5G and Security: What you don't know will hurt you!

David Lake, Sumedh Sathaye
Dell Technologies

Agenda

- Taxonomy of Protection Concerns
- Where to look for attack surfaces in 5G
- 5G top-3 industry verticals
- Safety by Integrity – Best Practices
- Conclusions
- Q&A

Taxonomy of Protection Concerns

Taxonomy of Protection Concerns

- Personal Security
  - Health and safety of the individual and family
  - Personal assets and effects
- National Security
  - Security of the nation
  - Ability to meet economic goals
  - Ability to meet social goals
- International Security
  - Impact to International trade
  - International relations
- Corporate Security
  - Protection of IP
  - Protection/Promotion of Brand
  - Protection of resources, both physical and human

Taxonomy of Protection Concerns

- Personal Security
  - Health and safety of the individual and family
  - Personal assets and effects
- National Security
  - Security of the nation
  - Ability to meet economic goals
  - Ability to meet social goals
- International Security
  - Impact to International trade
  - International relations
- Corporate Security
  - Protection of IP
  - Protection/Promotion of Brand
  - Protection of resources, both physical and human

5G Touches ALL of these areas!

5G Presents multiple Issues

- Network fragility
- Increasing system complexity (law of unintended consequences)
- Single points-of-failure
- Long recovery times designed around “best-efforts” tradition of Internet
- RF vulnerability (atmospheric effects, RF-based DoS)
- Disaggregated layers – difficult to define/deliver against outcome
- Multiple Actors
- Mission-critical nature of 5G
- 3GPP SDOs have considered interoperability, not system design.
- Security needs to be built in, not just an overlay as in IETF (e.g. IPSec).
- Security/Privacy in 5G is of public interest – high-profile, national security, societal benefits
- Network overload may be problematic – many billions of devices, simultaneous re-attach impact on infrastructure

Where to look for Attack Surfaces in 5G

Where to look for Attack Surfaces in 5G

- Signalling:
  - Re-route calls, intercept SMS
  - 2G assumed high-level of trust in signalling peers
  - Current system regularly attacked – SMS exploits, cold-calling with spoofed CLI
- User Payload:
  - Only extends to data-plane.
  - Integrity protection
  - Overlay security
- Management Plane:
  - Wide domain of attack
  - Complete system access
  - Manipulate/disturb entire traffic patterns
- Interoperability
  - Focus is on common-feature interoperability
  - Value-added features often vendor-specific
  - Issues of system-wide quality
- Crimeware
  - Industrialized – “as-a-service” mentality
  - Must think of attack as a “Business-as-Usual” not an exception

Malicious Actors

- Criminal
  - Malicious external actors
  - Money-focused – e.g. access to billing and charging systems
- Hacktivists
  - Politically motivated
  - Aim is to disrupt, deface, steal sensitive information. Financial damage, political message
  - Insider threats; disgruntled former employees.
- Industrial Espionage
  - Gain access to trade secrets
  - Gain competitive advantage

IoT

Industry Verticals – IoT: Consumer & Industrial

- 5G makes guarantees of latency & scale via special network slices
- Consumer IoT is commonplace now
  - heart-rate monitors, blood-pressure machines, sleep pattern monitors etc. are quite common
- As well, industrial use of IoT technology is exploding
  - Mission critical; high value at stake, different tolerance for risk compared to 4G and earlier
  - “Service” is not just telecoms network – IoT extends to OTT services
- Big questions
  - IoT sensors usually lack resources to manage communications security
  - Wide range of OS. Less homogeneity of OS = more possible vulnerabilities
  - Implications of DoS-like attacks via IoT: will side-channel DoS bring down all 5G communication?

