# An Advanced Persistent Threat in 3G Networks: Attacking the Home Network from Roaming Networks


**Prof. Christos Xenakis**

***Systems Security Laboratory***

***Department of Digital Systems,***

***University of Piraeus, Greece***

# Our profile

- University of Piraeus, Greece
- Department of Digital Systems
- Systems Security Laboratory founded in 2008
- Research, Development & Education
  - systems security, network security
  - computer security, forensics
  - risk analysis & management

- MSc course on "Digital Systems Security" since 2009

# Publication – Press

- Christos Xenakis, Christoforos Ntantogian, **"An advanced persistent threat in 3G networks: Attacking the home network from roaming networks,"** *Computers & Security, Elsevier Science, Vol. 40, Issue 1, pp:84-94, February 2014*
- Jesse Emspak, **How Hackers Could Crash a Cellular Network**, *Tom's Guide, February 18, 2014*
  - http://news.yahoo.com/hackers-could-crash-cellular-network-183120897.html
  - http://www.secnews.gr/archives/75518
  - ……
- Bruce Schneier, **DDoSing a Cell Phone Network**, *Schneier on Security, February 26, 2014*
- **New Findings from University of Piraeus in the Area of Security Research**, *www.4-traders.com, March 19, 2014*.

# Outline

- Related work – our motivation
- Cellular technology
  - 3G network architecture
  - Identification, registration & authentication
- Experiments (1st & 2nd)
- The discovered attack
- Impact of the attack

