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 29, 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 29, 2016

Security News

- SF LR hacked
  http://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware
- Snoopers Charter
  http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-invest
  html
- MD5 poisoning https://blog.silentsignal.eu/2016/11/28/an-update-on-md5-poisoning/
- Shodan Membership $5
  https://www.shodan.io/store/member
- RMCCDC is a go
- .mil open to hacking
  https://krebsonsecurity.com/2016/11/dod-opens-mil-to-legal-hacking-within-limits/
- windoes Priv esc via update

2016-11-29 Cell Phone Encryption

└Security News

Security News

- SF LR hacked http://www.theverge.com/2016/11/27/13758412/hackers-san-francisco-light-rail-system-ransomware
- Snoopers Charter http://www.independent.co.uk/voices/snoopers-charter-theresa-may-online-privacy-invest html
- MD5 poisoning https://blog.silentsignal.eu/2016/11/28/an-update-on-md5-poisoning/
- Shodan Membership $5 https://www.shodan.io/store/member
- RMCCDC is a go
- .mil open to hacking https://krebsonsecurity.com/2016/11/dod-opens-mil-to-legal-hacking-within-limits/
- windoes Priv esc via update

A brief history of cellphones

Stephen "ToxicSauce" Walker-Weinshenker

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

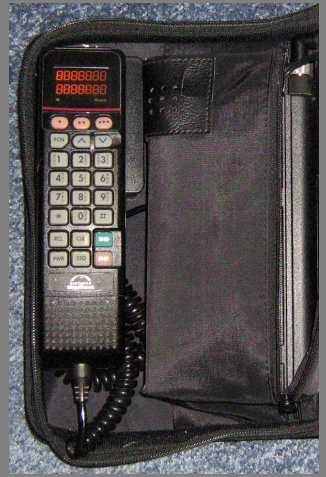
A brief history of cellphones

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

Analog

Stephen "ToxicSauce" Walker-Weinshenker

- 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

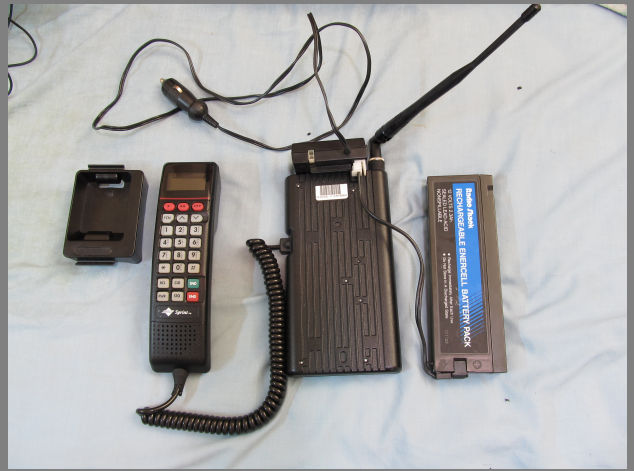


Analog
- 0G FM VHF half (later full) duplex (1946–2012)
  - large powerful towers that covered a long range
- 1G
  - smaller 'Cells'
  - digital signaling — analog voice
  - cellphone hackers — phone cloning and call interception
  - 800MHz blocking on scanners in US only

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

Stephen "ToxicSauce" Walker-Weinshenker



Bag Phone Full

CDMA

Stephen "ToxicSauce" Walker-Weinshenker

- Code Division Multiple Access
- Propriatary tech first developed by qualcom, later standardized
- Used primarily in US and South Korea, later migrated to Europe and Asia
- 2G was cdmaOne, 3G is CDMA2000 / EVDO (data) / 1x (voice)
- 2G not encrypted?, 3G is

1. does not limit number of active radios

CDMA

- Code Division Multiple Access
- Propriatary tech first developed by qualcom, later standardized
- Used primarily in US and South Korea, later migrated to Europe and Asia
- 2G was cdmaOne, 3G is CDMA2000 / EVDO (data) / 1x (voice)
- 2G not encrypted?, 3G is

GSM

Stephen "ToxicSauce" Walker-Weinshenker

- Time Division Multiple Access (2G) and CDMA (3G)
- 'open' standard
- Primarily deployed in Europe and Asia, but now deployed across world
- had support for encryption
- 2.5G is EDGE
- 3G is UMTS

1. TDMA limits number of active radios per cell

GSM

- Time Division Multiple Access (2G) and CDMA (3G)
- 'open' standard
- Primarily deployed in Europe and Asia, but now deployed across world
- had support for encryption
- 2.5G is EDGE
- 3G is UMTS

LTE

Stephen "ToxicSauce" Walker-Weinshenker

- Not 4G yet
- same system for both CDMA and GSM based carriers.

