On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core

Patrick Traynor et. al

Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS) 2009

Soohyung Kim

Yeojeong Yoon

2010. 4. 20

KAIST

KAIST 한국과학기술원

Outline

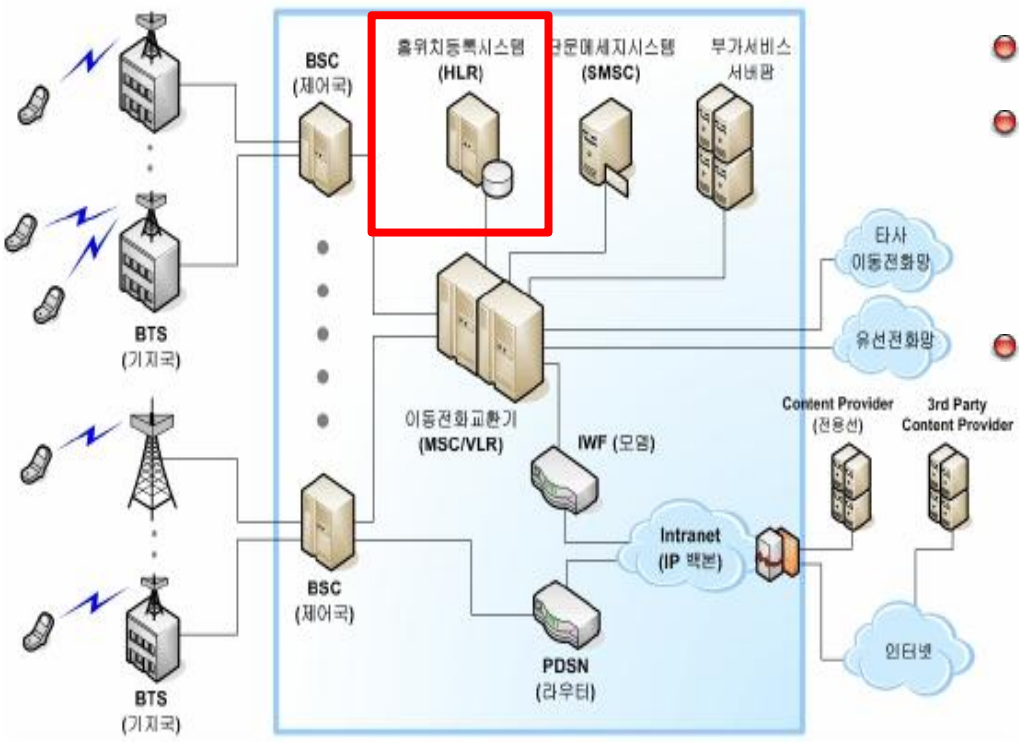
- Introduction
- Attack Overview
- Characterizing HLR Performance
- Profiling Network Behavior
- Attack Characterization
- Avoiding Wireless Bottlenecks
- Command and Control from a botmaster
- Attack Mitigation
- Conclusion

Introduction(1/5)

- **Bot**
  - Short for robots
  - Programs which run autonomously
  - Under the control of a human operator commonly known as a botmaster
- **Botnet**
  - Networks of infected bots
  - Distributed Denial of Service(DDos)
  - Installing Adware
  - Spamming

Introduction(2/5)

