5G security

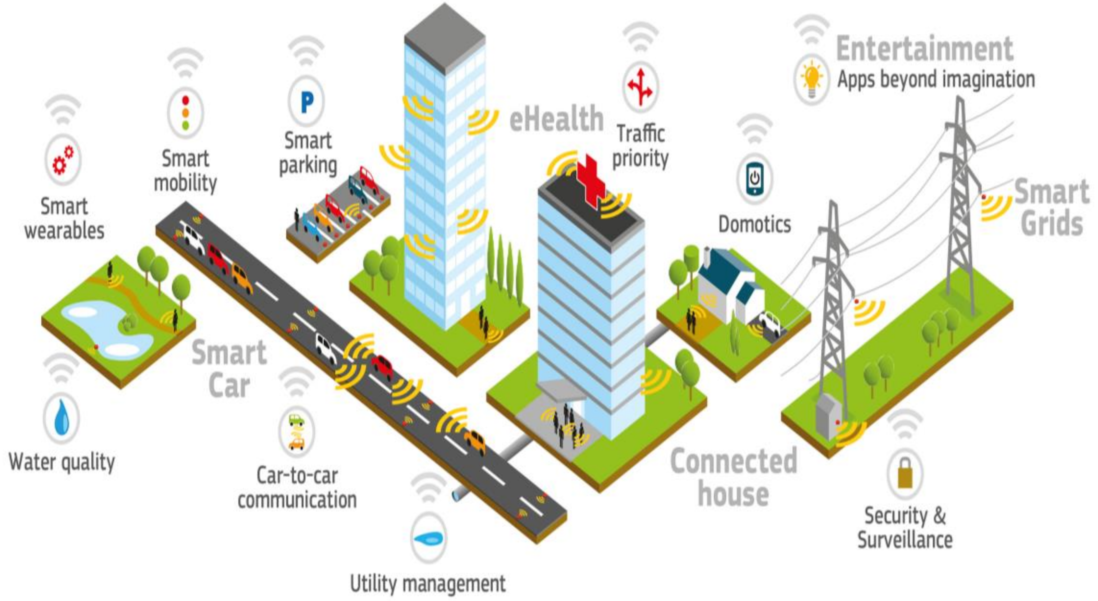
Maghsoud Morshedi Chinibolagh

5G vision and use cases[1]

- Broadband access in dense area
  - Pervasive video, smart offices, operator cloud services and HD video sharing in stadium
- Broadband access everywhere
  - 50+ Mbps everywhere, ultra low cost networks
- Higher user mobility
  - High speed train, moving hotspots, 3D connectivity for aircrafts and remote computing
- Massive Internet of Things (IoT)
  - Smart wearable, sensor networks and mobile video surveillance

5G vision and use cases(continues)

- Extreme real time communication
  - Tactile internet
- Lifeline communication
  - Natural disaster
- Ultra-reliable communications
  - Automated traffic control and driving, collaborative robots, eHealth, remote surgery, drones, public safety
- Broadcast-like services
  - News and information, local, regional and national broadcast-like services