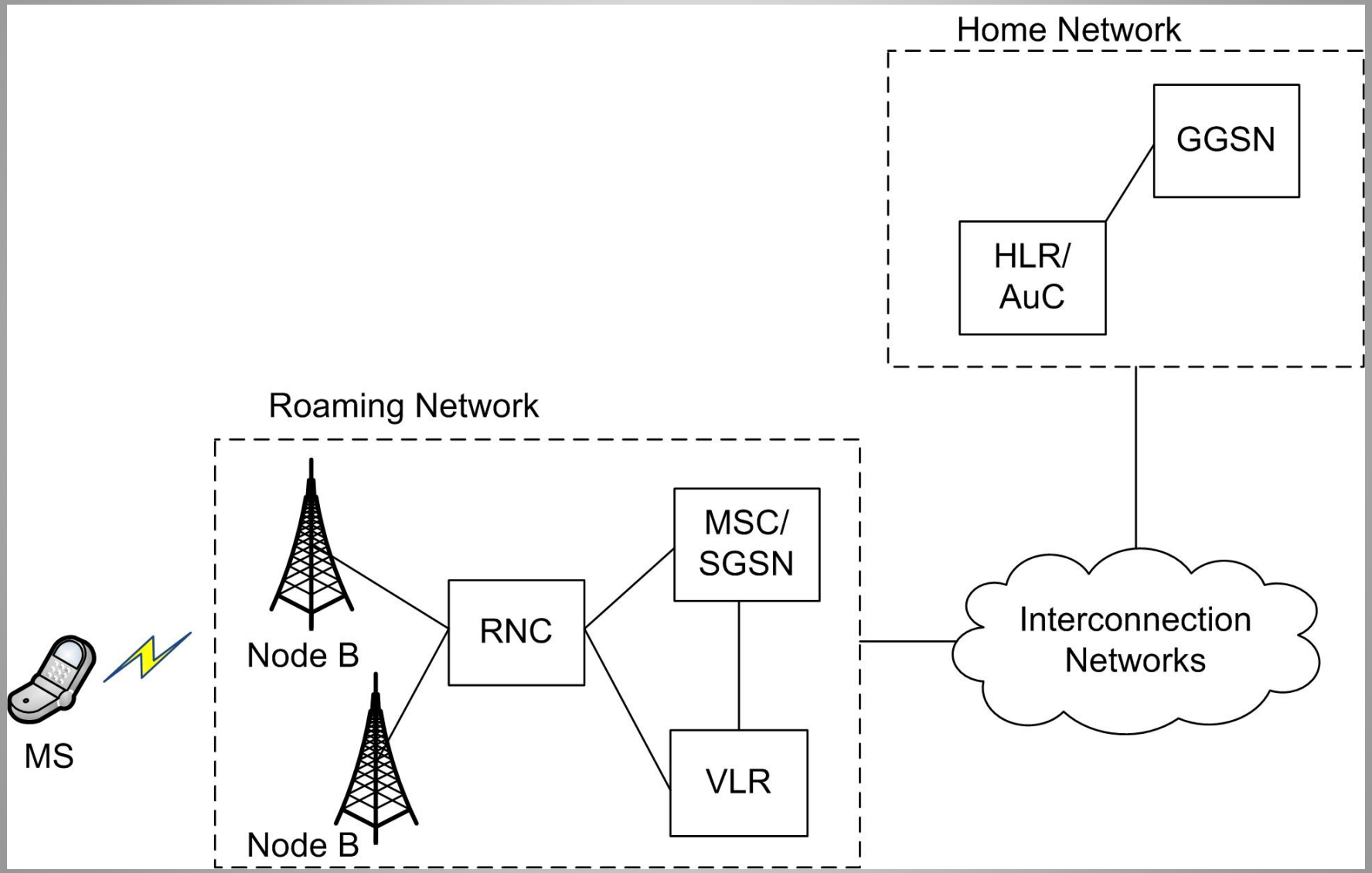
# Related work

- **Consume** the available control and signalling channels at the radio layer
- **DDoS** attack to HLR/AuC, coordinated by a botnet of infected mobile devices
- **SMS** DoS attack
- **Limitations → our motivation**
  - Studied only at a theoretical level
  - Their feasibility may be questionable
  - There are no technical details on how to practically exploit the discovered vulnerabilities

# In this work……

- We have proved the existence of a discovered 0-day vulnerability by carrying out an actual experiment on a mobile operator
- We exploit this 0-day vulnerability to perform a DDoS attack to HLR/AuC
- We have implemented the equipment for an adversary to launch the presented attack