- **Cellular Systems – GSM**



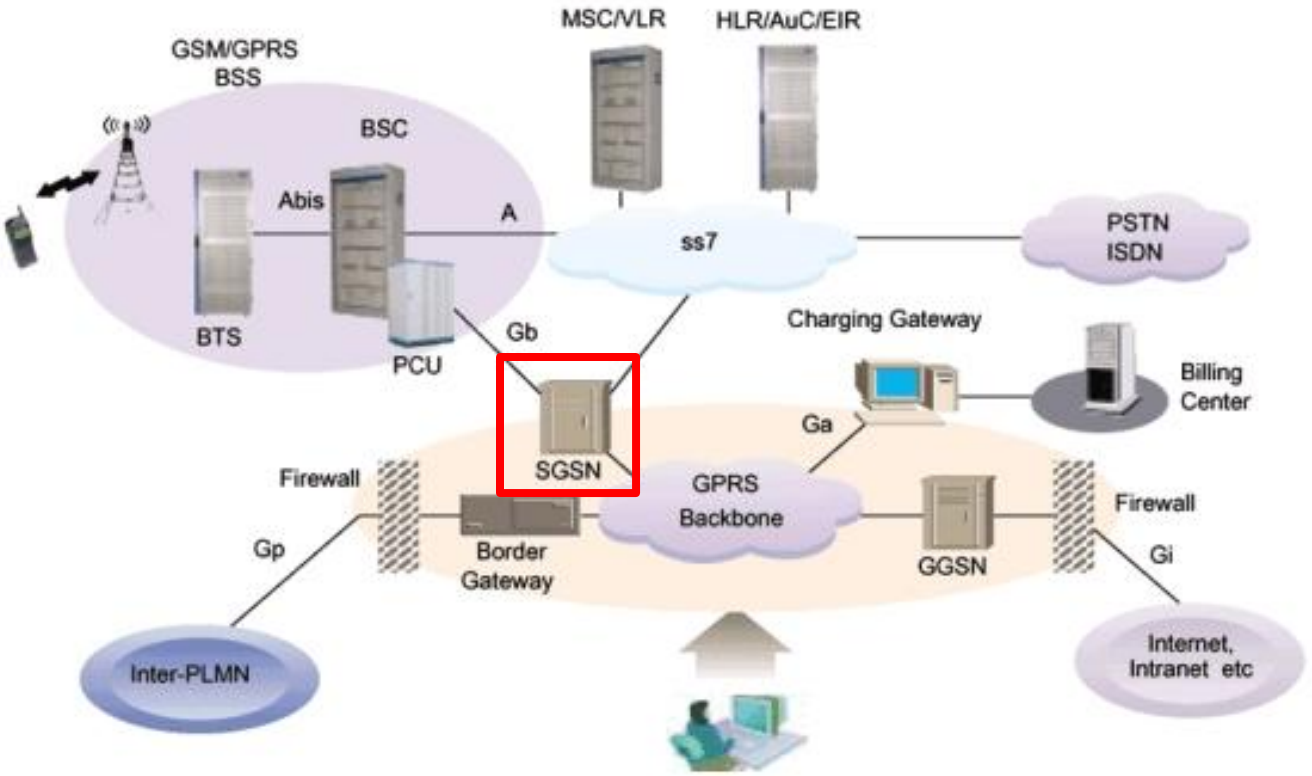
- Mobile Station(MS)
- Base Station Subsystem(BSS)
  - Base Tranceiver Station(BTS)
  - Base Station Controller(BSC)
- Network Subsystem
  - Mobile Switching Center(MSC)
  - **Home Location Register(HLR)**
  - Visitor Location Register(VLR)

Introduction(3/5)

- **Home Location Register(HLR)**
  - Heart of a cellular network
  - Central database that contains details of each mobile phone subscriber that is authorized to use the GSM core network
  - Keeps track of each user's location
  - Manages the power status of the mobile phones
  - Provides the subscribers information

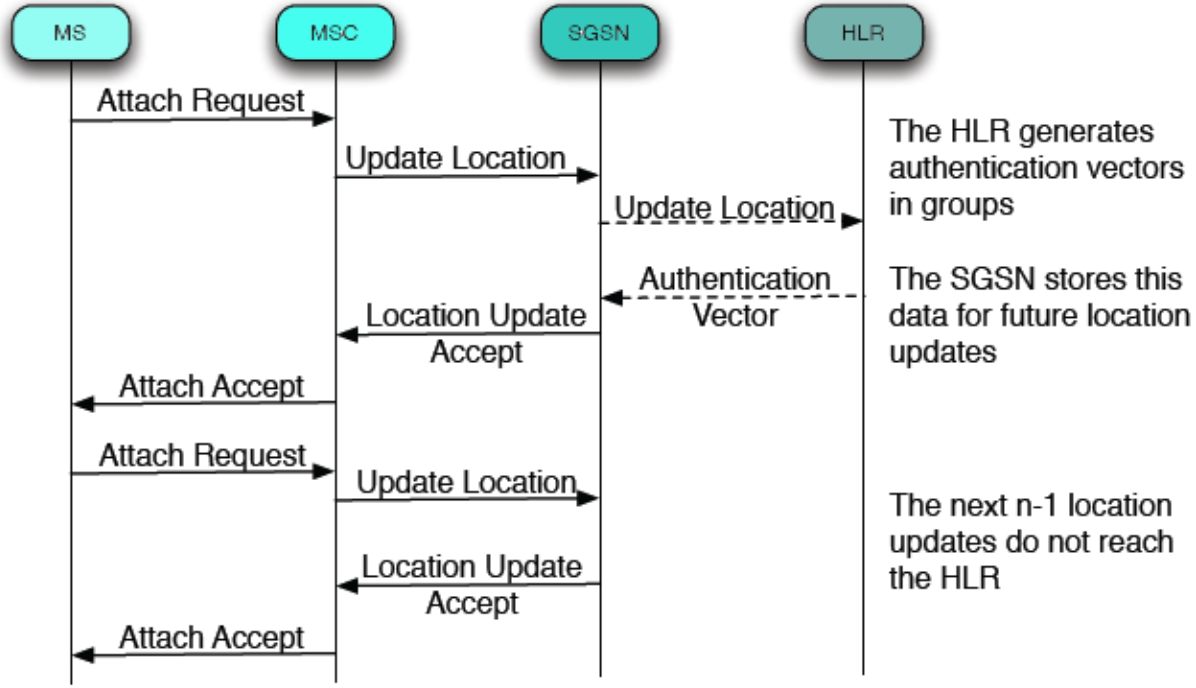
Introduction(4/5)

