Cellpot: A Concept for Next Generation Cellular Network Honeypots

Steffen Liebergeld, Matthias Lange and **Ravishankar Borgaonkar**

ravii@sec.t-labs.tu-berlin.de

SENT 2014 - 23 February, 2014 – San Diego CA, USA

Overview

- Cellular network attacks
- Honeypot works?
- Cellpot concept and architecture
- Applications for different stakeholders

Cellular networks under attack

- Cellular traffic network traffic growing exponentially
- Attacks against the network
  (Signaling DoS attacks on 2G, 3G, LTE)
- Attacks against end users
  (unwanted premium SMS, malware)
- Attack mitigation precludes ***knowledge*** about ongoing attacks

Honeypots

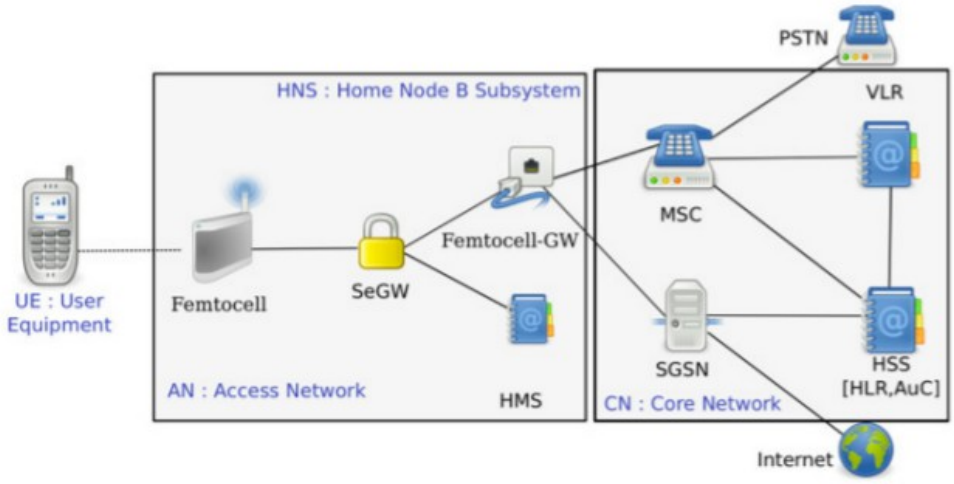
- Tool to detect ongoing attacks
- Simulate real machines/servers, but serve no real use
- Extensive logging of incoming traffic
- By definition ***all*** incoming traffic ***is malicious***

- ***Successfully used in IP networks***

- Does not fit our attacker model
- Need of new Honeypot for cellular network
- But location to deploy??

Cellular networks evolve

- Traditional base stations large, expensive to modify
- Small cell base station
- Low cost hardware, easy to deploy
- Acts like honeypots – stronger signal lures attackers



Cellpots: new Honeypot Concept

- Threat -
  - **Detection**
  - **Intelligence**
  - **Mitigation**
- Directly at the network perimeter (load balancing)
- Deployed on small cells
- 3 major components:
  1) Cellpot
  2) Peer to peer network
  3) Honeypot gateway server (HGS)

