The road to 5G security

Prof. Steve Babbage
Vodafone Distinguished Engineer
Contents of my talk

• The evolution of mobile security: 1G, 2G, 3G, 4G
• What is 5G anyway?
• New security improvements in 5G
• New areas of risk
• Work in progress
Cryptography in mobile phone networks
First generation analog phones
GSM security architecture

Visisted network

Home network

SIM

RAND, XRES, K_C

RAND

RES = XRES?

Encryption algorithm A5

RAND

Ki

AKA

RES

K_C

K_C

AKA

Ki

RES

K_C

RAND

Authentication and cipher key generation algorithm

ENCRYPT USING K_C
GSM security architecture

- Home network
- Visited network

Authenticate

Established shared session key

Session key

ENCRYPT

Authentication vector
Block ciphers and stream ciphers

Plaintext (128 bits) → Key → Ciphertext (128 bits) → Key → Plaintext

One bit error

Plaintext (any length) → Key → Ciphertext → Key → Plaintext

|=|
The SIM

- A miniature “hardware security module”
- Well made SIMs, with strong algorithms, remain highly resistant to attack
Some limitations of GSM security

• The goals of GSM security
• Key length
• One-way authentication
• Weak (“export”) crypto algorithms, initially
One-way authentication

TWO GUYS FROM QUANTICO
PIZZA
GSM algorithms

• Encryption algorithm must be standardised — operators can’t do their own thing

• Various algorithms: A5/0 (no encryption), A5/1, A5/2, A5/3, …
  – Always stream ciphers

I support:

\[\begin{align*}
A5/0 \\
A5/1 \\
A5/2
\end{align*}\]

Encrypt with A5/1

• Authentication and key agreement algorithm need not be standardised
  – More on this later
A5/1 attacks

• Several academic attacks from 1994 onwards
  – Guess-and-determine attacks
  – Statistical attacks
  – Algebraic attacks

• Time-memory-data trade-off attacks from 1995 onwards

• There’s also A5/2
  – For when A5/1 is too strong(!)
A protocol problem
The Barkan-Biham-Keller attack — eavesdropping

Enough to break A5/1 and recover cipher key; now attacker has cipher key and can decrypt recorded call
The Barkan-Biham-Keller attack

- Exploits weak encryption algorithms
- Exploits ability to manipulate signalling …
  - So let's add that to our list of GSM security limitations
3G, 4G
3G security architecture

Authenticate

Established shared session keys

Session keys

ENCRYPT TRAFFIC

ENCRIPT & INTEGRITY

PROTECT SIGNALLING

Authentication vector

Visited network

Home network

Prove it came from home network

Prove it’s fresh

Stronger (and public) algorithms, 128-bit keys
Barkan-Biham-Keller and 3G

Network

Victim mobile

Attacker

RAND

RES

Start ciphering with A5/3

Phone call

K_C

K_C

Same RAND

RES

Start ciphering with A5/1

“OK”, encrypted with A5/1

repeated several times

“OK”, encrypted with A5/1

Enough to break A5/1 and recover cipher key; now attacker has cipher key and can decrypt recorded call
Defining – and deploying – new GSM algorithms
New, strong, public GSM algorithm

3G encryption algorithm UEA1

GSM encryption algorithm A5/3
So now we can replace A5/1 with A5/3 …
## GSM encryption algorithm status

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>A5/2</td>
<td>Abandoned</td>
</tr>
<tr>
<td>A5/1</td>
<td>Common - sometimes with countermeasures</td>
</tr>
<tr>
<td>A5/3</td>
<td>Growing - now in all Vodafone markets</td>
</tr>
<tr>
<td>A5/4</td>
<td>Testing</td>
</tr>
</tbody>
</table>
Radio interface algorithms in 3G

- UEA1, UIA1 (already mentioned)
- UEA2, UIA2
  - Based on a stream cipher called SNOW 3G, developed from SNOW 2.0

Both mandatory from day one
Authentication and key agreement algorithms
Operators can choose their own … but:

• COMP128
• COMP128-2, COMP128-3
• MILENAGE
Vodafone dual algorithm

Authentication Centre

SIM manufacture SIM

K

h1

K1

MILENAGE

h2

K2

BRUT
# Evolution of security

<table>
<thead>
<tr>
<th>2G</th>
<th>3G</th>
<th>4G</th>
</tr>
</thead>
<tbody>
<tr>
<td>Key length</td>
<td>Increase to 128 bits</td>
<td></td>
</tr>
<tr>
<td>Oneway authentication</td>
<td>Mutual authentication, tamper-proof signalling</td>
<td>Proves which network</td>
</tr>
<tr>
<td>Authentication and key agreement algorithms</td>
<td>Much better example algorithm</td>
<td></td>
</tr>
<tr>
<td>Encryption algorithms</td>
<td>Full strength public algorithms</td>
<td></td>
</tr>
<tr>
<td>Same cipher key, whatever the algorithm</td>
<td></td>
<td>Different cipher key depending on choice of algorithm</td>
</tr>
</tbody>
</table>
Radio interface algorithms in 3G / 4G

3G
- UEA1, UIA1 (already mentioned)
- UEA2, UIA2
  - Based on a stream cipher called SNOW 3G, developed from SNOW 2.0

Both mandatory from day one

4G
- EEA1, EIA1
  - Identical to UEA2 and UIA2
- EEA2, EIA2
  - Standard constructions based on AES
- EEA3, EIA3
  - China specials!

