Random Thoughts on 5G Security

Prof. Jeffrey H. Reed
Bradley Dept. of ECE, Virginia Tech
Interim Director, Commonwealth Cyber Initiative
Founding Director, Wireless@Virginia Tech
reedjh@vt.edu
(540) 231-2972

Portions of this presentation extracted from the eBook, *5G Cellular Communications- Journey & Destination,* By Nishith Tripathi and Jeffrey Reed, avalable at *http://www.thewirelessuniversity.com*

Introduction and Motivation and Key Points

- Attacks on 4G and 5G can occur at any layer.
- Systems are extremely complex to analyze for vulnerabilities.
- While jamming is always possible, we do *not* want extremely efficient protocol-aware jamming attacks to exist.
- There is a large community focused on higher layer attacks (Go to Blackhat!).
- 3GPP has demonstrated a new level of security consciousness.
- Authentication and security customization in 5G.
- Potential new ways to address security.
- Difficulty in doing this research.

LTE Jammer

Obtaining IMSI by Software-Defined Radio (RTL-SDR) -- $32 IMSI catcher

Pictures from:
Roman V. Bulychev, Dmitry E. Goncharov, Irina F.
Babalova Institute Cyber Intelligent Systems
National Research Nuclear University
Russian Federation

Security Contributions for Rel.-15

- User plane (UP) integrity protection mechanisms.
- Enhance International Mobile Subscriber Identity Privacy
- Authentication and authorization (including identity management)
- RAN security
- Security in the UE (storage security, processing of credentials, eSIM)
- Network slicing security
- Increased home network control (i.e., EPC authentication and key management proof of UE presence in visiting network)

Not all security objectives of Rel. 15 were met and hence much security work remains for Rel. 16

Security Issues Addressed in Rel.-16

- Security mechanism for prevent access to other network slices
- Trusted non-3GPP access
- Authentication of the user
- Security for small data mode
- User plane DoS attacks
- Relay security
- Broadcast/Multicast Security

When you are 16 years old you can get your driver's license in the USA!

You might say the teenager is Released at 16

Potential Security Features of Rel. 16

- Customized security control of what slices a UE may use simultaneously or slice specific authentication.
- Features enabling private networks for factory automation, ultra reliable and ultra low latency (URLLC), and more.
- Security mechanism differentiation for network slices
- Trusted non-3GPP access
- Authentication of the user
- Security for small data mode for CIoT applications
- User plane DoS attacks
- Relay security
- Broadcast/Multicast Security

Security Studies On-Going in Rel. 16

- Study on Security Aspects of the 5G Service Based Architecture
- Study on Long Term Key Update Procedures Study on Supporting 256-bit Algorithms for 5G
- Security aspects of single radio voice continuity from 5G to UTRAN
- Study on authentication and key management for applications based on 3GPP credential in 5G IoT
- Study on evolution of Cellular IoT security for the 5G System
- Study on the security of the Wireless and Wireline Convergence for the 5G system architecture
- Study on Security Aspects of PARLOS Study on 5G security enhancement against false base stations
- Study of KDF negotiation for 5G System Security
- Study on Security aspects of Enhancement of Network Slicing
- Study on Security of the enhancement to the 5GC location services
- Study on security for 5G URLLC
- Study on SECAM and SCAS for 3GPP virtualized network products
- Study on Security for 5GS Enhanced support of Vertical and LAN Services
- Study on LTKUP Detailed solutions
- Study on User Plane Integrity Protection
- Study on Security Impacts of Virtualisation
- Study on authentication enhancements in 5GS

3GPP is taking security to a whole new level of rigor.

Security Vulnerabilities and Implementation Challenges in 5G [1]

- Null Encryption and Null Authentication still supported in valid configurations
- Trust in the base station is still implied before pre-authentication
- Lack of certainty that base station is enforcing a number of optional security features
- Key management functions left outside the specifications.

[1] R. P. Jover, V. Marojevic, “Security and Protocol Exploit Analysis of the 5G Specifications,” arXiv:1809.06925, Nov 2018.

While the 3GPP Security Process for 5G has Improved There are Other Issues

- Disruption to links.
- Hardware and/or software security flaws from a manufacturer.
- Continuous updates to software and infrastructure parameters.
- ....