Industrial IoT Forum Lists Many Use Cases

1. Smart factory warehousing applications
2. Predictive and remote maintenance
3. Freight, goods and transportation monitoring
4. Connected logistics
5. Smart metering and smart grid
6. Smart city applications
7. Smart farming and livestock monitoring
8. Industrial security systems
9. Nuclear power plant monitoring
10. Energy consumption optimization
11. Industrial heating, ventilation and air conditioning
12. Manufacturing equipment monitoring
13. Asset tracking and smart logistics
14. Ozone, gas and temperature monitoring in industrial environments
15. Safety and health (conditions) monitoring of workers
16. Asset performance management

Source: https://www.iiconsortium.org/wc-security.htm

Industrial IoT Forum's Security Report Paints a Scary Picture

- As 5G-based delivery of IoT services is enabled, which of the security aspects become more vulnerable?
- Which aspects have known implications?
- Which aspects might have unknown-unknowns?

- IoT over 5G has implications to safety and security at all levels and corners of the society

Source: https://www.iiconsortium.org/pdf/IIC_PUB_G4_V1.00_PB-3.pdf

Example of IoT attack: The Mirai IoT Botnet (2016)

- How Mirai operates – and how simple it is to exploit the transport carrying extremely sensitive data
  - Scan IPs and ports
  - Find vulnerable devices, install and link
  - Send instructions to launch DDoS
  - *SYN, ACK, DNS, GRE, UDP, STOMP…floods*
  - Close ports 22 and 23
- All IoT devices / types are exploited by the Mirai botnet
- Mirai wins by volume and scale: 1Tbps

- Could a Mirai-like botnet would be even more harmful with 5G network slicing
  - Can it bring down other 5G “slices”?
  - Can it bring down entire 5G networks?
  - Can it affect related (e.g. WiFi-6) networks expected to work closely with 5G?
- What are we not thinking about? I.e. are there any attack surfaces where we are not looking?

Source: https://www.networkworld.com/article/3136314/the-secret-behind-the-success-of-mirai-iot-botnets.html

Healthcare

Industry Verticals – Healthcare

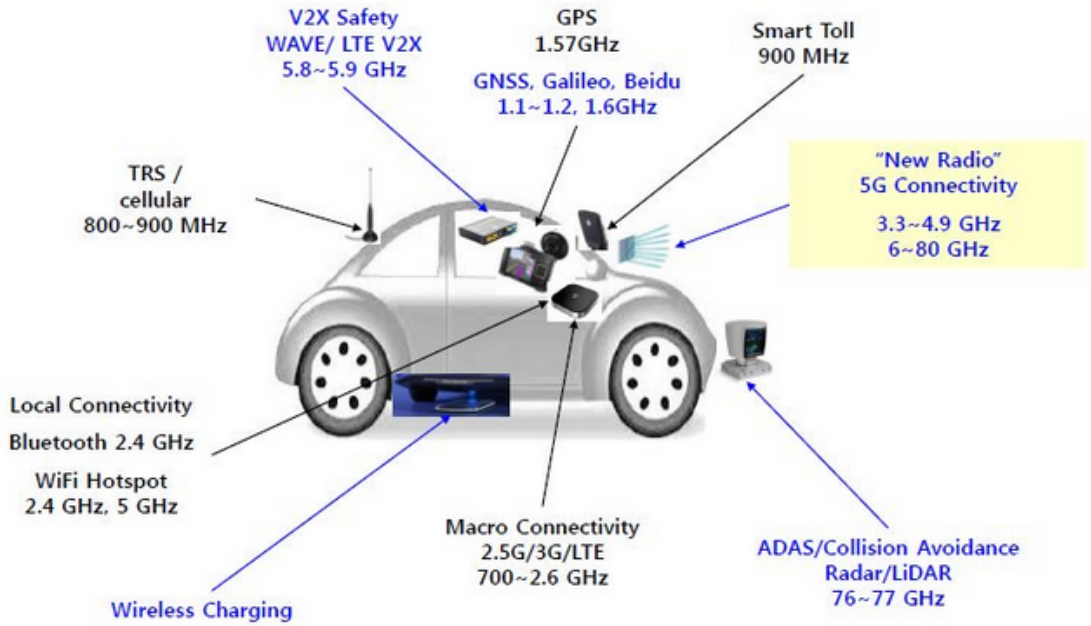
- 5G architecture offers dedicated network slices for applications such as remote health, remote/robotic surgery
- Guarantees of latency bounds, dedicated bandwidth, multiple connections with service guarantees
- Society will see unprecedented healthcare advances, for example:
  - Underserved & remote populations
  - Battlefield situations
  - Continuous monitoring & health emergency avoidance
  - Cross-ecosystem real-time collaboration to save lives