- **Cellular Systems – GPRS**
  - Upgrade GSM



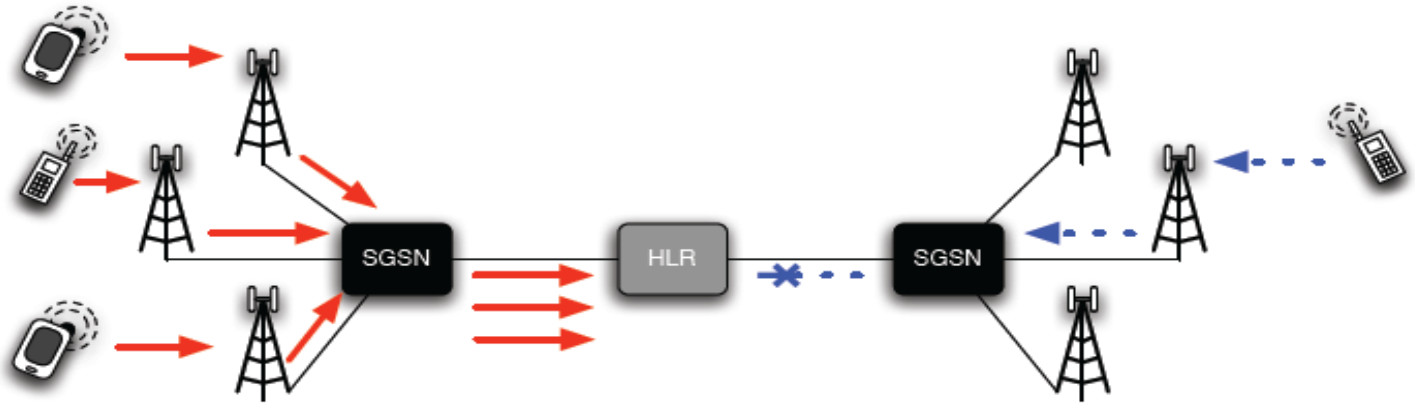
Introduction(5/5)

- **Serving GPRS Support Node(SGSN)**
  - Deliveries of data packets from and to the mobile stations within its geographical service area
  - Get the user's information from HLR



Attack Overview

- **DoS attacks using selected service request type on the Home Location Register(HLR)**



  - Failure of an HLR can cause all users serviced by this database to be denied service
- **Different from the Dos attacks observed on the Internet**
  - Mobile devices transmit only specific types of messages
  - Unnecessary traffic or side effects are not generated

Characterizing HLR Performance(1/2)

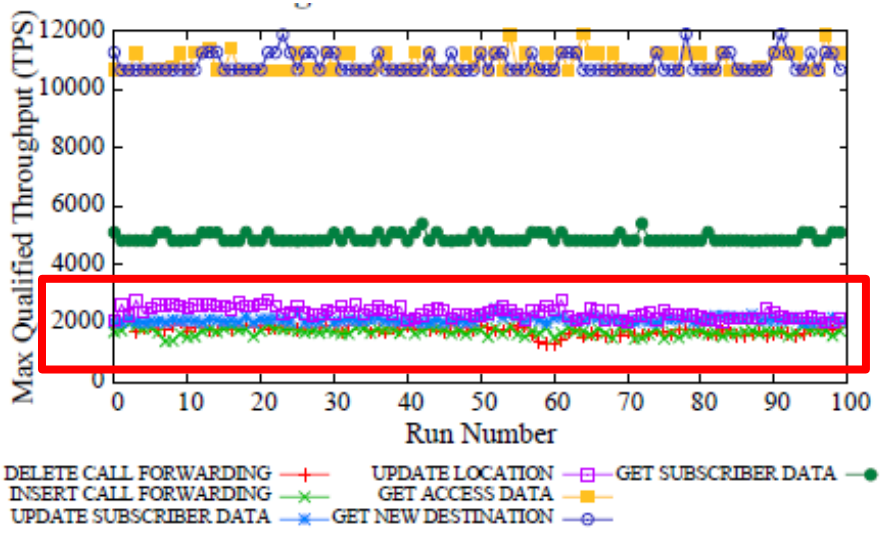
- **Using the Telecom One(TM1)**
  - First database benchmark designed for telecommunication applications
  - Simulates a typical Home Location Register (HLR) database used by a mobile carrier
  - Reducing the effort needed for an adversary to effectively render an HLR unavailable

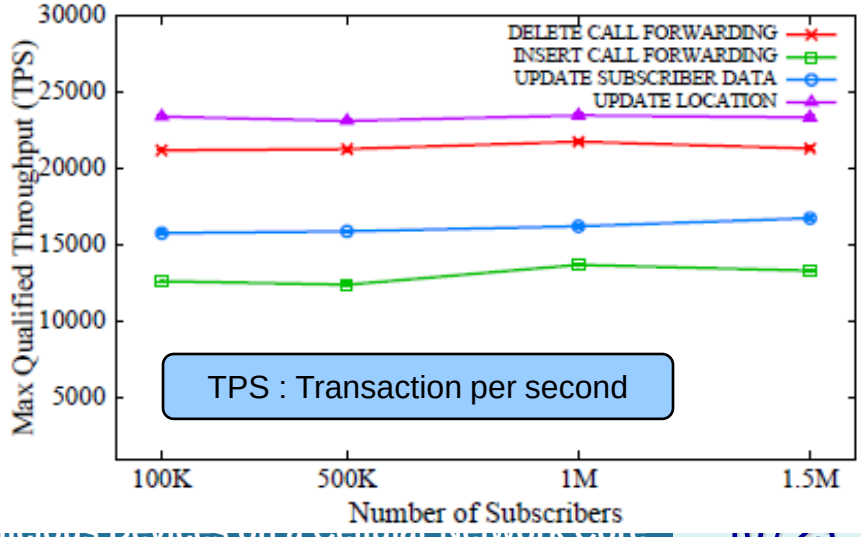
Characterizing HLR Performance(2/2)

