Cellphone Security

David Wagner

U.C. Berkeley

daw@cs.berkeley.edu

Organization

- Analog cellphones: historical notes
- US digital cellphones
- European digital cellphones (GSM)

In the beginning. . .

- Earliest cellphones were just a two-way radio.
  - Gave you nothing more than a voice channel to Ma Bell.
  - You told the operator the phone number and your billing information, and the operator connected you.
  - No handoff, no roaming, nothing fancy.

In the beginning. . .

- Earliest cellphones were just a two-way radio.
  - Gave you nothing more than a voice channel to Ma Bell.
  - You told the operator the phone number and your billing information, and the operator connected you.
  - No handoff, no roaming, nothing fancy.
- Security:
  - Engineers assumed specialized receivers too expensive to pose any real threat—and they were right.
  - With that caveat, you were safe.

Automated billing

- Second generation soon arrived:
  - Each cellphone given a MIN/ESN pair.
    - ESN: 32-bit serial number, “burned” into cellphone
    - MIN: your phone number
  - During call origination or registration, cellphone sends MIN/ESN pair to base station for billing purposes.

Automated billing

- Second generation soon arrived:
  - Each cellphone given a MIN/ESN pair.
    - ESN: 32-bit serial number, “burned” into cellphone
    - MIN: your phone number
  - During call origination or registration, cellphone sends MIN/ESN pair to base station for billing purposes.
- Security:
  - No worse than before…
  - Scanners still assumed to be too expensive.

Roaming

- Strong motivation to support inter-provider roaming
  - Consumers clamored for it!

Roaming

- Strong motivation to support inter-provider roaming
  - Consumers clamored for it!
- Security:
  - How to reconcile billing betw. remote & home provider?
  - Reconcile after fact?

Roaming

- Strong motivation to support inter-provider roaming
  - Consumers clamored for it!
- Security:
  - How to reconcile billing betw. remote & home provider?
  - Reconcile after fact?
  - Bad idea: too easy to cheat the system!
  - Detect cheaters & share blacklists between providers?

Tumbling

- Exploit lack of realtime authentication:
  - At one point, default was to accept roaming users, and blacklist misbehaviors after they're discovered.
  - Thus, the first call always went through when roaming.

Tumbling

- Exploit lack of realtime authentication:
  - At one point, default was to accept roaming users, and blacklist misbehaviors after they're discovered.
  - Thus, the first call always went through when roaming.
  - *And that call could last a long time. . .*

Tumbling

- Exploit lack of realtime authentication:
  - At one point, default was to accept roaming users, and blacklist misbehaviors after they're discovered.
  - Thus, the first call always went through when roaming.
  - *And that call could last a long time. . .*
- Attack: *tumbling phones*
  - Pick a new MIN/ESN pair at random for each call

Cloning

How to clone a cellphone:

1. Obtain a valid MIN/ESN pair.
   - Usually with the aid of a scanner.
2. Program that into your handset.
3. Call for free.

Cloning in practice

- Cloning attacks became very sophisticated
  - Black boxes automate the process, cheaply
  - Cloners harvest many MIN/ESN pairs from airports, highways
  - Stealthy cloning: combine with tumbling and/or roaming
- Cloning became a serious problem
  - Big players: Underground call-sell operations, anonymity-loving criminals
  - US industry loses $\approx$ \$650 million / year.
  - Perhaps 5% of all calls were fraudulent, as of 1995. (And in Oakland on Friday night, reportedly 60%–70%.)

Scanners & voice privacy

- Scanners became widely available
  - Mass-market items: $\approx$ \$300 @ Radio Shack
  - Range in miles, can scan many channels quickly

Scanners & voice privacy

- Scanners became widely available
  - Mass-market items: $\approx$ \$300 @ Radio Shack
  - Range in miles, can scan many channels quickly
- This became a serious privacy problem
  - $\approx$ 10-15 million scanners sold
  - $\approx$ 50 million users

$\Rightarrow$ *It seems plausible that the majority of analog cellphone users have had one of their calls intercepted at some point.*

Summary on analog cellphones

- Everything that could go wrong, has.
  - Threat models changed out from under the designers
  - Deployment scaled up; security architectures didn't
  - We've trained & funded a large criminal underground in cellphone hacking
- Analog systems are now totally insecure

Part II: US Digital Cellphones

Who's trusted?

- Internal network, PSTN
- Legitimate users and their handsets
- Roaming partners
- The crypto

Who's trusted?

- Internal network, PSTN
- Legitimate users and their handsets $\rightsquigarrow$ fraudulent!
- Roaming partners $\rightsquigarrow$ untrustworthy!
- The crypto $\rightsquigarrow$ broken!