AI May Help with Vulnerability Analysis Security Monitoring

UE

AI Control

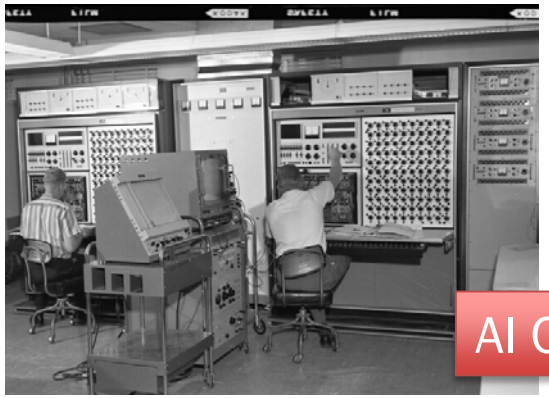
Smart Jammer

AI Control

Base Station

AI Control

Core Network



AI Control

- Use of AI and adversarial learning to find weakness.
- Use of Federated Learning for Scalability.
- AI may have a role in monitoring and mitigation of threats

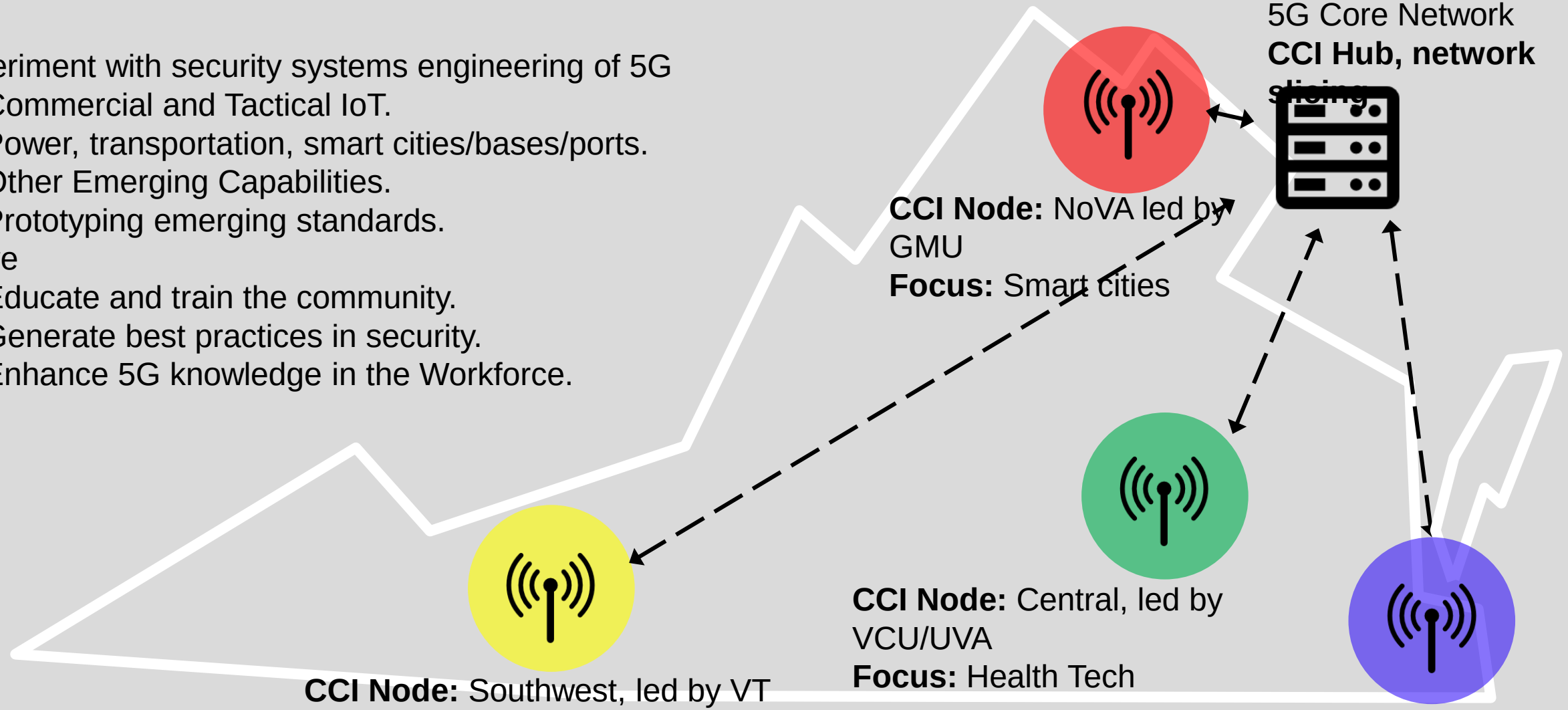
Problems in Doing 5G Security Researh

- Equipment is Expensive
  - > $1M for production quality core network.
  - Over the air protocol analyzer > $500k.
- Hard to find the right people and they are expensive and rare!
- Realistic testing situations.
- Privacy issues and impacting real networks though active probing– can inadvertently become the bad guy. FCC might get mad 
- **What's needed – Testbed Facilities with Trained Personnel.**

