Security Challenges and Opportunities in SDN/NFV and 5G Networks

Ashutosh Dutta, Ph.D.
Lead Member of Technical Staff, AT&T
IEEE 5G Initiative Co-Chair
Chief Security Organization
AT&T, New Jersey, USA
Email: ashutosh.dutta@att.com or ashutosh.dutta@ieee.org
June 15, 2017
Talk Outline

- Drivers for Network Virtualization
- Key 5G Characteristics
- Opportunities and Challenges in Security Virtualization
- 5G Security Use Cases
- Industry Standards and Eco System
- Testbed and Proof-of-Concept
- Summary
Emerging Services Trends
Our Connected World is Evolving!

- Internet of Things
- Mobilize Everything
- Big Data
- Social Internet
- mHealth
- Virtual Personal Assistant
- Gaming
- Digital Learning
- Mobile Payment
- Connected Car
- Augmented Reality
- BYOD
- Digital Content
- Smart City
- Asset Tracking
- Video
- Smart Meter
- Wearable Computing
- Samart Grid
- Location Based Services
- Gesture Computing
- UX
- Sensor Network
- Robotics
- Semantic Web
- Entertainment
- WebTV
- Virtual Personal Assistant
- Security
- Voice Recognition
- Social Media
- Internet of Things
- Virtual Personal Assistant
- Software Defined Anything
- User Generate Content
- Knowledge Management
- BYOD
- Internet of Things
- Big Data
What “5G and Advanced Communication Systems” is About

- Smart wearables
- Smart mobility
- Smart parking
- eHealth
- Traffic priority
- Connected house
- Entertainment
- Apps beyond imagination
- Domotics
- Smart Grids
- Security & Surveillance
- Water quality
- Smart Car
- Car-to-car communication
- Utility management
5G Applications Taxonomy

**Enhanced Mobile Broadband**
- Mobile Broadband, UHD / Hologram, High-mobility, Virtual Presence

**Critical Communications**
- Interactive Game / Sports, Industrial Control, Drone / Robot / Vehicle, Emergency

**Massive Machine Type Communications**
- Subway / Stadium Service, eHealth, Wearables, Inventory Control

**Network Operation**
- Network Slicing, Routing, Migration and Interworking, Energy Saving

**Enhancement of Vehicle-to-Everything**
- Autonomous Driving, safety and non-safety features

- Speed: >10 Gb/s $\Rightarrow$ Tb/s
  - Massive Content

- Massive Sensing
  - 1b/s over 10 years off an AAA battery

- Massive Control
  - Response: 1 ms
Key Characteristics of 5G

- Massive MIMO
- RAN Transmission – Centimeter and Millimeter Waves
- New Waveforms
- Shared Spectrum Access
- Advanced Inter-Node Coordination
- Simultaneous Transmission Reception
- Multi-RAT Integration & Management

- D2D Communications
- Efficient Small Data Transmission
- Wireless Backhaul / Access Integration
  - Flexible Networks
  - Flexible Mobility
  - Context Aware Networking
  - Information Centric Networking
  - Moving Networks
Virtualization of Mobile Core (EPC)/IMS

Virtualization of Mobile CORE and IMS

Virtualization of CDNs

Virtualization of CDN

Virtualization of Base Stations

Virtualization of Base Stations (vBS)

Virtualization of Fixed Access

Virtualization of Fixed Access

Virtualization of Home and Enterprise Networks

Legend

VNF

Hardware

Hardware resource pool

SDN/NFV Foundation of 5G – Operator Network Sample Use Case
## What are the Security Impacts?

**Security Benefits of a Cloud-Based Architecture**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Simplification &amp; Automation</td>
<td>Network is less vulnerable to security threats, consistent policy configuration, automated quarantine</td>
</tr>
<tr>
<td>Flexibility &amp; Scalability</td>
<td>Improved incident response, DDoS resiliency, block/reroute of malicious traffic</td>
</tr>
<tr>
<td>Multi-vendor Implementation</td>
<td>Eliminate single point of failure, Security Function Virtualization, Security as a service</td>
</tr>
</tbody>
</table>
Attacker creates a Botnet army by infecting many Mobile devices with a ‘remote-reboot’ malware, attacker then instructs the malware to reboot all the devices at the same time, this will cause excessive malicious Attach Requests, creating a Malicious Signaling Storm.
Malware on Mobile Devices sends malformed IP packets directed to a Customer Cloud Services

Analytics Engine detects the anomaly and sends real-time alerts

Analytics Engine detects the anomaly and sends real-time alerts

SDN Controller dynamically modifies the firewall rules for the related firewalls to thwart the attack

Non-malicious traffic
What are the Security Implications?

