Cell Phone Encryption

"Anyone remember the Clipper Chip?"

Stephen "ToxicSauce" Walker-Weinshenker

Department of Computer Science
Colorado State University

Department of Electrical and Computer Engineering
Colorado State University

November 28, 2016

Cell Phone Encryption
"Anyone remember the Clipper Chip?"
Stephen "ToxicSauce" Walker-Weinshenker
Department of Computer Science
Colorado State University
Department of Electrical and Computer Engineering
Colorado State University
November 28, 2016

Security News

Stephen "ToxicSauce" Walker-Weinshenker

- SF LR hacked
  `http://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomwar`
- Snoopers Charter
  `http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-inves html`
- MD5 poisoning `https://blog.silentsignal.eu/2016/11/28/an-update-on-md5-poisoning/`
- Shodan Membership $5
  `https://www.shodan.io/store/member`

Security News
- SF LR hacked http://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomwar
- Snoopers Charter http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-inves html
- MD5 poisoning https://blog.silentsignal.eu/2016/11/28/an-update-on-md5-poisoning/
- Shodan Membership $5 https://www.shodan.io/store/member

A brief history of cellphones

Stephen "ToxicSauce" Walker-Weinshenker

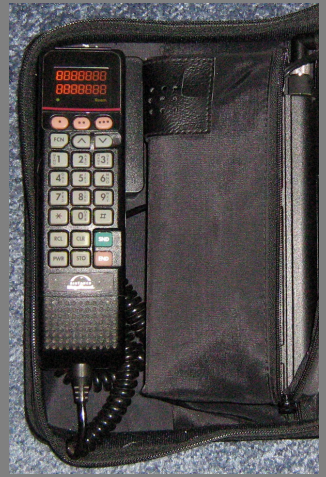
- Analog
  - 0G
  - 1G
  - bag phones
  - car phones
  - bricks
- Digital
  - CDMA
  - GSM
  - LTE
  - 4G?

A brief history of cellphones

- Analog
  - 0G
  - 1G
  - bag phones
  - car phones
  - bricks
- Digital
  - CDMA
  - GSM
  - LTE
  - 4G?

Analog

- 0G FM VHF half (later full) duplex (1946–2012)
  - large powerful towers that covered a long range
- 1G
  - smaller 'Cells'
  - digital signaling — analog voice
  - cellphone hackers — phone cloning and call interception
  - 800MHz blocking on scanners in US only

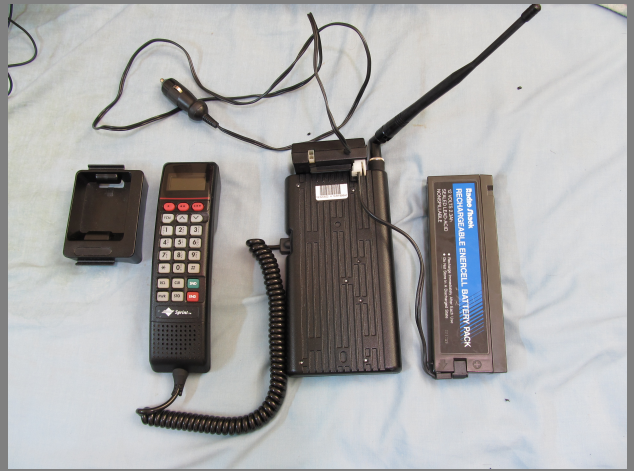


Analog

- 0G FM VHF half (later full) duplex (1946–2012)
  - large powerful towers that covered a long range
- 1G
  - smaller 'Cells'
  - digital signaling — analog voice
  - cellphone hackers — phone cloning and call interception
  - 800MHz blocking on scanners in US only

1. 0G only had 3 frequency pairs at first, everything was operator driven, mobile telephone service Bell/Motorola
2. this was later replaced by IMTS (1964) with the convience of **direct dial**
3. offered by both wireline common carriers and radio common carriers
4. IMTS had 25W at mobile station and 100–250W at base, unlike cellphones w/ 600mW
5. IMTS: limited number of customers, airtime expensive
6. 1G Advanced Mobile Phone System — started 1983 US no longer requiried by 2/2008
7. cloning involved recording the ESN/MDN and then adding it to another phone
8. 47cfr15.121

Bag Phone Full



Bag Phone Full

CDMA

Stephen "ToxicSauce" Walker-Weinshenker

- C Division Multiple Access
- Propriatary tech first developed by qualcom

CDMA
- C Division Multiple Access
- Propriatary tech first developed by qualcom