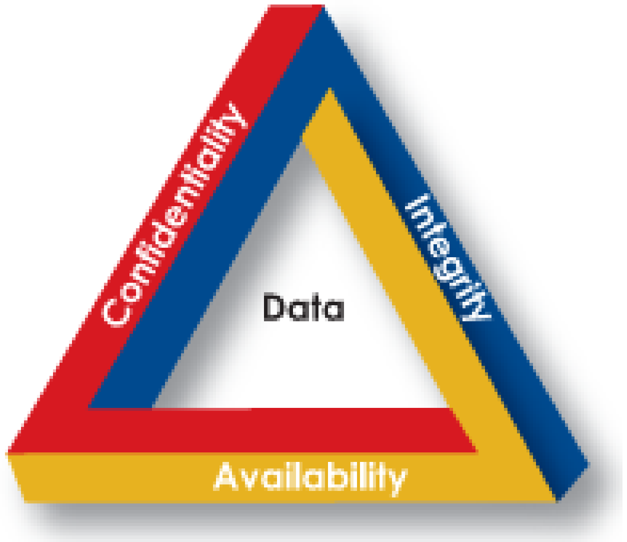


Source: http://mvnoeurope.eu/

Information Security

- Confidentiality
- Integrity
- Availability

- Authentication
- Non-repudiation
- Access control

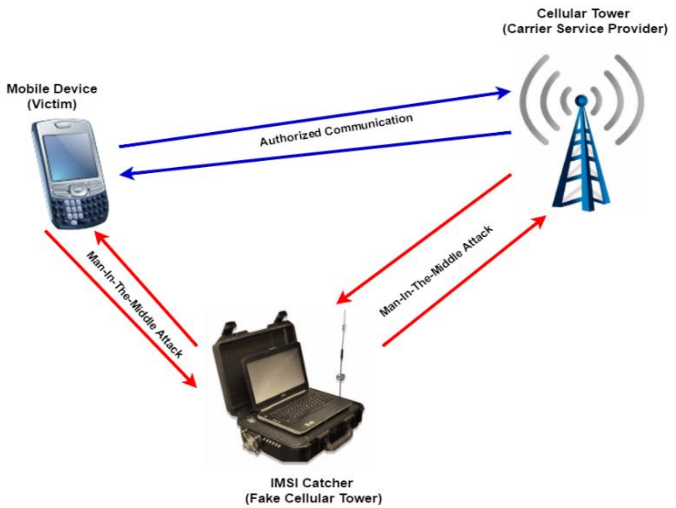


Potential Security Mechanism for 5G[4]

- User and device identity confidentiality
- Mutual authentication and key agreement
- Security between terminal and network
- Security in network interfaces
- Security visibility and configurability
- Platform security
- Protection against Denial-of-Service attacks

User and Device Identity Confidentiality

- International mobile subscriber identity(IMSI) is same in GSM,UMTS and LTE
- User identity confidentiality in LTE provide protection against passive but not active attacks
- IMSI catching attack
  - Public key, symmetric key and pseudonyms are potential countermeasures



Source: http://iisecurity.in/

- International mobile equipment identity(IMEI) shall be sent in LTE in confidentially-protected message but in GSM and UMTS, attacker may request in an unprotected message

Mutual Authentication and Key Management

- Authentication of user equipment and network has to be always coupled with key agreement.
- Authentication and key agreement (AKA) in UMTS and LTE
- Public-key-based authentication and key agreement
  - Home network does not need to be contacted for each authentication
- Storage credential on user equipment
  - Soft SIMs – credentials would be stored on the terminal or some form of Trusted Platform Module

Security Between Terminal and Network

- Signalling integrity is indispensable for preventing impersonation of users and networks
- Idle-to-connected transition in LTE for setting up security between terminal and base station may matter for 5G

Security Visibility and Configurability

- In existing mobile networks, network decides on security features and algorithms.
  - In 5G, user shall have possibility to see whether encryption is applied (ciphering indicator)

- User can configure that the use of a service should depend on whether security feature is in operation.
  - In 5G, user can tell the network, which security feature should be enabled

Security Attacks [5]

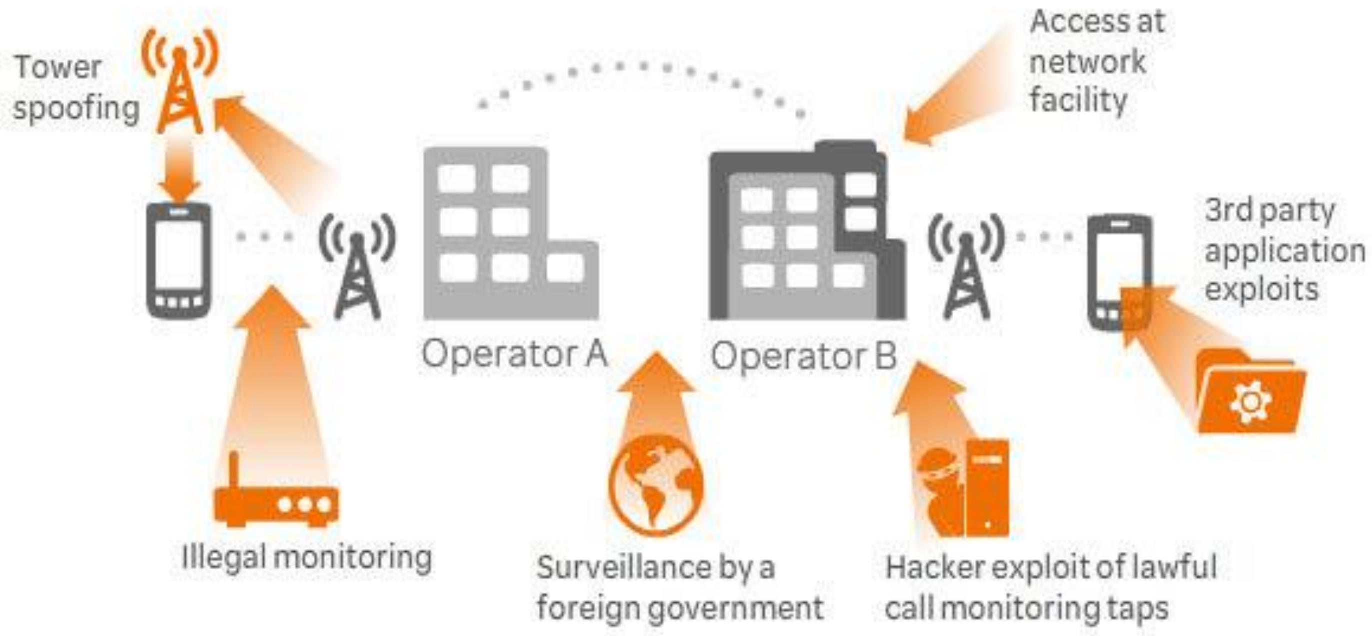
- Passive attacks
  - Release of message content, traffic analysis