Commonwealth Cyber Initiative
5G SECURITY TEST BED

Experiment with security systems engineering of 5G
- Commercial and Tactical IoT.
- Power, transportation, smart cities/bases/ports.
- Other Emerging Capabilities.
- Prototyping emerging standards.

Serve
- Educate and train the community.
- Generate best practices in security.
- Enhance 5G knowledge in the Workforce.



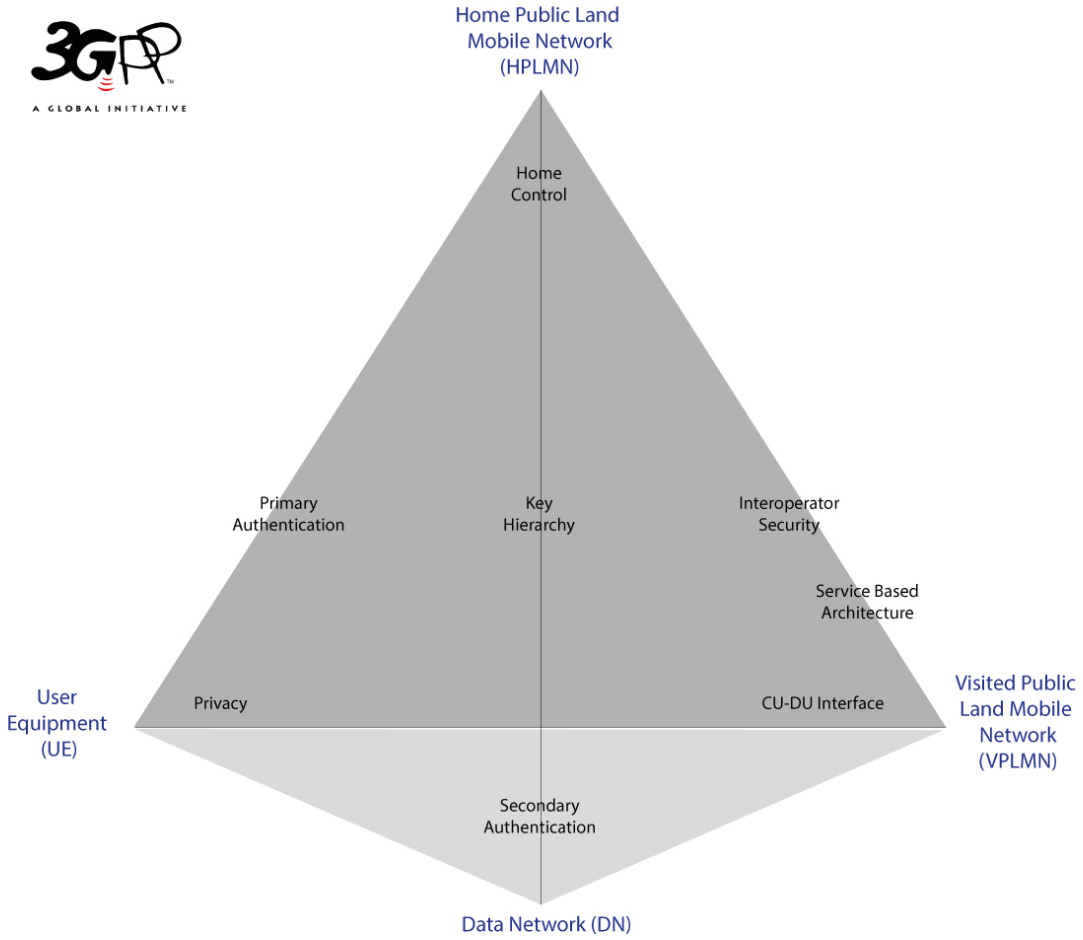
Summary

- 3GPP Release 15 (5G NR) adds new security features through modifications of the security architecture of LTE.
- 3GPP Release 16 is currently undertaking study items on 5G use cases such as IoT, URLLC, network slicing, mission critical communications etc.
- Even though 5G NR mitigates some of the known vulnerabilities of LTE, attacks pertaining to user subscriber identity, location and traffic profile are still possible.
- AI may have an important role in finding the vulnerabilities and mitigating these vulnerabilities
- Research in this area is important, but expensive and difficult to do.