Security Challenges of a Cloud-Based Architecture

Common Cloud Infrastructure
- Hypervisor vulnerabilities, VM/Guest OS manipulation, Data exfiltration/destruction

Software Enabled Automated Provisioning
- Orchestration vulnerabilities, Automated network configuration exploits, Malicious misconfiguration, SDN controller exploits

Flexibility & Elasticity
- Amplification of attacks due to elasticity
Security Challenges from Virtualization

Hypervisor Vulnerabilities

To prevent this type of attack, we must:

- Conduct security scans and apply security patches
- Ensure the Hypervisor is hardened and minimized (close vulnerable ports)
- Ensure the access to the Hypervisor is controlled via User Access Management,

1. Hacker exploits a vulnerability in the Open Source code and infects the Hypervisor with a Malware

2. Malware compromises VMs:
   - VM/Guest OS manipulation
   - Data exfiltration/destruction

3. To prevent this type of attack, we must:
   - Conduct security scans and apply security patches
   - Ensure the Hypervisor is hardened and minimized (close vulnerable ports)
   - Ensure the access to the Hypervisor is controlled via User Access Management,
Security Challenges from Virtualization

SDN Controller Vulnerabilities

1. **Vulnerability:** ODL controller did not disable external entity access to XML parser due to a bug in the ODL SDN controller code.

2. **Exploit:** Using Northbound API hacker does XML External Entity (XXE) attack and exfiltration of configuration data from ODL SDN controller.

3. **Mitigation Strategy:** Open source community reported the problem, Patch was applied that disabled external entity access and fixed the problem.

- Hypervisor Vulnerability
- API security
- Orchestration Vulnerability
- Virtual monitoring
- Limited visibility to Mobility/EPC interfaces (e.g. S6a, S11, S8)
- Virtualized firewalls
- Secure boot
- Secure crash
- User/tenant authentication, authentication and accounting
- Topology validation and enforcement
- Performance isolation
- Authenticated Time Service
- Private Keys within Cloud Images
- Detection of attacks on resources in virtualization infrastructure
- Security monitoring across multiple administrative domains (i.e., Lawful Interception)
Network Function Virtualization
Security Challenges and Opportunities

- DDoS Mitigation Scheme
- Security Function Virtualization
- Exploit Orchestration Vulnerability
- DDoS/Attacks from the Internet
- Exploit Hypervisor Vulnerability
- Amplification Attacks Enhanced by Elasticity Function
- Orchestration
  - vMME
  - vHSS
  - vPCRF
  - vS-GW
  - vP-GW
  - vPCEF
- Hypervisor
- Common Hardware
- SDN

Existing Threats
New Virtualization Threats
Security Opportunities

DDoS Mitigation Storm by Mobile Devices
Attacks from User Plane by Mobile Devices
Exploit Hypervisor Vulnerability
Exploit Orchestration Vulnerability
DDoS/Attacks from the Internet
Amplification Attacks Enhanced by Elasticity Function

Mobile Devices (Smartphones, M2M, IoT)
LTE RAN
S1-MME
S1-U
SGi

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
5G Pillars for Security

RAN
(Cloud RAN / vRAN)