- **Simulate normal traffic by providing a "Default Mix" of read and write operations**

Transaction	Type	Default Mix
get_subscriber_data	r	35%
get_new_destination	r	10%
get_access_data	r	35%
update_subscriber_data	w	2%
update_location	w	14%
insert_call_forwarding	rw	2%
delete_call_forwarding	rw	2%

80%



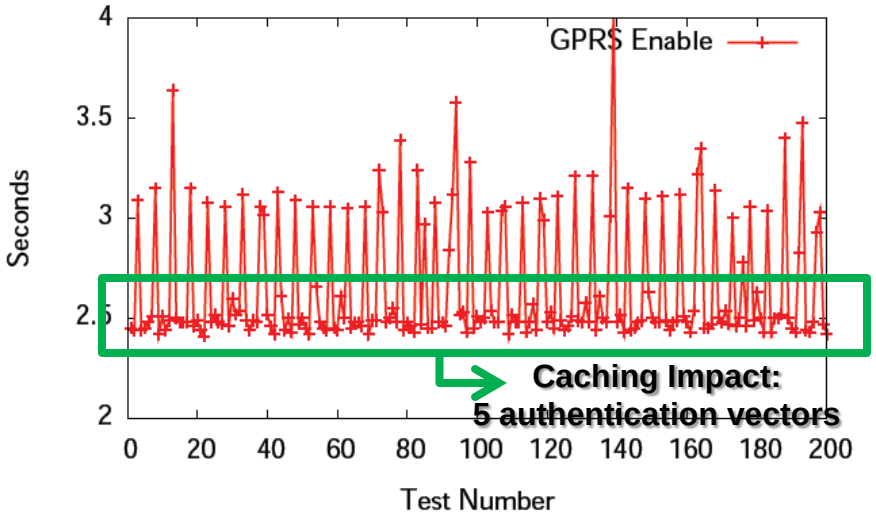


Profiling Network Behavior (1/4)

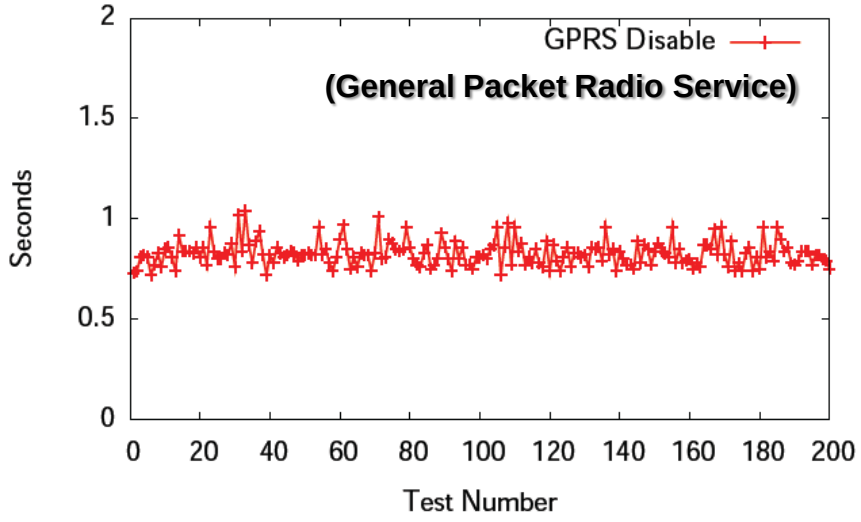
- **Profiling network behavior from an attack perspective**
  - Write-based service requests more expensive than read-based service requests
  - Reconcile the differences between simulations and reality
  - Consult standards documents to verify discrepancies in expected and observed behavior
- **Measuring network behavior**
  - Injected and measured service requests representing each of the four write-based meta-commands on live cellular network
  - Test phone: Nokia 9500 running Symbian Series 80
  - Each AT command was executed a total of 200 times during low traffics with a two second delay between the sequential execution of commands

Profiling Network Behavior (2/4)

- **Update Location**
  - Operation to keep track of each user's location as a device moves between two base stations or turn on/off
  - All location update operations require "device authentication"
  - The caching of authentication data on a real network: making attacks using the update_location meta-command difficult



