How can 5G security improve on earlier generations?

Steve Babbage

Vodafone Distinguished Engineer

Who am I?

- Vodafone Distinguished Engineer
  - Cryptography, security, mathematics
- Chair of ETSI SAGE
  - Security Algorithms Group of Experts
  - Specifies all new standardised crypto algorithms for 3GPP, amongst other things
- Co-chair of NGMN's 5G security workstream
  - Making pre-standardisation recommendations on 5G security
- On GSMA's Fraud and Security Advisory Panel

These views are mine –
not the official views of any of the companies or bodies above

Evolution of security

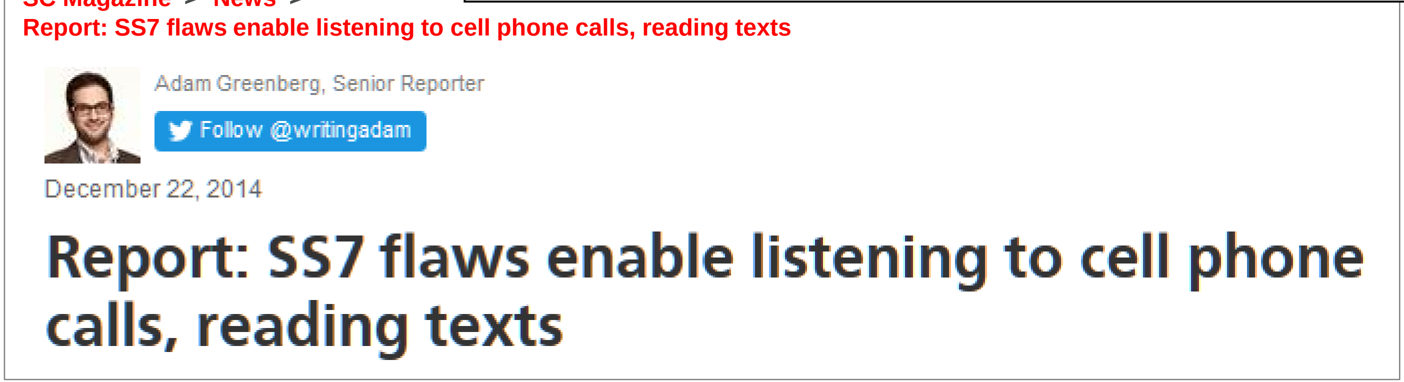
2G	3G	4G
Key length	Increased to 128 bits	
One-way authentication	Mutual authentication, tamper-proof signalling	Proves *which* network
Authentication and key agreement algorithms	Much better example algorithm	
Encryption algorithms	Full strength public algorithms	
Same cipher key, whatever the algorithm		Different cipher key depending on choice of algorithm

So 4G security is very good …

… but in some ways, fragile

Home > News > How NSA and GCHQ hacked world largest SIM card maker Gemalto: "game over for cellular encryption"

How NSA and GCHQ hacked world largest SIM card maker Gemalto: "game over for cellular encryption"