- Active attacks
  - Denial of service, jamming, false data injection(FDI) and masquerade

Release of Message Content(eavesdropping)

- Attack
  - Due to openness of utilized medium can not be easily prevented

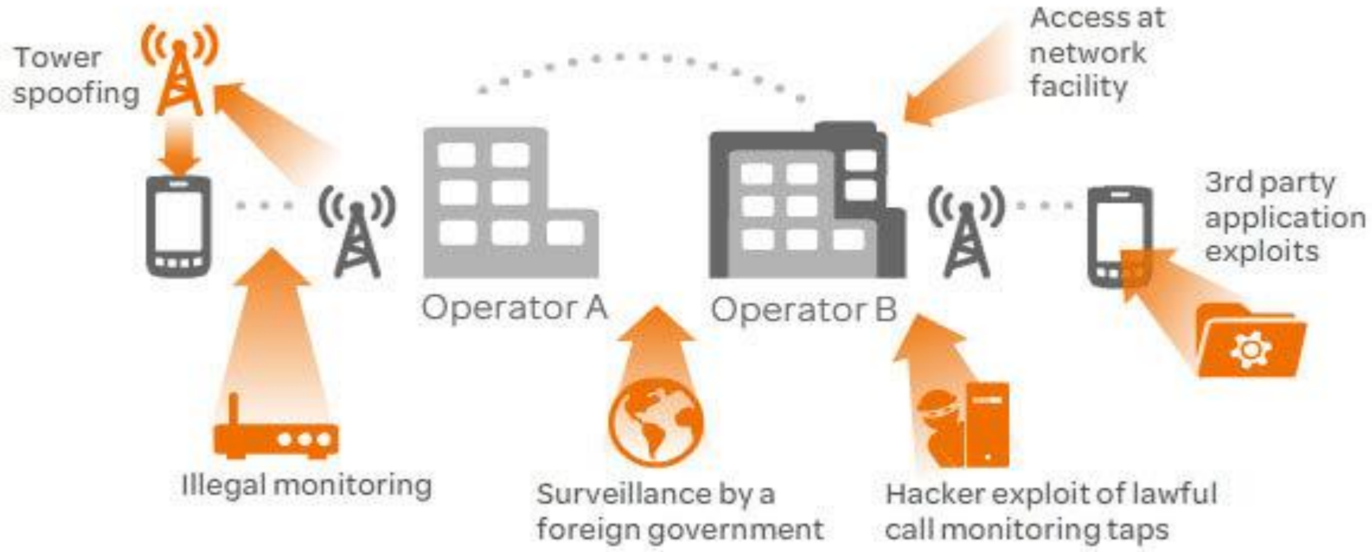
- Countermeasures
  - Encryption
  - Elliptic Curve Cryptography


Tower spoofing
Access at network facility
3rd party application exploits
Operator A
Operator B
Illegal monitoring
Surveillance by a foreign government
Hacker exploit of lawful call monitoring taps

Source: www.securevoicegsm.com

Traffic Analysis

- Attack
  - Obtaining transferred message and observing patterns in their transmission.
  - Find location and identity as well as frequency and length of message
  - Find topology of network


Tower spoofing
Access at network facility
3rd party application exploits
Operator A
Operator B
Illegal monitoring
Surveillance by a foreign government
Hacker exploit of lawful call monitoring taps

Source: www.securevoicegsm.com

Denial of Service (DoS)