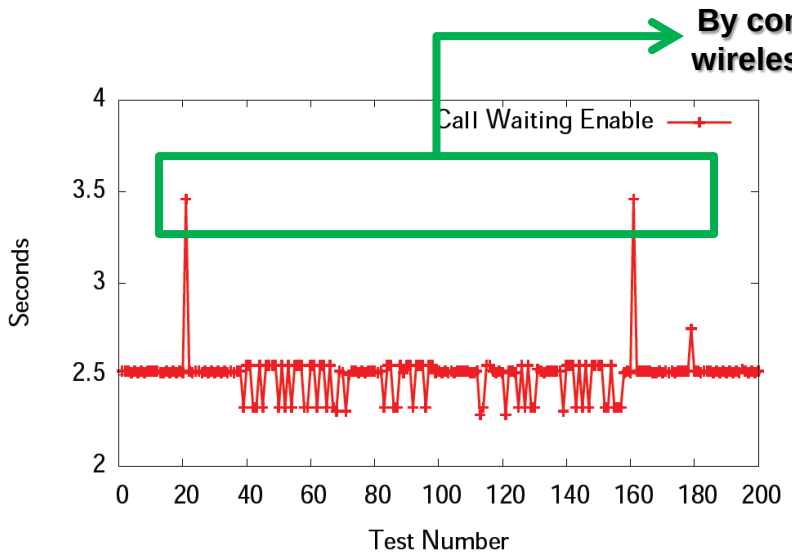
Response times for location updates via the GPRS attach AT command



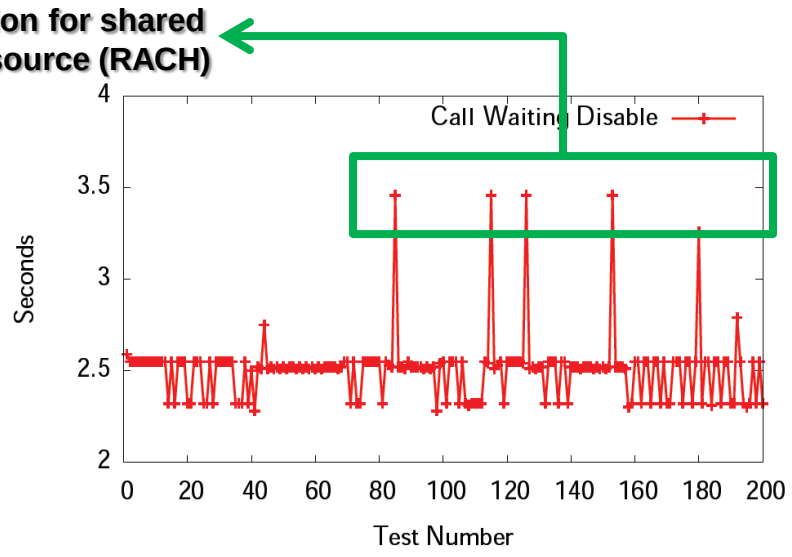
Response times for location updates via the GPRS detach AT command

Profiling Network Behavior (3/4)

- **Update Subscriber Data**
  - Activation, deactivation or modification of the parameters of many services requires the HLR to modify a number of fields
  - Ex. Call Waiting, Call Barring, Modify PDP(Packet Data Protocol) Context
  - All Call Waiting enable requests are directed to the HLR