Backup Slides

Backup Slides

Security Enhancements in 3GPP Rel. 15



Source: 3GPP 5G Security, URL: http://www.3gpp.org/images/articleimages/5G_security_2018_08/

- Primary authentication with built-in home control.
- Integrated secondary authentication.
- Inter-operator security intrinsic to the standard
- Subscriber identity privacy using home network public key
- Service-based architecture (SBA)
- Security for the Central Unit-Distributed Unit (CU-DU) Interface.
- Possibility of integrity protection of user plane.
- Mobility anchor can be separated from the security anchor.

5G Security Use Cases

Cellular IoT Security [1]

- Efficient frequent small data transmissions.
- Integrity protection of small data
- Encryption of small data
- Signaling overload due to malicious apps on UE
- gNB protection from CIoT DoS attack
- Key refreshing for protection of small data
- Key and mac size for protection of small data
- Protection of Non-IP Data Delivery Systems
- User plane data transmission with connectionless signaling.

Mission Critical Security [2]

- Cross-service issues:
  - DoS, user impersonation, manipulation, traffic analysis, edge protection etc.
- Common functional architecture issues:
  - Config and service access, group key management.
- Push-to-talk (PTT) issues:
  - Interception, key stream reuse, private call confidentiality etc.
- Data Communications issues:
  - Protection of short data services (SDS).
- Video communications issues:
  - Similar issues as PTT.
- Migration and Interconnect (MCSMI):
  - Maintaining security during migration and interconnection,, inter-domain authentication, protection against external systems.
- Interworking with 3GPP Systems:
  - Terminating mission-security mechanisms.

[1] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on evolution of Cellular IoT security for the 5G System (Release 16),” 3GPP TS 33.861 v0.3.0, Nov 2018.
[2] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects Study on mission critical security enhancements (Release 15),” 3GPP TR 33.880 v15.1.0, March 2018.

Other 5G Security Use Cases

1. **Ultra-reliable low latency communications (URLLC) [1]**
   - Security implications of architecture on low latency, low jitter and high reliability
     - between UE and network
     - between UEs.
   - Security using 256-bit algorithms.

Study on the Security of the enhancement to the 5GC Location Services

2. **Network Slicing [2]**
   - Inter-slice security isolation
   - Slice-specific security in roaming scenarios.

3. **Enhancements against False Base Stations [3]**
   - Study and mitigation of possible DoS attacks caused by fake gNBs.

4. **Location Services [4]**
   - Study and mitigation of location privacy/security attacks for roaming and non-roaming cases.

[1] 3GPP, “Study on the security of URLLC for 5GS (SP-180910),” 3GPP TSG-SA Meeting #81, Gold Coast, Australia, 12th Sept-14th Sept 2018.
[2] 3GPP, “Study on Security Aspects of Enhancement of Network Slicing,” 3GPP TSG-SA Meeting #81, Gold Coast, Australia, 12th Sept-14th Sept 2018.
[3] 3GPP, “Study on 5G security enhancements against false base stations,” 3GPP TSG-SA Meeting #81, Gold Coast, Australia, 12th Sept-14th Sept 2018.
[4] 3GPP, “Study on the Security of the enhancement to the 5GC Location Services,” 3GPP TSG-SA Meeting #81, Gold Coast, Australia, 12th Sept-14th Sept 2018.

Impact of 4G Vulnerabilities on 5G [1]

LTE Protocol Exploit	Threat	Impact on 5G
IMSI Catching	Privacy threat, location leaks etc.	Possible to catch the SUPI by setting up a rogue BS.
Attach/ TAU-update request	DoS	DoS of 5G mobile devices with rogue BS
Silent downgrade to GSM	Man in the middle (MitM) attacks, phone call and SMS snooping	Silent downgrade to GSM with rogue BS
Location tracking with RNTI	Location leaks, traffic estimation, service estimation	Potential device location traffic and traffic profiling
Insufficient protection of DNS traffic at layer 2	DNS hijacking over LTE	MitM attacks, credential stealing, remote malware deployment

[1] R. P. Jover, V. Marojevic, “Security and Protocol Exploit Analysis of the 5G Specifications,” arXiv:1809.06925, Nov 2018.