Healthcare served over 5G – new security concerns

- Pervasiveness of devices that talk to each other – too many to track
- The transport could double as man-in-the-middle
- Scale of connections, amount of data – fragility of infrastructure will open 5G healthcare to attacks
- Complexity of device connectivity graph will make intrusion detection a needle in the haystack
- Finally, who is responsible for all the risk?
  - Loss of life and limb
  - How to calculate risk?
  - How and who underwrites the risk?
- Will we need legislation to regulate this new landscape?

Connected Vehicles

Industry Verticals – Connected Vehicles
Future modes of Connectivity



*Source: **Comprehensive Experimental Analyses of Automotive Attack Surfaces**, University of California, University of Washington*

Industry Verticals – Connected Vehicles Current Attack Vectors

Vulnerability Class	Channel	Implemented Capability	Visible to User	Scale	Full Control	Cost
Direct physical	OBD-II port	Plug attack hardware directly into car OBD-II port	Yes	Small	Yes	Low
Indirect physical	CD	CD-based firmware update	Yes	Small	Yes	Medium
	CD	Special song (WMA)	Yes*	Medium	Yes	Medium-High
	PassThru	WiFi or wired control connection to advertised PassThru devices	No	Small	Yes	Low
	PassThru	WiFi or wired shell injection	No	Viral	Yes	Low
Short-range wireless	Bluetooth	Buffer overflow with paired Android phone and Trojan app	No	Large	Yes	Low-Medium
	Bluetooth	Sniff MAC address, brute force PIN, buffer overflow	No	Small	Yes	Low-Medium
Long-range wireless	Cellular	Call car, authentication exploit, buffer overflow (using laptop)	No	Large	Yes	Medium-High
	Cellular	Call car, authentication exploit, buffer overflow (using iPod with exploit audio file, earphones, and a telephone)	No	Large	Yes	Medium-High

Source: Comprehensive Experimental Analyses of Automotive Attack Surfaces, University of California, University of Washington

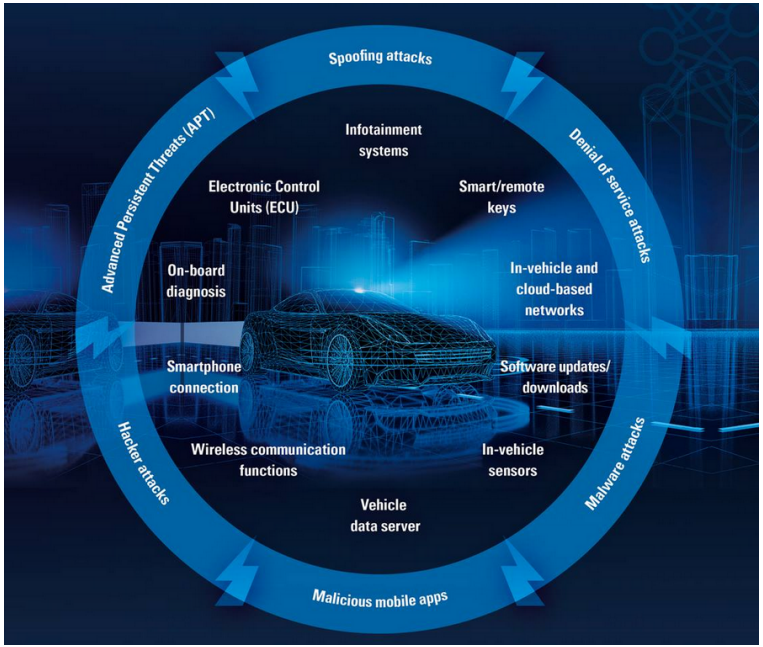
Industry Verticals – Connected Vehicles Multiple Perspectives