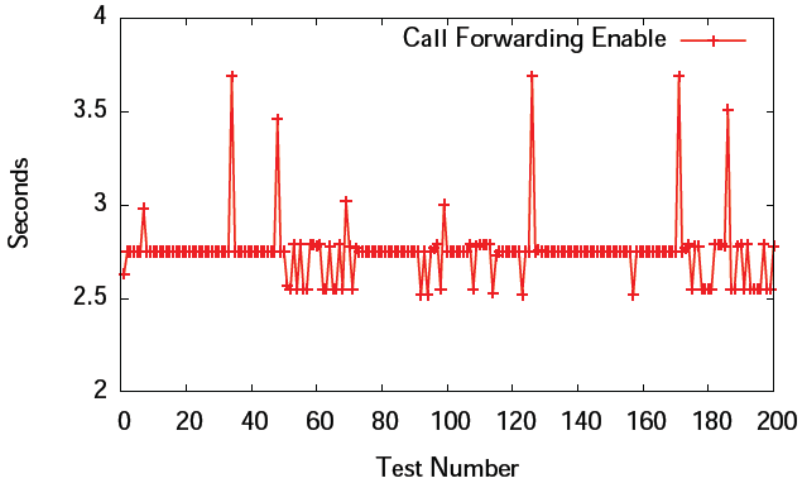
Response times for CW enable request



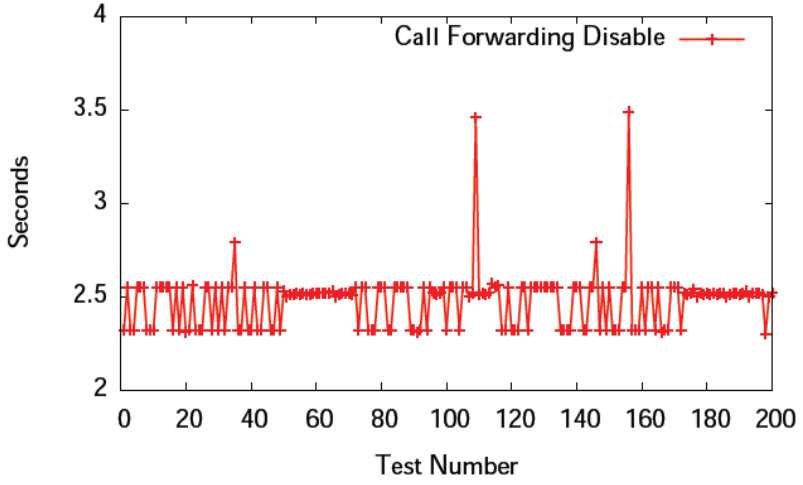
Response times for CW disable request

Profiling Network Behavior (4/4)

- **Insert/Delete Call Forwarding**
  - Redirecting incoming phone calls to other devices
  - The activation and deactivation of this service requires a single exchange with the HLR. Insert call forwarding performs additional checks and an extra database read
  - A good candidate for attack traffic: more expensive for the HLR compared to Update Subscriber Data



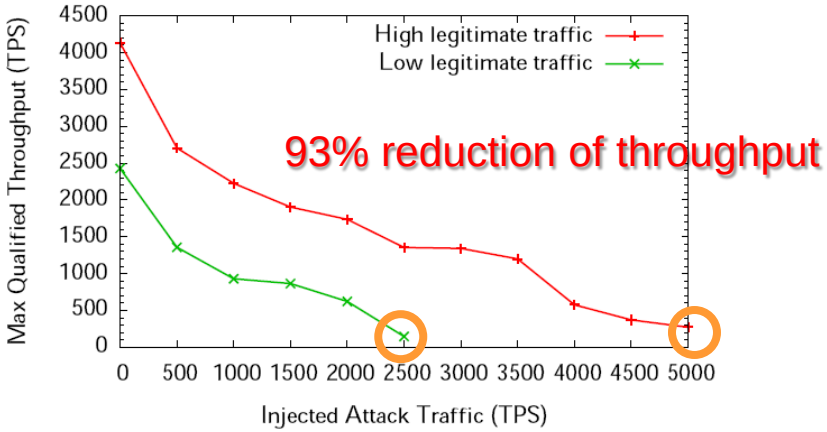
Response times for CF enable request



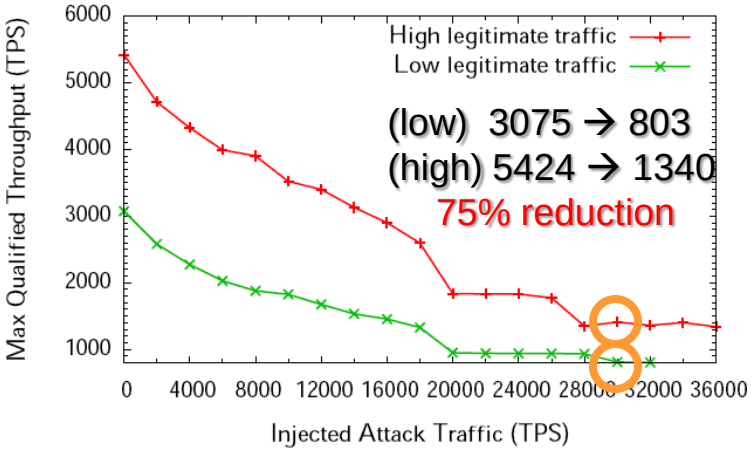
Response times for CF disable request

Attack Characterization (1/2)

- The optimum meta-command to attack HLR: insert_call_forwarding
- The number of requests (or infected devices) needed to degrade the HLRs throughput beyond a certain point to cause widespread outages
  - Modeling attacks by modifying TM1's client code (multi-threaded)
  - (low traffic) 2427 mix TPS → 146 mix TPS at attack rate of 2500 icf TPS
  - (high traffic) 4132 mix TPS → 274 mix TPS at attack rate of 5000 icf TPS