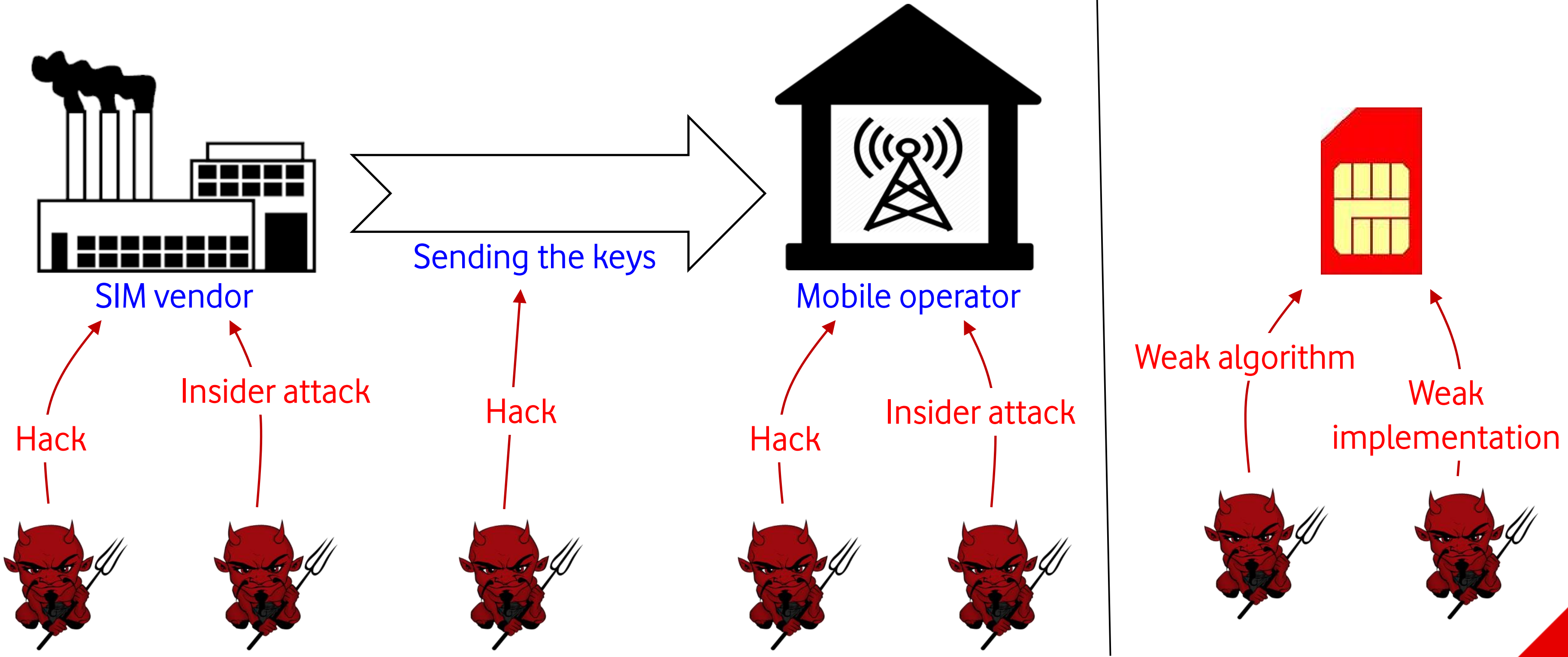

SC Magazine > News >
Report: SS7 flaws enable listening to cell phone calls, reading texts

Adam Greenberg, Senior Reporter

December 22, 2014

Report: SS7 flaws enable listening to cell phone calls, reading texts

How can the long term secret key leak?