# 3G Network Architecture



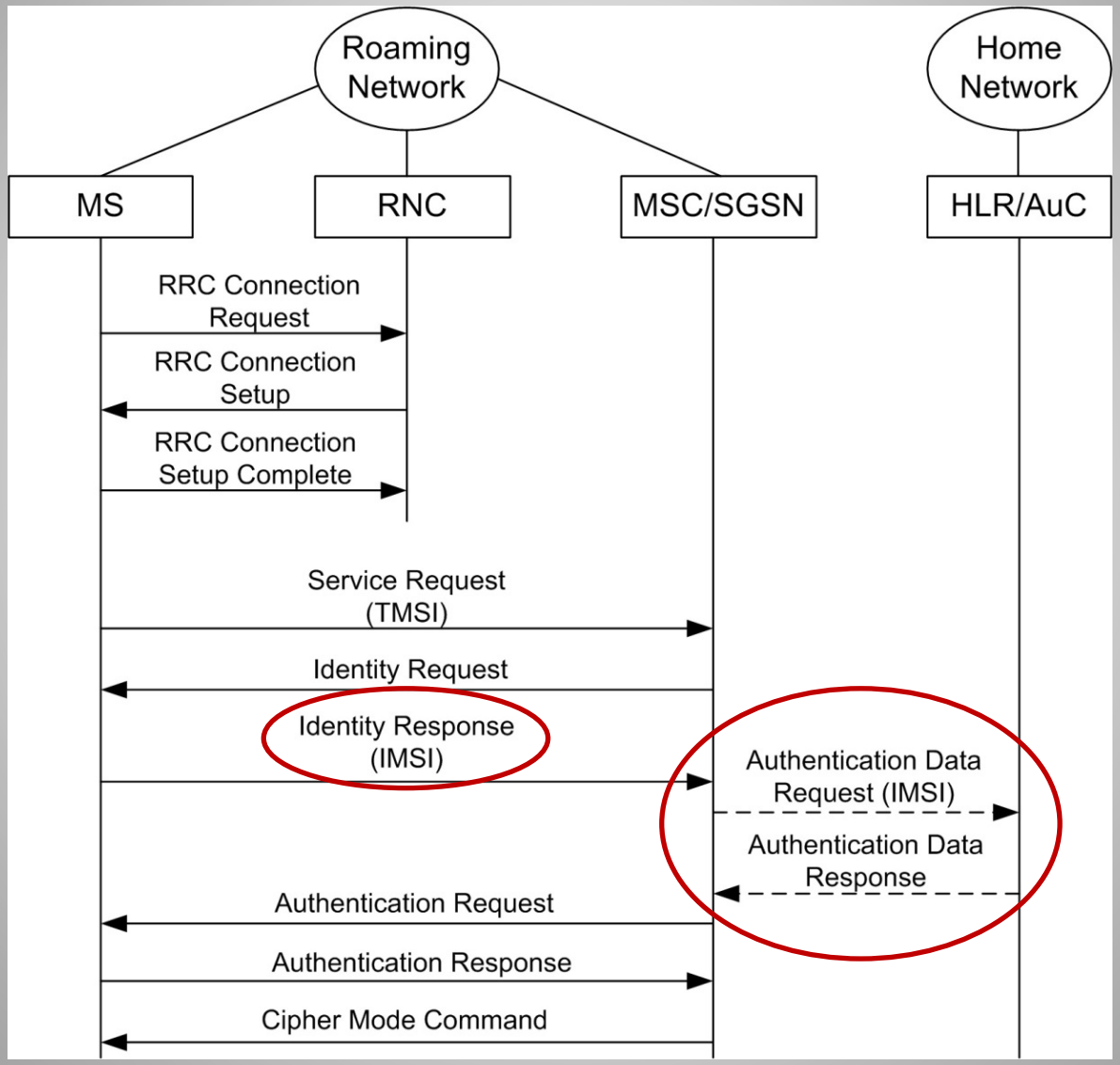
# Identification & Registration

- Each cellular subscriber is assigned a unique identity
  - International Mobile Subscriber Identity (IMSI)
  - For anonymity is identified by a Temporary Mobile Subscriber Identity (TMSI)
- Before a roaming user initiates a phone call/data session
  1. RRC (layer2) connection between MS and RNC.
  2. MS sends *service request* to the roaming MSC/SGSN including its TMSI
  3. The MSC/SGSN cannot recognize the received TMSI, the MS is forced to send the IMSI in plaintext.

# Registration & Authentication

- After that, the cellular network (roaming & home)
  1. The roaming MSC/SGSN initiates an **authentication data request (ADR)** to the home HLR/AuC.
  2. The home HLR/AuC generates L different authentication credentials named Authentication Vectors (AV).
  3. The home HLR/AuC sends AVs to the roaming MSC/SGSN.
  4. The roaming MSC/SGSN selects the first AV and sends it to MS for mutual authentication, while it caches the remaining (L-1) AVs for future use.