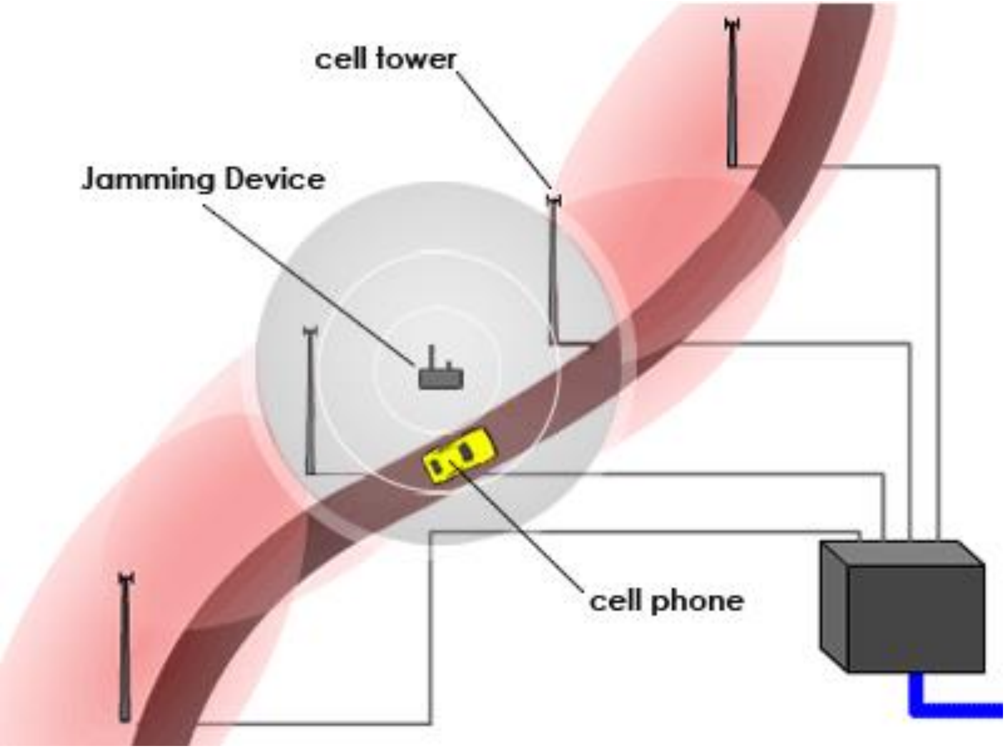
- Attack a network availability by disrupting the transmission of information
- DoS attack carried out by mobiles (ikee.B botnet [2]).
- Botnet of mobile devices for jamming

- Countermeasures
  - Limiting the rate of incoming request from other networks
  - Blocking offending source temporarily
  - Overload protection mechanism
  - Flocking based model against DoS attacks
  - Warning system against malicious Events

Jamming

- Filling wireless channel with noise signal
- Proactive jamming
- Reactive jamming

- Countermeasures
  - Spread spectrum technique
    - Frequency-Hopping Spread Spectrum(FHSS)
    - Direct-Sequence Spread Spectrum(DSSS)
    - Time-Hopping spread Spectrum(THSS)
    - TDMA Spread Spectrum
  - Jamming attack detection based on estimation

