Security and Privacy Challenges in 5G Networks

Georgios Karopoulos

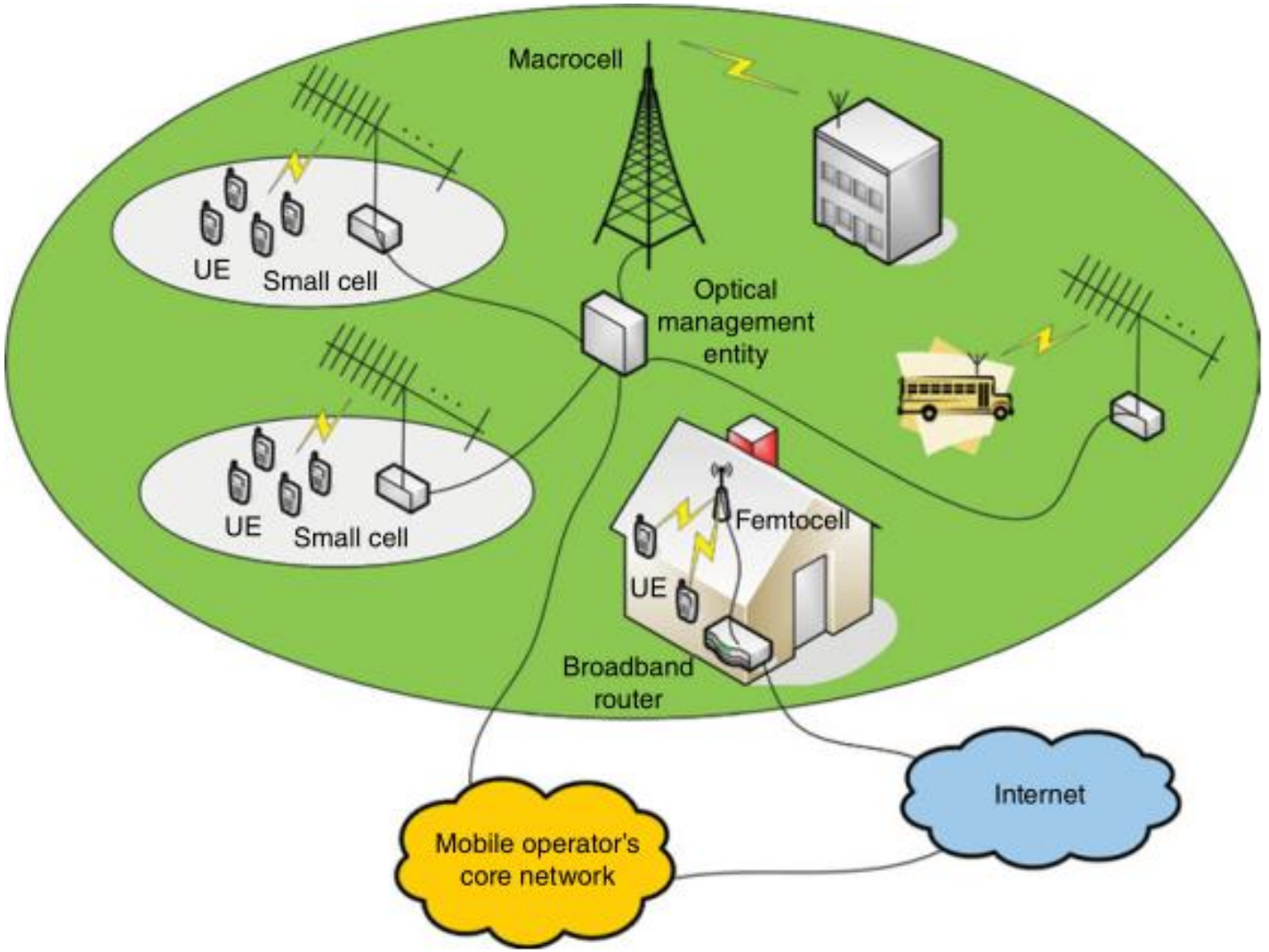
Department of Informatics and Telecommunications

University of Athens

Outline

- 5G architecture
- 5G use cases
- 5G characteristics
- Security in 2G, 3G, 4G
- What is different in 5G?
- Potential targets in 5G networks

5G architecture



Source: Mantas, G., Komninos, N., Rodriguez, J., Logota, E. and Marques, H. (2015) Security for 5G Communications, in Fundamentals of 5G Mobile Networks (ed J. Rodriguez), John Wiley & Sons

5G use cases

- Broadband experience everywhere, anytime
- Internet of Things (IoT)
- Smart vehicles and transportation
- Critical Infrastructures, e.g. Smart Grid
  - SMART-NRG (http://smart-nrg.net)

5G characteristics

- Not mature, not standardized yet from 3GPP
- The vision is to be deployed by 2020 and beyond
- Higher bandwidth and networking capability, extensive signal coverage
- Integration of existing technologies with new methods
- This leads to security and privacy challenges

Security in 2G, 3G, 4G

- Targeted protection
  - Only a few basic services to protect: initially voice only, later on data
- Limited protection needs
  - User: data encryption, basic identity protection (temporary IDs)
  - Network: strong authentication for billing (solved with SIM cards)
- Relative stability
  - Threats did not change much over time
  - Countermeasures included in next generations
- Successful overall
  - It has worked well in general
  - Although there were some crypto issues (mainly in 2G)
  - Zero-config from the user’s point of view

What is different in 5G?