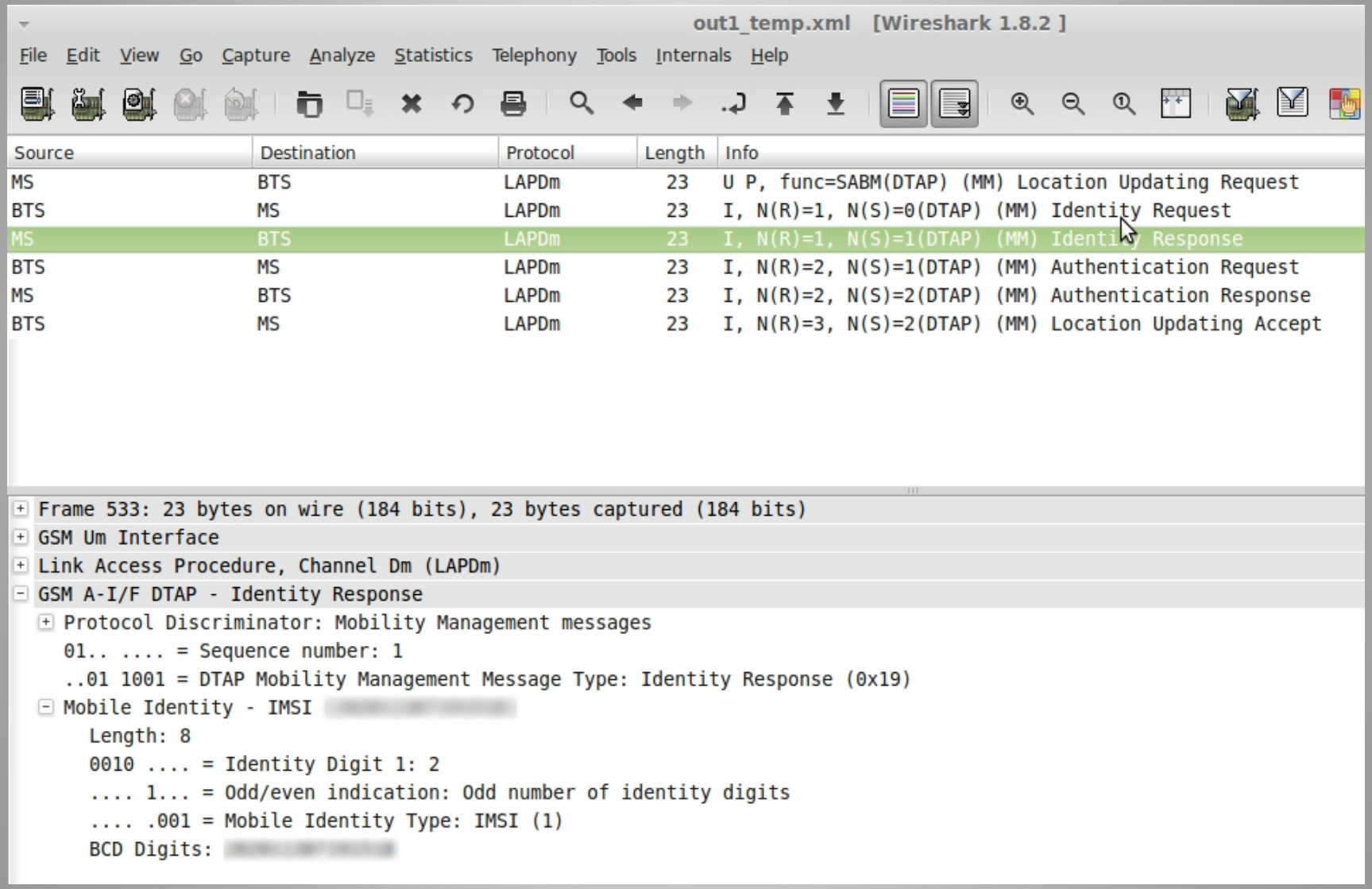
# Identification, Registration & Authentication



# 1st experiment

- **Goal**: Verify that the home HLR/AuC **always** accepts and proceeds an ADR from a roaming network.
- **Steps**:
  1. We cloned a SIM card of a Greek mobile operator
  2. We powered on a mobile device using the original SIM in Athens/Greece, and we initiated phone calls to register the IMSI of the SIM card in the HLR/AuC of its home network
  3. Then, powered on a mobile device with the cloned SIM in Lisbon/Portugal.
  4. Captured the network traffic using a tool named Nokia Net monitor.
  5. Analysed the captured packets using the protocol analyser Wireshark

# 1st experiment - Wireshark



# 2nd experiment

- **Goal**: Study the behaviour of the home network to various management procedures that **refer to already registered mobile subscribers to the network**, which are originated from other serving/roaming networks.
- **Steps**:
  1. We simultaneously made several outgoing calls using the two SIM cards.
  2. We made incoming calls to the cloned phone number
     - Both the cloned & the original SIM have the same number
  3. The mobile device that rang was the one that had made the last outgoing call