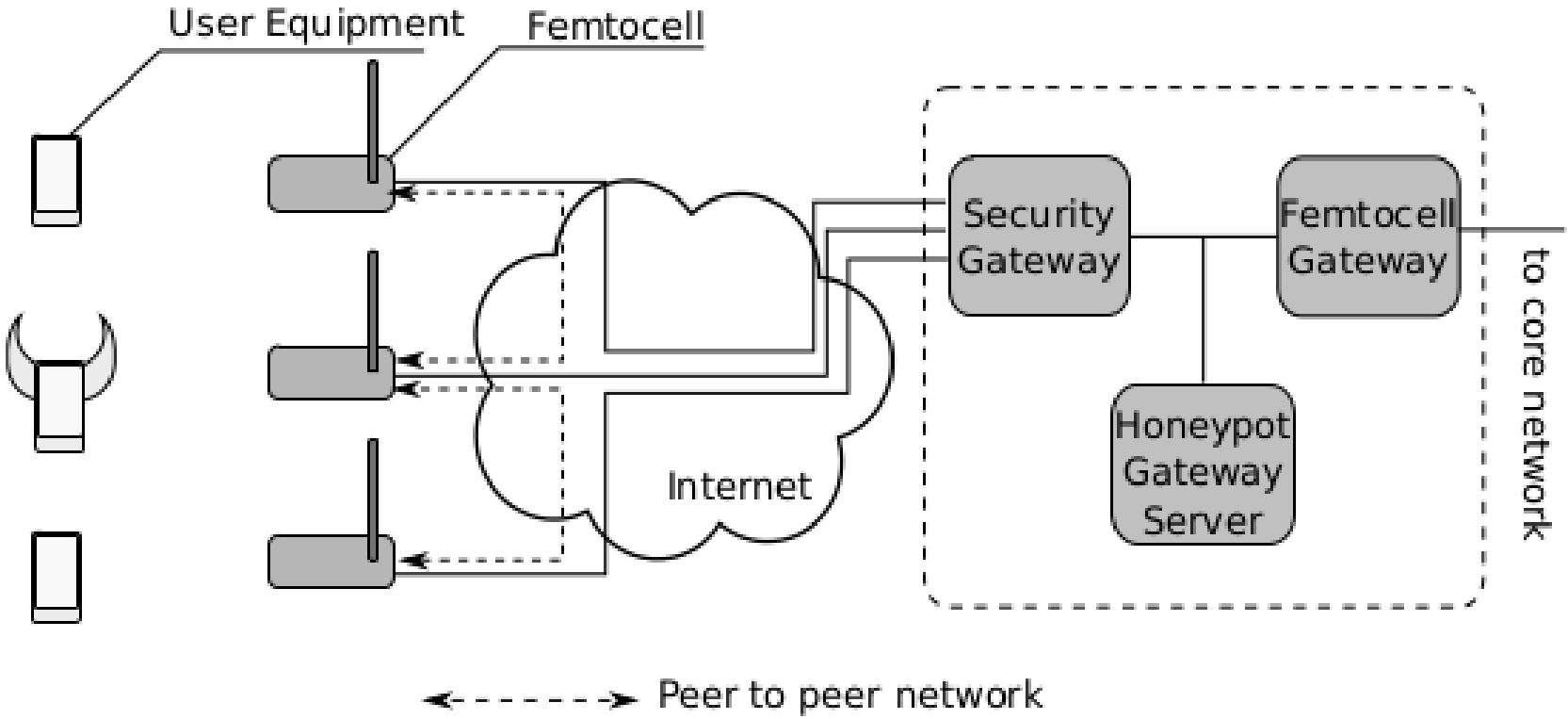
Cellpot

- Original small cell hardware with customized firmware
- Interposes between mobile devices and core network
- Hosts sensors to do
  - signaling traffic
  - anomaly detection
- Hosts countermeasures against threats
  - Rate limit signaling that goes to the core network
  - Filter expensive premium SMS
- Act as a honeypot:
  - Stronger signal lures attacker's device into connecting to cellpot instead of base station
- More on software architecture later on