- New business and trust models
- New service delivery models
- Increased privacy concerns
- Evolved threat landscape

New business and trust models

- Not only voice and data in a well defined network structure but different devices (mobile phones, tablets, unattended machines, sensors, smart meters, cars), architectures (cloud, IoT)
- Higher bitrate, lower latency, more devices
- Connecting industries: manufacturing, transport, smart grid, e-health
- 5G will have a crucial role in society operation and security, privacy and resilience will span beyond technology involving regulation and legal frameworks

New service delivery models

- Cloud, virtualization, anything-as-a-service:
  - Reduce costs, deploy and optimize services more rapidly
  - Increase dependency on secure software
  - Decoupling software and hardware means that software can no longer rely on the security attributes of dedicated hardware
- Telecom network Application Programming Interfaces (APIs)
- Mixing of provider with third-party applications, shared and dedicated hardware platforms
  - Strong isolation properties are necessary

Increased privacy concerns

- Awareness of user privacy in society has been increased after recent events and news stories (Julian Assange, Edward Snowden)
- Big data analytics push these concerns further
- The approach followed in 3G with permanent and temporary identities did not actually solved the issue

TMSI values assigned to static users

Operator A	Operator B	Operator C
23B9C7A8	701590D9	A8B32A7A
23BA25D0	701590D9	A8B32A7A
23BA82D0	701590D9	A8B32A7A
23BAE940	701590D9	A8B32A7A

Source: Christoforos Ntantogian, Grigoris Valtas, Nikos Kapetanakis, Faidon Lalagiannis, Georgios Karopoulos, Christos Xenakis: Attacking GSM Networks as a Script Kiddie Using Commodity Hardware and Software. TrustBus 2015: 73-86

Evolved threat landscape

- 5G will be a Critical Infrastructure itself suffering from cascading effects
  - Example: a malfunction in a gas infrastructure can lead to a blackout which can lead to loss of telephony and internet access
- Data are critical in decision-making and value creation: 5G networks will be the carriers of such data, thus adequate protection measures are needed
- 5G security protocols should be designed with attack resistance in mind while phasing out traditional methods that are not effective anymore (for example username/password authentication)
- Emphasis should be given to measurable security assurance and compliance due to legal and regulatory concerns

Potential targets in 5G networks

- The most attractive target in 5G will be:
  - User equipment
  - Access networks
  - Mobile core and external IP networks
- In the following, threats and attacks against legacy systems (2G/3G/4G) that can affect 5G will be explored

User equipment

- Equipment examples: powerful smartphones and tablets
- Why user equipment is targeted?
  - Popularity
  - Increased data transmission in 5G
  - Adoption of open operating systems and third-party app stores
  - Large variety of connectivity options (2G/3G/4G/5G, WiFi, Bluetooth)

User equipment

- Mobile malware
  - Innocent looking applications downloaded from an untrusted app store
  - Exploit or steal personal data
  - Mount attacks (e.g. DoS) against the same UE or other entities (other UE, own or other networks)
- Mobile botnets
  - Target many UE at the same time in an automated way
  - Networks of compromised UE under the (remote) control of the bot-master
  - Distributed DoS (DDoS) attacks, spamming, theft of sensitive data, infection of other UE

Access networks

- Attacks on 4G
  - UE location tracking in a specific or over multiple cells
  - Attack the packet scheduling algorithm to steal bandwidth
  - Message insertion leads to DoS attack against a new arriving UE
- Femtocell attacks
  - Physical tampering with equipment (interference with other devices)
  - Configuration attacks (misconfiguration of ACL)
  - Protocol attacks (MitM during first access)
  - Attacks on mobile operator’s core network from compromised nodes
  - Credential theft, user data and identity privacy attacks from open access nodes
  - Attacks on radio resources and management to increase handovers

Mobile core and external IP networks

- DDoS attacks
  - Signaling amplification
  - Home Subscriber Server (HSS) saturation
- DDoS attacks targeting external entities over a mobile operator’s core network
- Compromise enterprise networks through bring-your-own-device (BYOD) trend

Conclusion

- 5G will support the vision of “everything connected”
- Instead of individual security mechanisms, a systematic and analytical approach is needed
- 5G security cannot be “copied” from 4G (or older) security
- While there are still valid security approaches they need to be revisited (trust models, devices, assurance)
- Attacker targets include pretty much everything: user devices, access and core networks, home and external networks

Thank you!

Georgios Karopoulos

University of Athens

gkarop@di.uoa.gr