tr>
<tr>
<td>ATD</td>
<td>1</td>
<td>Use</td>
<td>Issue a voice call.</td>
</tr>
<tr>
<td>AT+CCFC</td>
<td>3</td>
<td>Use</td>
<td>Query forwarding settings.</td>
</tr>
<tr>
<td>AT+CCFC</td>
<td>2</td>
<td>Use</td>
<td>Set a call-forwarding.</td>
</tr>
</tbody>
</table>
The HLR Attack Setup

- Numbers taken from “On Cellular Botnets”
  - Access to number of actual setup very hard
  - We evaluated against the attack described in:


- Simulated HLR supported 1 million users
The HLR DoS Attack

- HLR collapse at 2500 transactions per second (TPS)
  - 2500 TPS relate to example HLR setup and network size

- 4.7 seconds/transaction = ~12 transactions/minute
  → 11750 bots required for attack

- 12 transaction/minute → maximum possible speed
  → Number of commands/minute, can only issue one after another
Preventing the HLR DoS Attack

- Limit number of transactions/minute
- Force botnet size increase!
Preventing the HLR DoS Attack

- Commands/minute are on average
- Android issues 5 commands for configuring call forwarding
- Our filter has two values: 1. cmd count  2. time-interval
  e.g. 15 commands over 10 minutes = 1.5 cmds/minute
Our Virtual Modem protects the Network
Virtual Modem further prevents...

- PDP-context switching Denial-of-Service attack
  - Similar filter rules as used to prevent HLR attack

- Prevent SMS-based C&C for mobile botnet
  - Detect and prevent large number of binary SMS messages

- Prevent Premium rate SMS fraud
  - Prevent sending SMS to “short codes”

Detail are in the paper.
Lessons learned...

- Modem is just a network interface
  - Can be abused by malware

- Modem is not protected
  - Permission systems are not enough

- Specialized protection required
  - Control usage of modem interface
Summary and Contributions

- Signaling Attacks are a serious problem for cellular networks
  - Various kinds of signaling related attacks
  - Easy to execute using hijacked smartphones

- Our Virtual Modem mitigates
  - Signaling Attacks
  - SMS-based fraud and botnets

- System architecture resilient against rooting
  - Android OS and policy enforcement are separated
Virtual Modem ported to current Smartphones

- Smartphone virtualization for security is an ongoing project

- Now also runs on
  - Samsung Galaxy S II
Q & A

Thank you for your attention!

Questions?
Future Work

- VPN in virtual modem
  - secure credentials if system is hijacked and rooted

- Advanced IPS / IDS in virtual modem
  - vmodem can monitor and/or block IP traffic

- Policy update infrastructure
  - System to update and modify vmodem policy from network

- Secure GUI
  - Ask user for permission for some actions

- Hardware virtualization
  - Make use of HW virtualization support to improve performance