HLR running MySQL
supporting one million users



HLR running SolidDB
supporting one million users

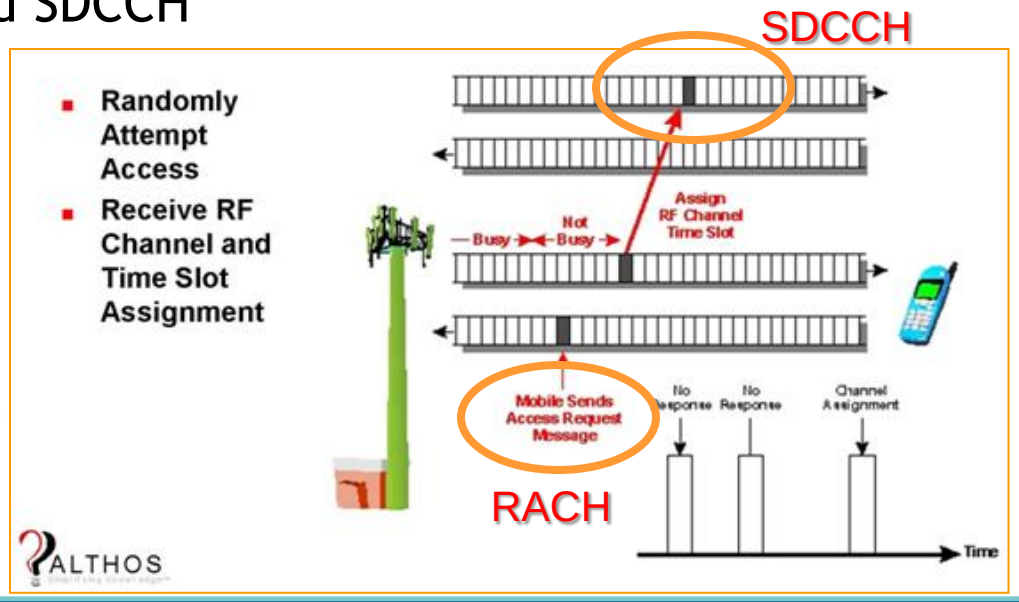
Attack Characterization (2/2)

- The number of devices an adversary requires to successfully launch an attack against an HLR
  - 4.7 second wait between the successful transmission of AT commands
  - HLR running the MySQL database under normal conditions
  - (low traffic) 11,750 infected phones
  - (high traffic) 23,500 infected phones
  - Assuming that each of these HLRs service one million users, only 1.2% and 2.4% rates of infection
  - 141,000, or an infection rate of 14.1% on an HLR running SolidDB

Avoiding Wireless Bottlenecks (1/3)

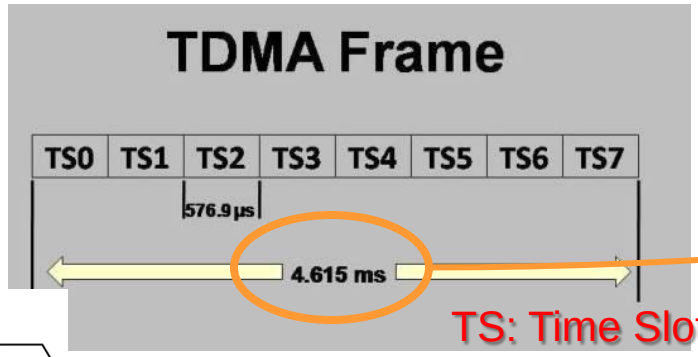
- With a realistic characterization of an attack on the wired portion of a cellular network, a number of obstacles to the successful execution of such an attack exist: wireless bottlenecks
  - GSM multiplexes traffic on a single frequency through the use of TDMA (time division multiple access): incurring collision
  - Therefore, Considering the limited capacity of two channels: RACH and SDCCH

Reference slide from "Introduction to GSM, 2nd ed"



Avoiding Wireless Bottlenecks (2/3)

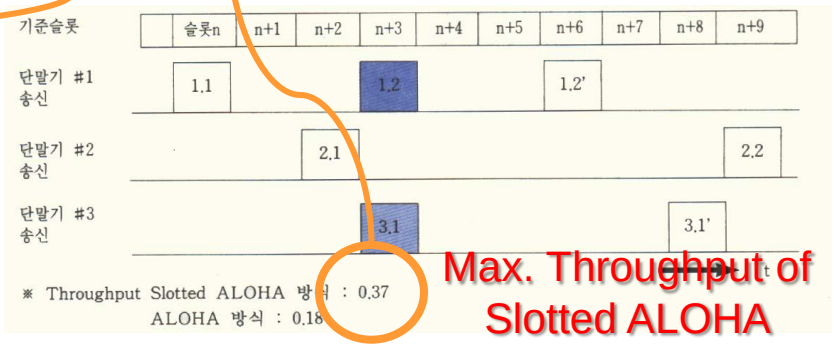
- RACH(Random Access CHannel) Capacity



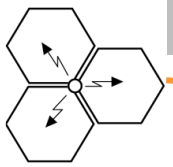
TS: Time Slot

Max # of Access Request:

(1000/4.615) * 0.37 ≒ 80



Max. Throughput of Slotted ALOHA



$$\alpha = \frac{5000 \text{ messages/sec}}{3 \text{ sectors/cell} * 80 \text{ RACH transmissions/sec}}$$

$$\alpha = 21 \text{ base stations}$$

→ Botnets must be well distributed over at least 23 base stations to send 5000 msg/sec

- If 3 areas per Base stations, 200 base stations per MSC, 10 MSCs per HLR , then network wide RACH capacity = 481,074 commands per second

Avoiding Wireless Bottlenecks (3/3)

- SDCCH(Standalone Dedicated Control Channels) Limitations
  - Sectors in a GSM network typically allocate 8 or 12 SDCCHs
  - Hold time of SDCCH channel based on experiment = 2.7 sec

$$\alpha = \frac{msgs/sec}{sectors * SDCCHs * \rho_{SDCCH}}$$

1 / 2.7

$$\alpha = \frac{5,000}{3 * 12 * 0.37} = 375 \text{ base stations}$$

  - 375 base stations will be needed to handle the air interface load of an attack: 14 or 13 botnets at most in a base station
  - Coordination of thousands of compromised phones and avoiding contention when high concentrations of such devices are present must therefore be considered