LTE

- Not 4G yet
- same system for both CDMA and GSM based carriers.

CDMA encryption

Stephen "ToxicSauce" Walker-Weinshenker

- CAVE (Cellular Authentication and Voice Encryption)
- CDMA2000 and related 3G tech uses 64 bit primary key along w/ 128 bit shared secret

CDMA encryption
- CAVE (Cellular Authentication and Voice Encryption)
- CDMA2000 and related 3G tech uses 64 bit primary key along w/ 128 bit shared secret

1. primary key only used to generate shared secret which is used for signing and auth
2. shared secret is actually 2 64 bit keys, one for auth signatures and one for session key gen

GSM encryption

Stephen "ToxicSauce" Walker-Weinshenker

- uses A5/1 A5/2 and A5/3 stream ciphers for voice
- GPRS uses GEA/1, GEA/2 (vulnerable) and GEA/3 (secure?)
- most countries do not encrypt GPRS data for snooping porpises
- A5/1 has 54 bit key, originally going to be 128 but Germans
- A5/2 is same as A5/1 but without irregular clocking, used for export
- A5/3 aka KASUMI used in 3G GSM
- All three of these are broken.

GSM encryption

- uses A5/1 A5/2 and A5/3 stream ciphers for voice
- GPRS uses GEA/1, GEA/2 (vulnerable) and GEA/3 (secure?)
- most countries do not encrypt GPRS data for snooping porpises
- A5/1 has 54 bit key, originally going to be 128 but Germans
- A5/2 is same as A5/1 but without irregular clocking, used for export
- A5/3 aka KASUMI used in 3G GSM
- All three of these are broken.

1. irregular clocking: essentially randomly chooses shift registers

GSM encryption

Stephen "ToxicSauce" Walker-Weinshenker

- A5/1 is vulnerable to known-plaintext attacks with rainbow tables
- A5/2 is vulnerable to known-ciphertext attacks
- both of these can be decrypted in realtime by a 1999 era desktop PC

¡WARNING!

Currently, decrypting GSM traffic using these methods are illegal

GSM encryption

- A5/1 is vulnerable to known-plaintext attacks with rainbow tables
- A5/2 is vulnerable to known-ciphertext attacks
- both of these can be decrypted in realtime by a 1999 era desktop PC

¡WARNING!
Currently, decrypting GSM traffic using these methods are illegal

Clipper Chip

Stephen "ToxicSauce" Walker-Weinshenker

Clipper Chip

References

[allowframebreaks] https://en.wikipedia.org/wiki/Mobile_Telephone_Service https://en.wikipedia.org/wiki/Improved_Mobile_Telephone_Service https://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System https://en.wikipedia.org/wiki/0G https://en.wikipedia.org/wiki/1G http://www.arrl.org/forum/topics/view/112 https://upload.wikimedia.org/wikipedia/en/4/46/Motorola2950.jpg https://upload.wikimedia.org/wikipedia/commons/0/06/Motorola_Bag_Phone_Outside_Bag.JPG https://en.wikipedia.org/wiki/2G https://en.wikipedia.org/wiki/CDMA2000 https://www.cdg.org/resources/files/white_papers/Qualcomm_Security_Provisions_in_CDMA2000_Networks_

References

[allowframebreaks] https://en.wikipedia.org/wiki/Mobile_Telephone_Service https://en.wikipedia.org/wiki/Improved_Mobile_Telephone_Service https://en.wikipedia.org/wiki/Advanced_Mobile_Phone_System https://en.wikipedia.org/wiki/0G https://en.wikipedia.org/wiki/1G http://www.arrl.org/forum/topics/view/112 https://upload.wikimedia.org/wikipedia/en/4/46/Motorola2950.jpg https://upload.wikimedia.org/wikipedia/commons/0/06/Motorola_Bag_Phone_Outside_Bag.JPG https://en.wikipedia.org/wiki/2G https://en.wikipedia.org/wiki/CDMA2000 https://www.cdg.org/resources/files/white_papers/Qualcomm_Security_Provisions_in_CDMA2000_Networks_