SIM vendor

Hack

Insider attack

Sending the keys

Hack

Mobile operator

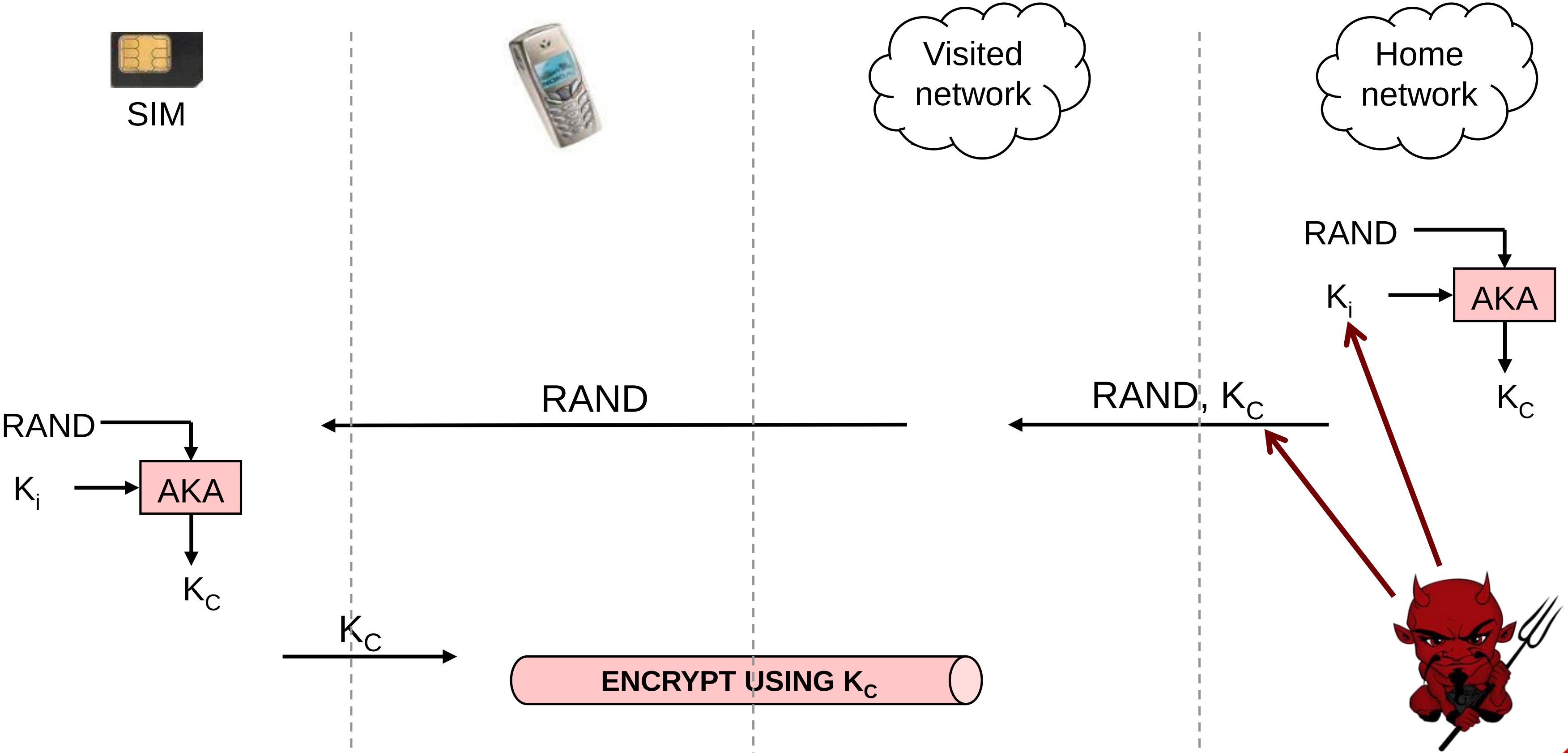
Hack

Insider attack

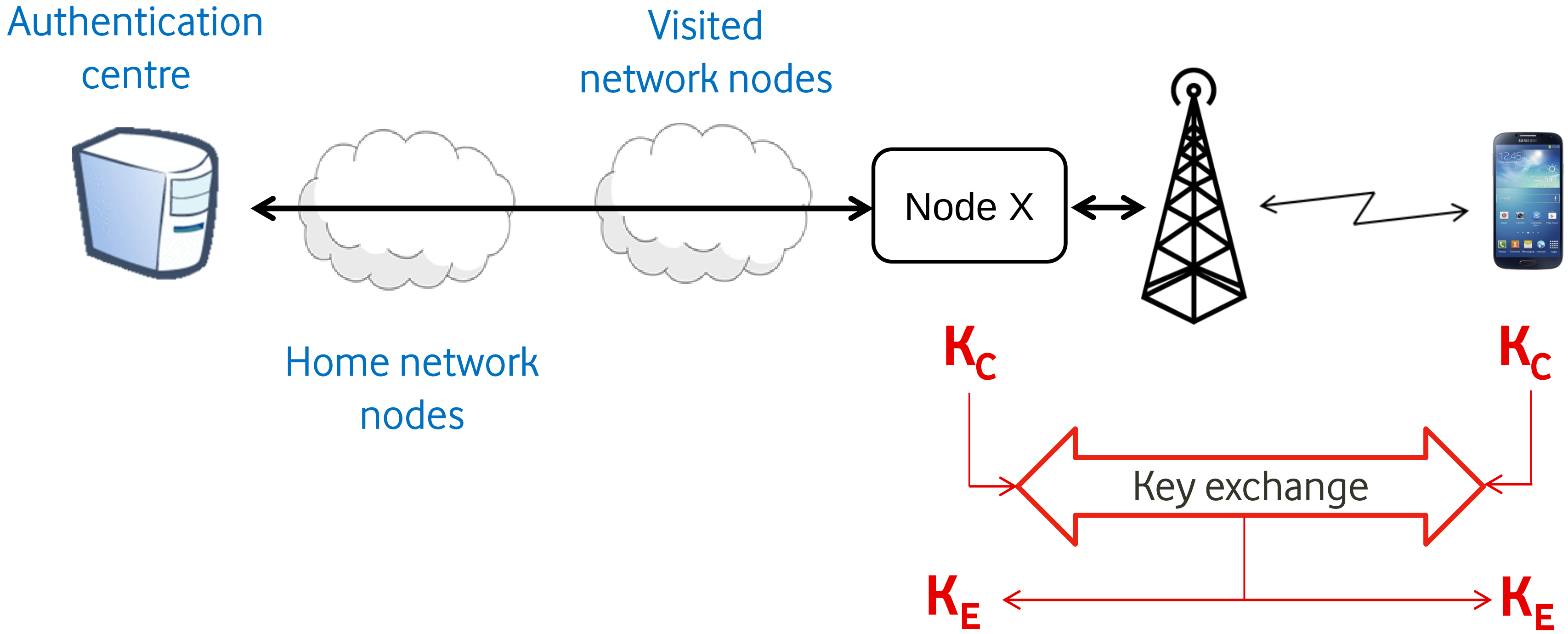
Weak algorithm

Weak implementation

Creating shared session keys

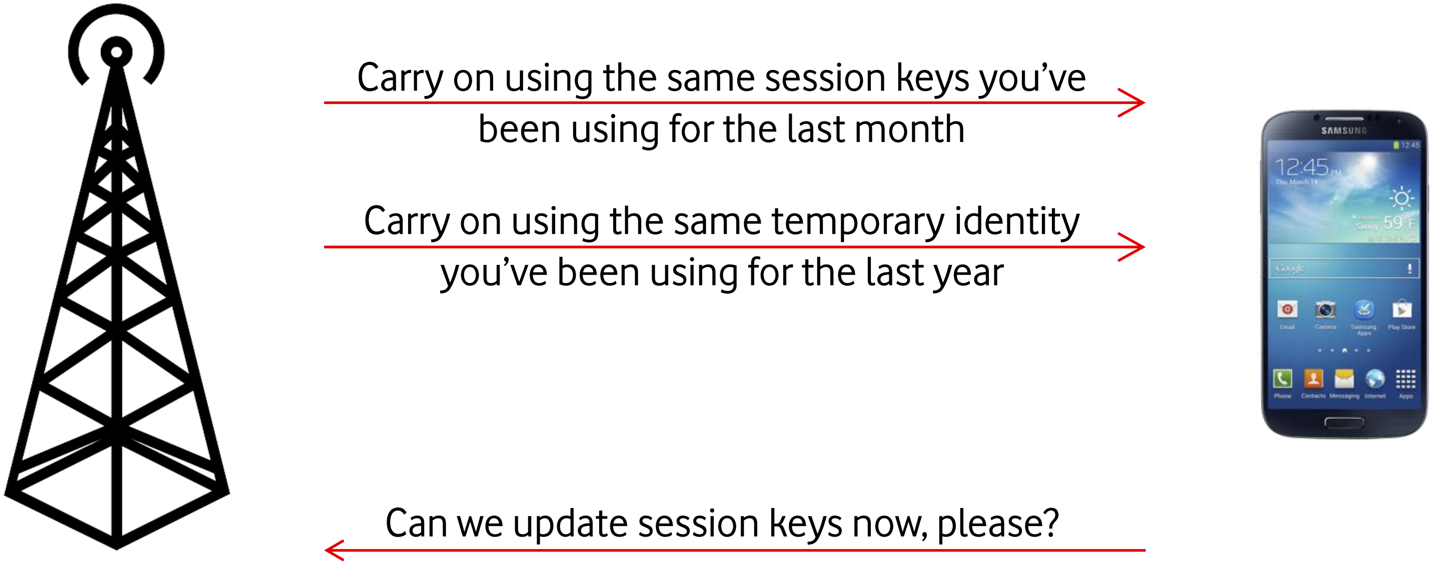


Can do key agreement differently …



… when time allows

Giving the device more control over security



Carry on using the same session keys you’ve been using for the last month

Carry on using the same temporary identity you’ve been using for the last year

Can we update session keys now, please?