Both mandatory from day one
SIM evolution
Embedded SIM

Image from ETSI slides by Dr Klaus Vedder, G&D
Authentication and key agreement algorithms (reprise)

- COMP128
- COMP128-2, COMP128-3
- MILENAGE
- TUAK
**Integrated SIM**

- Other baseband components
- SIM component

Physically separate silicon within chip

(not “Soft SIM”)
What is 5G anyway?
5G is a family of technologies …

4G Evolution
- Gigabit Speeds
- Low latency radio
- Massive IoT

5G New Radio
- New spectrum
- Very high bandwidths
- Even lower latency radio
- Ultra reliable

Architectural Evolution
- Network Virtualisation
- Mobile Edge Computing
- Network Slicing

Applications at Edge Compute sites
Application servers in the Internet

Internet

Radio

Low latency radio
1-3ms
<10ms

More spectrum & new antennas

New 5G Devices

Core &

Network Slicing enables new services

<10ms
… and a family of architectures
Low Power, Wide Area IoT service

10+ Years Battery Life
Deep Penetration
Mass Deployment
Low Bandwidth
Device Cost

LTE+
NB-IoT

$\rightarrow$ $\rightarrow$

NR
NB-IoT
5G

– roaming fraud protection
Roaming fraud protection

Authentication and session key establishment

Authentication vector

Proof of authentication

Bill for roaming traffic

SECURE TRAFFIC

Visited network

Home network NG core

C1 Unrestricted

39

26 June 2018
5G
– privacy enhancement
Improved privacy

Temporary ID
Permanent ID

Request authentication vector for ‘ID’

Visited network
Home network

`ID`

Authentication and cipher key generation algorithm A3/A8

RAND
K_i
AKA
RES
K_c

K_c

RAND

RAND

K_i

AKA

XRES
K_c

XRES

RES = XRES?

Encryption algorithm A5

ENCYPRT USING K_c

C1 Unrestricted

26 June 2018
IMSI catcher / Stingray
IMSI sniffer
IMSI SUPI privacy

Temporary ID

or

Encrypted SUPI

Authenticated and session key establishment

Visited network

Home network

Encrypted SUPI

Authentication vector

Proof of authentication

Why?

SUPI

NG core

NG core
5G

– user plane integrity
Block ciphers and stream ciphers

Plaintext (128 bits) → Key → Ciphertext (128 bits)

One bit error

Plaintext (any length) → Key → Ciphertext

Plaintext (any length) → Key → Ciphertext

Plaintext

Key

Key

Key

=
Traffic = mobile voice
User plane integrity protection

- Encrypt traffic
- Encrypt & integrity protect signalling
- Integrity protect and encrypt traffic

Visited network
IoT communication security
The attack surface
End to end security

The things

Mobile operator

Internet

Application server

Security

… if your battery can handle it
BEST: battery efficient security for very low throughput Machine Type Communication devices
BEST: battery efficient security for very low throughput Machine Type Communication devices
Work in progress
So 4G security is very good … … but what if the secret isn’t secret?

How NSA and GCHQ hacked world largest SIM card maker Gemalto: “game over for cellular encryption”
How can the long term secret key leak?

- SIM vendor
  - Hack
  - Insider attack
- Sending the keys
- Mobile operator
  - Hack
  - Insider attack
- Weak algorithm
- Weak implementation
Creating shared session keys

- RAND
- K_i
- AKA
- K_C
- ENCRYPT USING K_C

- RAND
- RAND, K_C
- AKA
- K_i
- K_C

SIM

Visited network

Home network

C1 Unrestricted

56

26 June 2018
LTKUP: Long Term Key Update

SIM vendor → Sending the keys → Mobile operator

Key exchange:

Ki → Ki*
Ki* → Ki

Ki

Ki
Quantum

How's your quantum computer prototype coming along?

Great!

The project exists in a simultaneous state of being both totally successful and not even started.

Can I observe it?

That's a tricky question.
Performance constraints on security

• Call set-up time matters to customers
  – Establishing a new key at the start of each call would take noticeably longer
  – So does that mean we can’t do it?

• Fast handover between cells is important for some services
  – So pass session key from old cell to new cell, rather than establishing a new one?

• Some devices need to run on batteries for years
  – So do we need to keep security protocol transmissions to a minimum?

• Some services need very high availability
  – So we mustn’t risk false positives when policing network access?
Network slices

Optimise for integrity and availability
Optimise for battery life
Optimise for speed
Optimise for security and privacy
Handle with care
Service based architecture
Edge Computing

Application servers in the Internet

Core & Applications at Edge Compute sites

Network Slicing enables new services

New 5G Devices

Low latency radio

More spectrum & new antennas

1-3ms

<10ms

Application servers in more exposed sites

Network info or capabilities exposed to applications
Final remarks
Security evolution
Thank you