## Overview

### Physical Security

- Self-Driving Car: Hyundai, KAIST
- Drone: Government, Korean Power, ...
- GyrosFinger: Fingerprinting Drones for... TOPS 2018
- Illusion and Dazzle: Adversarial Optical ... CHES 2017
- Sampling Race: Bypassing... Usenix WOOT 2016
- Rocking Drones with Intentional Sound... Usenix Sec 2015
- Ghost Talk ... Oakland 2013

### Blockchain and Cryptocurrency

- Samsung: Blockchain Application
- KAIST: Blockchain Seed Funding
- BOSCoin: Blockchain vulnerability Analysis
- Fickle Mining and other papers... In submission
- Be Selfish and Avoid Dilemmas ... ACM CCS 2017
- Doppelganger in Bitcoin... WISA 2016

### Embedded/OS/Web Security

- Industry: Samsung, SKT, Korean Power, Line, ...
- Government: NSR, KRF, MSIT
- Enabling Automatic Protocol..., ACM CoNEXT 2016
- Pikit: A New Kernel..., Usenix Sec 2016
- Taking Routers Off Their Meds, NDSS 2013

### Cellular/Mobile Security

- Industry: SKT (USIM, Core Network, ...), Samsung
- Government: MSIT, KISA, NSR
- Peeking over the Cellular Walled Gardens... TMC 2018
- GUTI Reallocation Demystified... NDSS 2018
- When Cellular Networks Met IPv6... EuroS&P 2017
- Breaking and fixing volte... ACM CCS 2015
- Gaining Control of Cellular... NDSS 2014
- Location leaks on the GSM... NDSS 2012
# Korea vs US

<table>
<thead>
<tr>
<th></th>
<th>US</th>
<th>Korea</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Annual Budget</strong></td>
<td>USD 200 K</td>
<td>USD 1.5 M</td>
</tr>
<tr>
<td><strong># students</strong></td>
<td>3</td>
<td>20</td>
</tr>
<tr>
<td><strong>Industry Funding</strong></td>
<td>0</td>
<td>At least 3/year</td>
</tr>
<tr>
<td><strong>Industry Relation</strong></td>
<td>Bad</td>
<td>Very close (small world)</td>
</tr>
<tr>
<td><strong>Teaching</strong></td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td><strong>Travel</strong></td>
<td>Almost none</td>
<td>3/week to Seoul (1 hour train)</td>
</tr>
<tr>
<td><strong>Call for Proposal</strong></td>
<td>Almost none</td>
<td>Frequently</td>
</tr>
<tr>
<td><strong>Government Funding</strong></td>
<td>Better Review (😊)</td>
<td>Terrible Review (Off-line only)</td>
</tr>
<tr>
<td><strong>Reporting</strong></td>
<td>Same # of pages</td>
<td>More pages for more funding</td>
</tr>
<tr>
<td><strong>Requirement</strong></td>
<td>Best Effort</td>
<td># papers, # patents, # of tech xfer</td>
</tr>
</tbody>
</table>
4G LTE Cellular Network Overview

- **User Equipment (phone, modem)**
- **HeNB**
- **eNodeB**
- **SGSN**
- **HSS**
- **MME**
- **S-GW**
- **P-GW**
- **PCRF**
- **Billing Domain**
- **IMS**
- **Internet**
- **Global Cellular Network**

**Key Components:**
- **SGSN**: Service GPRS Support Node
- **HSS**: Home Subscriber Server
- **MME**: Mobility Management Entity
- **S-GW**: Serving Gateway
- **P-GW**: PDN Gateway
- **PCRF**: Policy and Charging Rule Function
- **HeNB**: Home eNodeB
- **EPC**: Evolved Packet Core
Cellular Security

- A lot of systematic problems from cellular industry

- Standard has a lot of security problem itself.
- Device vendors are making a lot of mistakes.
- Cellular ISPs are making a lot of mistakes.
- New generation deployment for every 10 years
  - New system deployment for every 3-4 years.
- ISPs don’t talk to each other. They don’t respond to public scrutiny either.
  - Vendors don’t talk to each other.
Fake CMAS broadcast attack
VoLTE makes cellular network more complex

- Let’s check potential attack vectors newly introduced in VoLTE

- 3GPP standards

- IMS Bypassing

- Free Data Channels

- Device HW interface

- Accounting infrastructure

- LTE Core

- 4G Gateway

- IMS

- Permission Mismatch

- Mobile OS support?

- No Encryption

- No Session Manage

- No Auth

- Implementation of LTE core
Questions?

❖ Yongdae Kim
  - email: yongdaek@kaist.ac.kr
  - Home: http://syssec.kaist.ac.kr/~yongdaek
  - Facebook: https://www.facebook.com/y0ngdaek
  - Twitter: https://twitter.com/yongdaek
  - Google “Yongdae Kim”