# The discovered DDoS attack

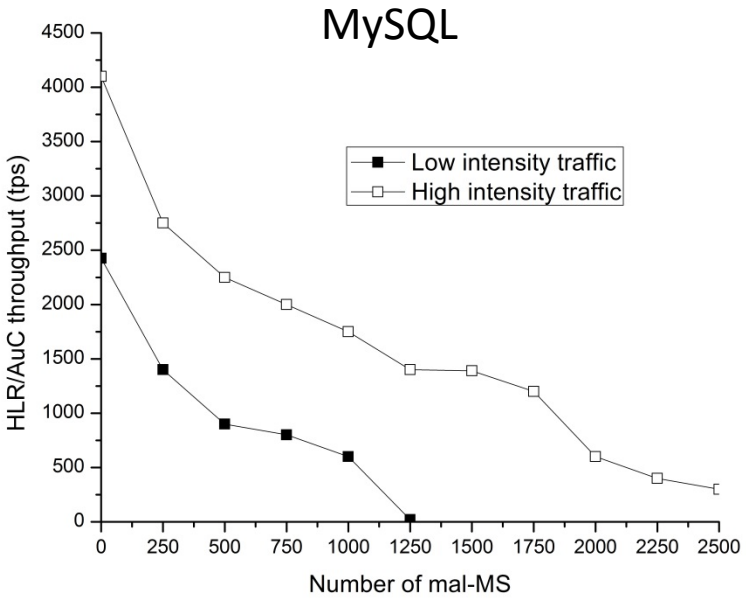
- The discovered a **DDoS** attack **aims to flood HLR/AuC**
  - The adversary first collects IMSIs of the targeted operator
  - A group of adversaries perform continuous registrations from roaming networks
  - Each registration attempt should use a different IMSI
- It is an **Advanced Persistent Threat (APT)** in cellular:
  1. Exploits a series of vulnerabilities of 3G networks.
  2. The adversaries can easily evade detection.
  3. Once launched it cannot be blocked in any trivial manner.

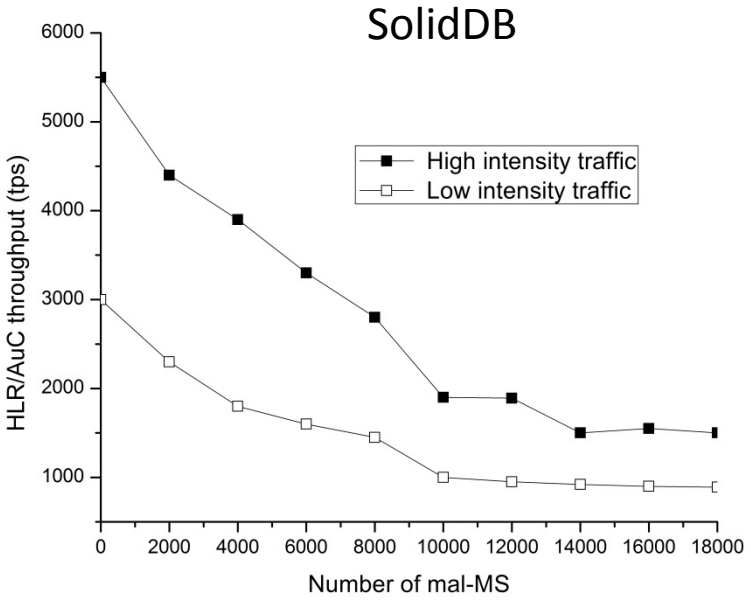
# Impact of the attack !

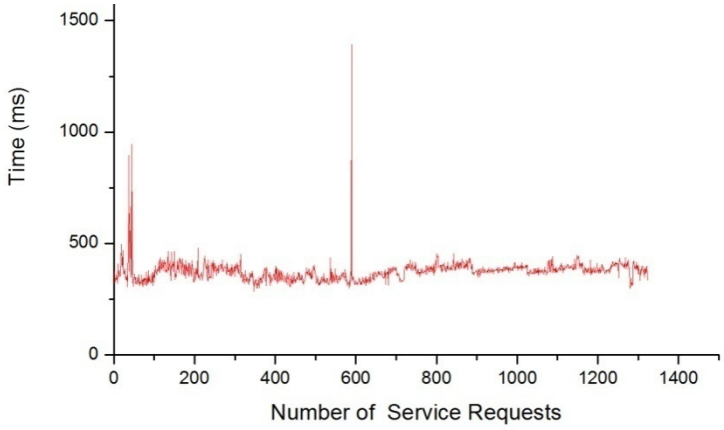
- The functionality of **HLR/AuC**
  - Delivery of all phone calls
  - Delivery of text messages
  - Authentication server
  - Billing
  - .....

- **Unavailability of HLR/AuC** → Devastate nearly **all services in the network** of the mobile operator.

# Impact of the attack !



# Thank you

# ?

UNIVERSITY
OF PIRAEUS

**Christos Xenakis**
***Systems Security Laboratory, Department of Digital Systems***
***University of Piraeus, Greece***
http://ssl.ds.unipi.gr/
http://cgi.di.uoa.gr/~xenakis/
email: xenakis@unipi.gr