The crypto

- CAVE: authentication and key derivation
- XOR mask: voice encryption
- CMEA: control channel encryption
- ORYX: wireless data encryption

The crypto

- CAVE: authentication and key derivation

  ⇝ no attacks known

- XOR mask: voice encryption

  ⇝ breakable in realtime via ciphertext-only attack [B92]

- CMEA: control channel encryption

- ORYX: wireless data encryption

The crypto

- CAVE: authentication and key derivation
  - $\rightsquigarrow$ no attacks known
- XOR mask: voice encryption
  - $\rightsquigarrow$ breakable in realtime via ciphertext-only attack [B92]
- CMEA: control channel encryption
  - $\rightsquigarrow$ breakable in hours via known-plaintext attack [WSK97]
- ORYX: wireless data encryption
  - $\rightsquigarrow$ breakable in seconds, ciphertext-only attack [WSDKMS98]

Bypassing the crypto

- Attack #1: Look for plaintext
  - Encryption is rarely, if ever, enabled

Bypassing the crypto

- Attack #1: Look for plaintext
  - Encryption is rarely, if ever, enabled

    $\rightsquigarrow$ Can snoop on calls, credit card numbers, . . .

Bypassing the crypto

- Attack #1: Look for plaintext
  - Encryption is rarely, if ever, enabled

    $\leadsto$ Can snoop on calls, credit card numbers, . . .
- Attack #2: Check for known keys
  - Many handset manufacturers use all-zeros keys

    (key management considered too expensive)

Bypassing the crypto

- Attack #1: Look for plaintext
  - Encryption is rarely, if ever, enabled

    $\rightsquigarrow$ Can snoop on calls, credit card numbers, ...
- Attack #2: Check for known keys
  - Many handset manufacturers use all-zeros keys

    (key management considered too expensive)

    $\rightsquigarrow$ Can make fraudulent calls, intercept other calls

Bottom line: it all relies on lack of digital scanners

Part III: European Digital Cellphones: GSM

A trust analysis

Who’s trusted?

- Internal network, PSTN
- Legitimate handsets
- The crypto

Who’s not? (mostly)

- Roaming partners
- Owners of legitimate handsets

A trust analysis

Who’s trusted?

- Internal network, PSTN
- Legitimate handsets $\rightsquigarrow$ unreliable
- The crypto $\rightsquigarrow$ mostly broken

Who’s not? (mostly)

- Roaming partners
- Owners of legitimate handsets

The crypto (GSM)

- A3/A8: end-to-end authentication and key derivation
- A5/1, A5/2, A5/0: voice & control channel encryption

The crypto (GSM)

- A3/A8: end-to-end authentication and key derivation

  $\rightsquigarrow$ breakable with 2^{17} chosen plaintexts ($\approx$ 8 hours) [BGW98]

- A5/1, A5/2, A5/0: voice & control channel encryption

The crypto (GSM)

- A3/A8: end-to-end authentication and key derivation
  - $\rightsquigarrow$ breakable with 2^{17} chosen plaintexts ($\approx$ 8 hours) [BGW98]
- A5/1, A5/2, A5/0: voice & control channel encryption
  - $\rightsquigarrow$ A5/0: no security
  - $\rightsquigarrow$ A5/2: breakable in realtime [BGW99]
  - $\rightsquigarrow$ A5/1: breakable in practice, with non-trivial effort [BSW00]

Bypassing the crypto

- Bypassing the crypto in GSM is not so easy
  - Same party handles both SIMs and Authentication Service
    $\rightsquigarrow$ They got the key management right
  - And they tend to be good at details like PIN management
- Some risks exist, though
  - Many providers put so much trust in the crypto that they didn’t bother with a second line of defense
  - And there are some protocol attacks

Comparing the systems

Standard	Security	
	Anti-fraud	Privacy
Analog	Terrible	Terrible
GSM	Mediocre	Poor
US digital	Mediocre*	Bad

(*) Poor when digital scanners become prevalent, better if industry introduces strong keying.

Note. A digital cellphone is no panacea: they're often dual-mode and will fall back to analog outside of digital coverage areas.

Lessons for infrastructure analysis?

- Questions for security evaluation:

  Whom do you trust?

  What is your threat model?

  How will bad guys be thinking?

- Public scrutiny *works*
  - Flaws found within days/months of public release of standards

  $\leadsto$ public standards permit early debugging

Summary

- Think of your cellphone as a party line
  - Analog cellphone systems widely exploited
  - Digital cellphone systems have many weaknesses; not widely exploited today, but the future is unpredictable
- Technologically, fixes are not hard
  - But the political realities and the economics of deployment are big barriers
- Strong cellphone security is a long way off. . .