Performance constraints on security

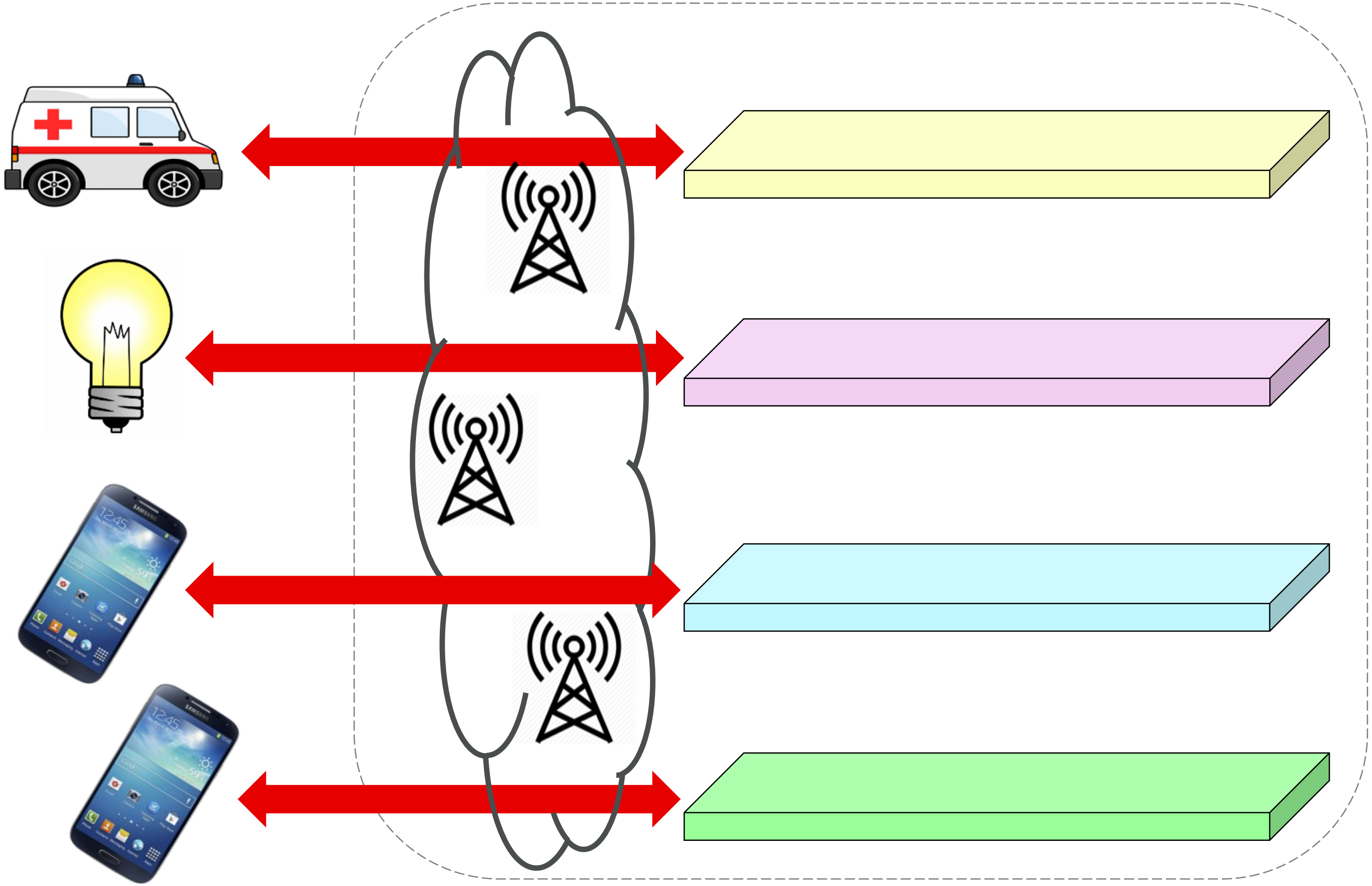
- Call set-up time matters to customers
  - Running a full key exchange protocol would take noticeably longer
  - So does that mean we can’t do it?

- Fast handover between cells is important for some services
  - Key derivation on handover is optimised for speed, not for security

- 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

Thank you