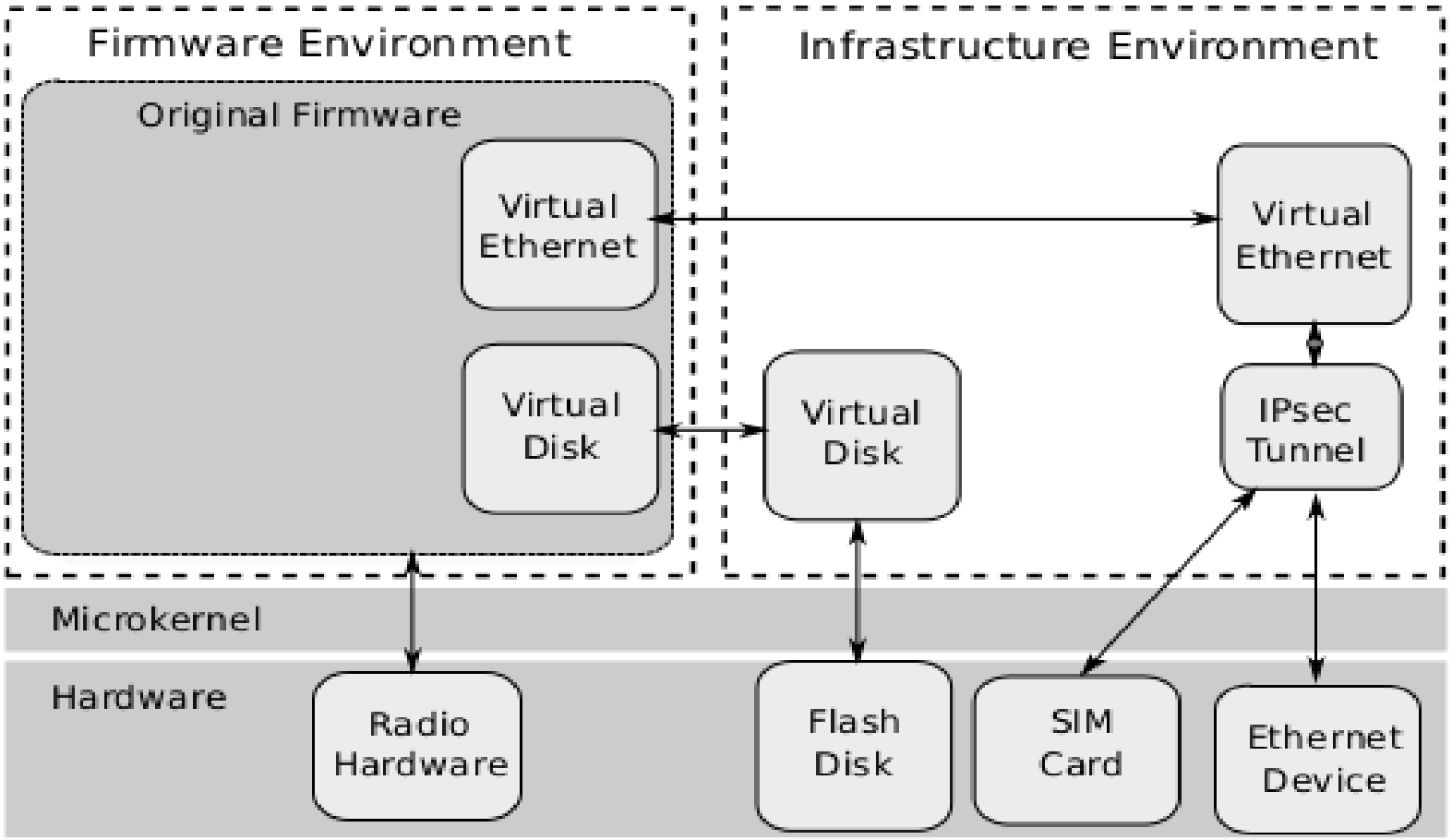
Peer to Peer Network and HGS

- Cellpots are interconnected with each other in **peer to peer fashion**
- Ease distribution of
  - Sensordata
  - Countermeasures
- Self-elected master nodes are being used to connect back with HGS
- **Honeypot Gateway Server** (HGS) is the central point of control for the MNO

Cellpot Architecture



Cellpot Software Architecture



Cellpot Software Architecture

- Based on modern third-generation microkernel
- Original firmware demoted into virtual machine
- Second VM hosts infrastructure
- Sensors and countermeasures can be updated quickly
- No re-certification of radio stack required
- Very little performance overhead

Cellpot Applications

- Overall benefit for carriers
  – minimize signaling overhead into core network

- SMS Spam Prevention
  - Block before SMSC, unlike in SMS filters
- Mobile Theft
  - EIR not effective, addition cost
- Malware and Phishing
  - anti-phishing framework on Cellpot

- Research tool for CERT, antivirus labs, security analyzers

Legal Issues

- User data raises privacy concerns
- Cellpot does not store data
- However, only subset of data transferred to the operator
- Solution: certified anonymizing algorithm
- Note: Operators already stores ALL user data under Lawful Interception procedure

Summary

- Introduced new concept for small cell honeypots
- Allows for threat detection and mitigation at the network perimeter
- Cheap hardware, easy to deploy
- Cellpots easy to update, no re-certification of radio stack need

Thank you!