Command and Control from a botmaster

- Means of communicating with and coordinating the actions of compromised hosts to avoid the wireless bottlenecks
  - Internet Coordination: using number of Internet-capable phone
    - Reapplying current techniques. Ex. Polling a known communication channel, Peer-to-peer communication with time triggered techniques
    - Disadv: constrained by the architecture of the network (network bottelneck). easily identified and blocked by mobile operator
  - Local Wireless Coordination: using bluetooth or 802.11
    - Adv: no bottleneck, no monitoring
    - Disadv: communication range. Increasing the density of infected devices will increase contention for local resources
  - Indirect Local Coordination: modifying GSM back off algorithm

Attack Mitigation

- Meaningless defenses
  - Database replication
    - Useless against a large-scale attack
    - In particular, an attack targeting a large portion of the HLRs
  - Centrally located, highly capable HLRs
    - attacks may in fact be more likely to succeed
- Possible (useful) defenses
  - Filtering: blocking some functions
    - Ex: insert call forwarding is not critical to the basic functioning of the network
  - Call gapping: blocking calls for a period of time, periodically
    - a load control method for throttling telephone traffic on a telephone network when the network is overloaded
- Challenges: developing mechanisms intelligent enough to respond to a more dynamic attacks

Conclusion (1/2)

- This paper demonstrated that relatively small botnets pose significant threats to the availability of mobile network
  - Considered mobile network architecture, functions of HLR, wireless bottlenecks, command and control
  - Possible threat in near future
    - By mainly smart phones which lack relatively basic security mechanism compared to feature phones

News about security threats against smart phone

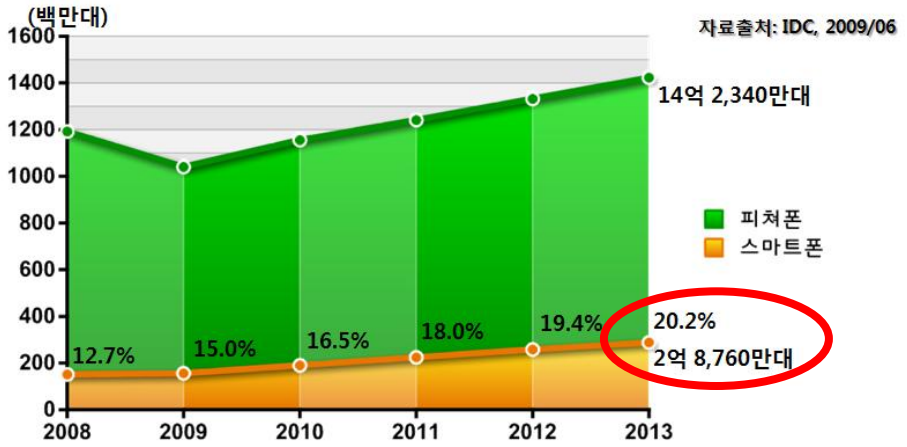
손 안의 PC '스마트 폰', 보안은?

모바일 악성코드 30개국 800건 발생…보안 대책 시급

2010년 03월 31일 (수) 21:36:16

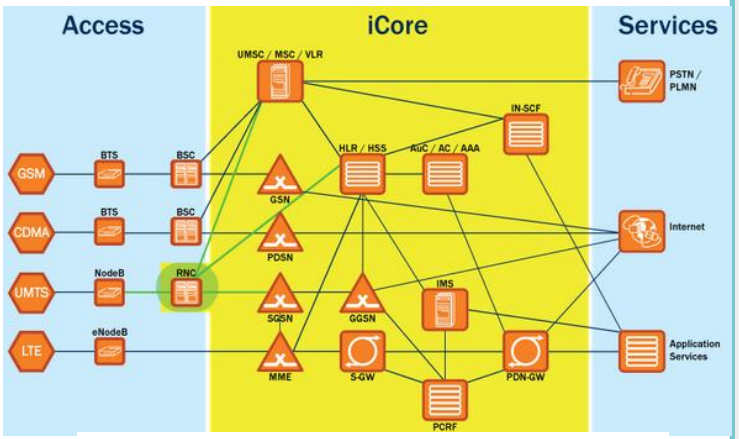
개방형OS 앱스토어 '보안이 문제'

등록일 2010.03.29 09:38:31 | 조회수 697



Conclusion (2/2)

- Attacks against CDMA ?
  - Similar properties of HLR
    - Authentication Mechanism is slightly different: no SIM card in CDMA
    - But features for attacks seem to be similar to those of GSM: database, structure of core network and call forwarding service
  - Less limitation of wireless bottlenecks
    - CDMA has more network capacity
    - Therefore, more compromised phones can be located within same area



Mobile Network Architecture (2G, 3G, 4G)

Question or Comment