In the blue corner are carmakers including Renault, Toyota, and Hyundai who favor a vehicle-to-vehicle system (V2V). This is a short-range technology using an exclusive band of spectrum for inter-car communication. Supporters of this technology argue that is already available, so there will be no delay in introducing vehicles with connected safety features to our roads.

In the red corner are the telcos, alongside car manufacturers such as Volkswagen and BMW. This group is in favor of a long-range cellular system, whereby cars share the airwaves alongside mobile phone signals and other data traffic.

Source: https://www.datacenterdynamics.com/opinions/telcos-fork-road-autonomous-vehicle-infrastructure/

Industry Verticals – Connected Vehicles
Wide Range of Attacks



- Standard range of “IT” breaches (DoS, Malware, etc) now apply to vehicles
- Not only the vehicle which is vulnerable; any cloud-like service also vulnerable
- Scope of attack in centre can be disruptive externally – domain of attack much wider

Source: TÜV Süd

Industry Verticals – Connected Vehicles Wide Range of Impact

- The range of potential failures due to an attack are wide and varied
- Human impact
- Commercial impact

Source: TÜV Süd

Safety by Integrity

All Solutions are now Multi-Owner

The 5G Architecture is split between different actors

5G PLATFORM SECURITY MATRIX		Affected Areas											
Security Layer	Vulnerability Topic	Radio Network and Air Interface			Mobile Core Network			Transport Network (Backhaul and Fronthaul connectivity)			User Equipment, Device		
		HW	SW	SYS	HW	SW	SYS	HW	SW	SYS	HW	SW	SYS
Services, Applications, and Use Cases	QoS	x	x	x	x	x	x	x	x	x			
	Access rights to network slices	x	x	x	x	x	x	x	x	x			
	Vertical use cases											x	x
	Data confidentiality	x	x	x	x	x	x	x	x	x	x	x	x
	Service and application genuineness, safety, and reliability										x	x	x
	Edge computing and service vulnerability				x	x		x	x				
Users and Things	Device and connection genuineness		x	x		x	x				x	x	x
	Resource limitation of M2M devices										x	x	x
	Device identification for M2M and IoT					x	x						
Inter-networking	Operator models			x			x			x			
	Distributed core				x	x	x						
	Use of various RAN technologies	x	x	x		x	x	x	x	x			
	Separate ownership of RAN for rural and enterprise use cases	x	x	x		x	x	x	x	x			
5G Mobile Network and Virtualisation Systems	Legacy core network vulnerabilities			x			x			x			
	Functional split in the new RAN	x	x	x									
	Software-based operations						x						
	Multi-attribute context authentication					x	x				x	x	x
	Multi-network latency				x			x					
	Network slicing				x	x	x	x	x	x			
	System restoration after failover						x						
Physical Infrastructure	NFV and SDN controllers					x		x	x				
	5G new radio and RAN	x	x	x									
	Active Antenna Management		x	x									
	Commodity hardware vulnerabilities	x			x			x					
	Hardware performance deterioration							x		x			
	Physical Security of base stations, computing systems, and core networks	x		x	x		x	x		x			