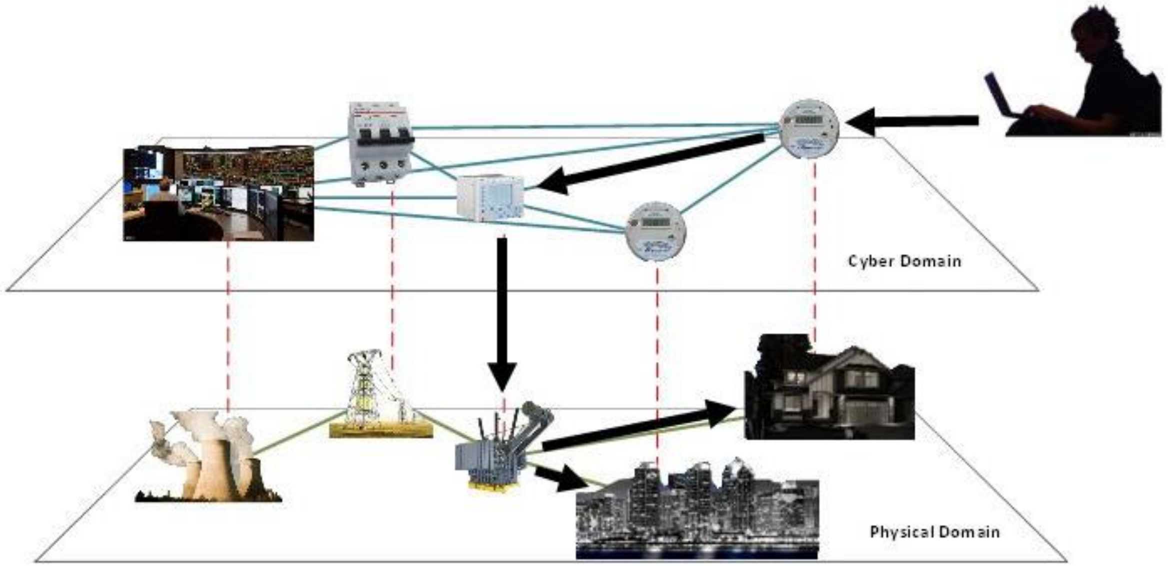


Source: http://electronics.howstuffworks.com/

False Data Injection (FDI)

- Manipulating the data of system to compromise system integrity

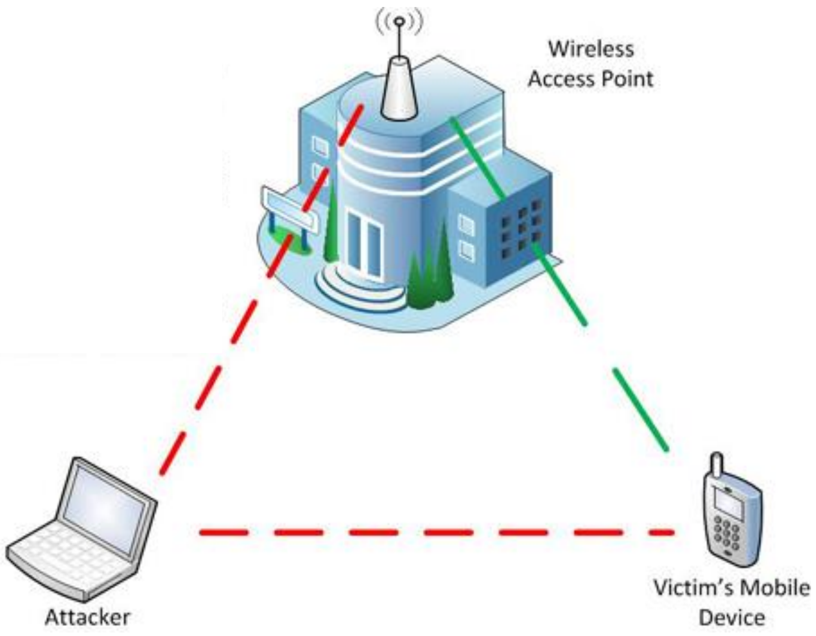
- Countermeasures
  - Real-time detection of FDI scheme
  - Secure booting with signature
  - Endpoint firewall
  - Patches and updates
  - Backup data periodically



Masquerade

- An entity impersonates and pretend to be another entity in the network.
- Replay attack
- ARP spoofing

- Countermeasures
  - Device certificate



Discussion

- Should 5G security Build on LTE?
- Should 5G increase security configurability?
- Should 5G consider end point security?

Conclusion

- In order to ensure security, 5G should have following characteristics:
  - ✓ Built-in security from start point
  - ✓ Clarifying security requirements
  - ✓ Reviewing existing security architecture
  - ✓ Security measures should be in tight interworking with 5G network architecture

References

[1] Next Generation Mobile Network Alliance, “5G White Paper”, Version 1.0, Feb 17, 2015.

[2] P. A. Porras, H. Saidi, and V. Yegneswaran, “An analysis of the ikee.b iphone botnet,” MobiSec, Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, Springer, vol. 47, pp. 141–152, 2010

[3] A. Berger and M. Hefeeda, “Exploiting sip for botnet communication,” in Proc. 5th IEEE Workshop Secure Network Protocols, 2009, pp. 31–36

[4] P. Schneider and G. Horn, "Towards 5G Security," *Trustcom/BigDataSE/ISPA, 2015 IEEE*, Helsinki, 2015, pp. 1165-1170. doi: 10.1109/Trustcom.2015.499

[5] Constandinos X. Mavromoustakis, George Mastorakis, and Jordi Mongay Batalla. 2016. *Internet of Things (Iot) in 5G Mobile Technologies* (1st ed.). Springer Publishing Company, Incorporated.

Thank you