How to make 5G security a reality

Chris Mitchell
Royal Holloway, University of London
www.chrismitchell.net

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G security – where are we?

- Release 15 (R15) of 5G incorporates updated security features by comparison with LTE.
- R15 is ready for deployment.
- Future releases (R16, R17, …) will likely incorporate further new features.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G security – scope I

- Like previous generations of mobile networks (GSM, 3G and LTE), 5G security protects the mobile/network link, offering:
  - fraud prevention;
  - data/voice traffic security;
  - subscriber anonymity.
- Protects against eavesdroppers (active and passive) – but not against curious or malicious operators.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G security – scope II

- That is the standardised features stop at the network, i.e. they do not offer end-to-end security.
- This is to some extent inevitable, since the 5G standards do not cover all means of network access (either for voice or data).

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G security – novel feature

- One new feature in R15 is enhanced mobile subscriber confidentiality.
- Achieved using asymmetric encryption of permanent mobile ID using public key of 'home network'.
- Decryption done by home network.
- This addresses the 'IMSI catcher' threat.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

5G – architectural issues

- Main focus of R15 security is *enhanced mobile broadband* (*eMBB*), offering reduced latency and higher bandwidth.
- Very much an evolution of LTE security (as LTE was over 3G, and 3G over GSM).
- No radical new techniques.
- Real issue, as ever, is achieving the right cost/risk balance.
- Designing security is about risk management!

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Need for assurance

- As our reliance on mobile networks grows, the issue of *assurance* becomes ever more important.
- Operators need to have confidence that infrastructure equipment implements protocols correctly and does not have vulnerabilities.
- Errors/flaws in implementation threaten *availability*, a key plank of security.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Historical developments

- The IT industry has decades of experience in product and system security evaluations.
- From the Orange Book in the 1980s to today's common criteria evaluations, standardised proceesses exist to enable assurance to be gained in *IT* security products and systems (primarily for government customers).
- Evaluation of *ICT* products/systems is not in such a mature state.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Scalability issues

- Some current national approaches to evaluation/certification of mobile products, such as the HCSEC in the UK, are not universally applicable.
- Whilst such a national approach works for some markets, the costs are clearly non-trivial and the approach does not scale.
- A harmonised system is needed to avoid duplication of effort.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Common criteria

- The multipart international standard ISO/IEC 15408 describes how common criteria (CC) evaluations should be performed.
- CC evaluations are perfomed against protection profiles (PPs) , with the PP being specific to a type of product or system.
- Whilst the underlying ideas are key, CC evaluations are very expensive and time-consuming and are likely too heavy for mobile telecommunications systems.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

3GPP SECAM

- Within 3GPP, the *Security Assurance Methodology* (*SECAM*) has been developed as a framework for evaluating 5G products and systems.
- This methodology relies on product-specific *Security Assurance Specifications* (*SCASs*), analogous to PPs.
- A wide range of SCASs are being developed.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

GSMA NESAS

- In parallel, GSMA has been developing its *Network Equipment Security Assurance Scheme* (*NESAS*).
- The scheme has been piloted, and is still being developed.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Advantages of standards approach

- Once the standards are in place, they will enable equipment certifications whose basis and scope is internationally recognised.
- Individual countries might choose to accept these evaluations unchanged or could require 'supplementary' evaluations to address issues outside the scope of the evaluation schemes.
- In either case, this should lead to significant economies of scale for manufacturers and operators.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Quantum computing – the threat

- 5G security, as defined in R15, relies on a mix of symmetric crypto (essentially the same as 4G) and asymmetric encryption.
- The current key lengths and choices of algorithm make quantum computing a genuine threat to 5G security.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Quantum computing – the reality

- However, large scale quantum computing is still years away (indeed, some question whether it will ever be a reality).
- Since the main threat is to mobile/network authentication and key establishment, there is time to replace currently used techniques .
- Advance planning is in place to enable evolution to post-quantum crypto.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Security as a cost

- Security is a cost for manufacturers and operators.
- The current 5G security features are present primarily to:
  - prevent fraudulent network use;
  - give assurance to users that their privacy is not impacted by use of a broadcast communications medium.
- The current features are present by default and do not offer operators the opportunity to charge or offer a 'high security' premium product.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Cost versus benefit

- As has always been the case, adding new security features will require careful cost/risk analysis.
- A good example of this is the fact that only in 5G have IMSI catchers been fully addressed.
- The (ever-decreasing) cost impact of implementing asymmetric crypto on mobile devices was finally deemed worth paying to address the IMSI catcher threat.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

New security features

- R16 and later versions of the standards will provide support growing numbers of vertical applications of 5G.
- This is likely to necessitate additional security features.
- Decisions will be made on a cost versus risk basis.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Agenda

- Security – a high level look
- Assurance
- Role of standards
- Issues
- The way ahead?

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Limits to security

- There is only so much that can be achieved by adding security features to 5G.
- End-to-end security is likely to be something requiring security at the application layer.
- There are limits also to the levels of availability possible for mobile networks, since coverage will never be 100%.
- We need to be realistic …

ROYAL HOLLOWAY UNIVERSITY OF LONDON

A global approach to assurance

- The industry urgently needs agreement on a unified basis for product evaluation and certification.
- This should be provided by SECAM and/or NESAS.
- However, effort is needed to ensure the standards are delivered in a timely way.

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Integration with other initiatives

- The recent EU Cyber Security regulation covering an assurance framework for a wide range of IT and ICT products potentially dovetails with current 3GPP/GSMA assurance standards efforts.
- **Ultimately, we (users and operators alike) all need a unified, robust and cost-effective way of gaining an appropriate level of assurance in mobile systems.**