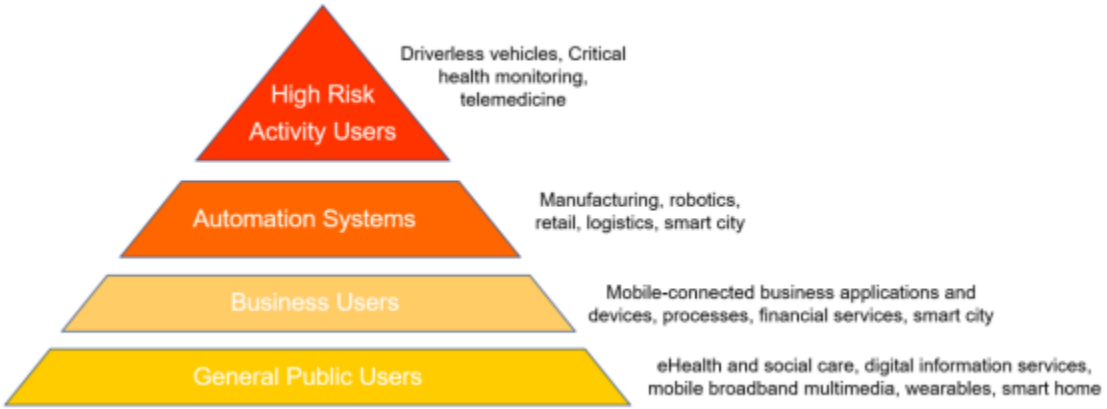
- Total solution relies on components from multiple suppliers
- Security of application is therefore a combination of risks in each area

Source: University of Surrey

Risk Owners Vary by Use Case

Impact on Users

- Scope of risk varies according to use-case
- Risk Calculation and mitigation not currently modelled in system design
- Engineering must include concepts of ethics, human impact and insurance underwriting
- Points to wider use of AI in building outcome-based solutions



Source: University of Surrey

5G Security issues still being understood

criminals will be able intercept 5G communications and steal data because "critical security gaps are present," the group says in their press release. That's in part because "security goals are underspecified" and there's a "lack of precision" in the 3GPP standards

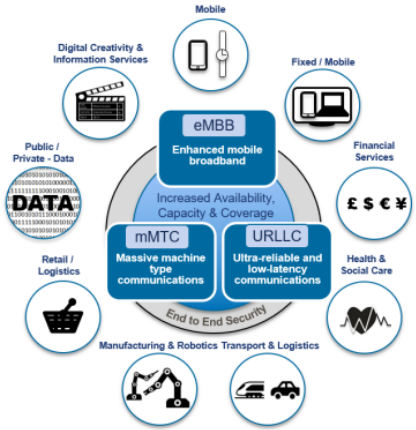
Source: ETH Zurich, the University of Lorraine/INRIA, and the University of Dundee

5G Security – traditional attacks remain

- The common and simplest forms of attacks will be pervasive & quite effective with 5G
  - DoS and DDoS, Intrusion via credential stealing, Sniffing side-channels for information, etc.
- Most attacks will go unnoticed
- Most attacks will remain hidden forever. What has been stolen, how it was used, or to whom was it sold – may not ever be known
- Physical security of remote locations will be a bigger challenge. Why? 5G needs 100x more remote locations

Safety by Integrity

Taking an End to End Cross Layer Approach



- We lack an End-to-End approach to application security due to domain-centric view of SDOs
- We must learn to balance risk appetite and trade-offs per use-case
- Security should be “by design” not added afterwards.
- Risk assessments informed by modelling and trials should become the norm for system design
- Artificial Intelligence may be able to help by providing augmented modelling, but poorly designed AI can itself be a risk and a potential attack surface
- Once deployed, network visualisation and application metadata must be used to ensure compliance with defined risk.

Source: University of Surrey

Conclusions

Conclusions

- 5G Enables a wide-range of differentiated services across multiple substrates
- Multiple actors = multiple exposed attack surfaces
- Security must be considered not just from a technical level, but at different levels of societal risk
- Some solutions are now mission-critical rather than best-efforts
- Do we have the co-ordination and mindset between the Domain SDOs to enable truly secure solutions?

Thank You

Follow Up

{D_Lake, Sumedh_Sathaye}dell.com