Network Slicing

Mobile Edge
## Security Opportunities and Challenges of 5G

### Radio Access Network

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>• The 5G networks will facilitate many more devices (IoT) accessing the RAN with shared access</td>
<td>• Potentially increases the risk of RAN resource overload via Distributed Denial of Service (DDoS)</td>
</tr>
<tr>
<td>• Programmability and Virtualization of RAN will adapt to dynamic nature of traffic and multi provider access</td>
<td>• Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack at the base station</td>
</tr>
<tr>
<td>• Massive MIMO and densification will enable high capacity mobile broadband traffic</td>
<td>• Jamming can potentially be launched against control-plane signaling or user-plane data messages</td>
</tr>
<tr>
<td>• SoftRAN (cRAN) in 5G networks will have embedded DoS detection and mitigation functions</td>
<td>• Compromised IoT devices are orchestrated to launch packet injection attacks</td>
</tr>
<tr>
<td>• Dynamic Radio Resource Scheduling would significantly reduce the risk of jamming attacks targeting mission critical devices</td>
<td>• External flooding attacks may be launched by a botnet consisting of large number of bots</td>
</tr>
<tr>
<td>• Access to control plane and media plane at the base station will enable security monitoring of traffic</td>
<td>• Increased risk of compromise shared resources</td>
</tr>
</tbody>
</table>
DDOS attacks against Network Infrastructure

- Overload of the signaling plane by a huge number of infected M2M/IOT devices that attempt to gain access
- Overload of the signaling plane by a huge number of infected M2M/IOT devices that transmit intermittently and simultaneously
- Resource Starvation at cRAN vFW
- Leverage IOT for Distributed Denial of Service
- Resource Sharing by multiple service providers at cRAN
- Deliberate triggering of network and overload mechanisms
- Bulk configuration
5G will Facilitate many more Devices (IoT) accessing the RAN

Risk of 5G RAN Resource Overload

Use Case: Leveraging IoT for Distributed Denial of Service (DDoS) Attack against 5G RAN

Malicious hackers create a Botnet army by infecting many IoT devices with a ‘remote-reboot’ malware, these malicious hackers then instruct the malware to reboot all the devices in a specific area at the same time, this will cause excessive malicious Attach Requests, creating a Malicious Signaling Storm (Distributed Denial of Service (DDoS) attack against RAN).

5G will facilitate billions of mobile devices accessing the RAN due to increased mobile video sessions, M2M, IoT and RAN-WiFi interoperability

Potential Solution:
1. Develop DDoS detection and mitigation functions into the Cloud RAN functions (e.g. Key Security Indicators)
2. Cloud RAN elasticity feature should scale-out to sustain the higher traffic load

This Distributed Denial of Service (DDoS) attack can overload RAN resources
Virtualization (NFV and SDN) is the Foundation upon which 5G will be Built

**Use Case:** CRAN (Cloud RAN) Resource Starvation due to 5G RAN Firewall Functions

A significant increase in malicious traffic from millions of IoT devices to 5G RAN

5G will facilitate billions of mobile devices accessing the RAN due to increased mobile video sessions, M2M, IoT and RAN-WiFi interoperability

vFirewall VNF in the Cloud RAN to detect and mitigate malicious traffic (Mobile Edge protection)

A significant increase in malicious traffic causes the vFW to demand more compute resources, as a result, starving the other Cloud RAN VNFs

**Potential Solution:**
1. Hypervisor Separation
2. Intelligent VM resource allocations
5G will Increase the Possibilities for Multiple Providers to Collaborate on a System
Increase the Risk of Compromise Shared Resources

*Use Case:* Compromise Shared Resources

5G will increase the possibilities for multiple providers to collaborate on a system.

**Compromised 3rd Party Provider VNFs** can have the following impact on Cloud RAN:
1. Shared resource starvation
2. VM/Guest OS manipulation
3. Data exfiltration/destruction

**Potential Solution:**
1. Hypervisor Separation
2. Intelligent VM resource allocations
3. vFirewalls

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
## Opportunities

- Reduced Latency for authentication for time sensitive applications
- Security Context at the Edge of the network
- Reduced handover time and Data off-loading
- Server Computation at the edge of the network
- Edge Detection and Mitigation

## Challenges

- Persistent caching of old Security Association by both the UE and visited network will weaken security
- Sensitive security assets are compromised at virtualized functions at the edge
- Use of multiple access technologies may require multiple types of network credentials to authenticate a user
- Attacker can gain connectivity or carry out a spoofing, eavesdropping or data manipulation attack during context transfer
- Man-In-The-Middle Attack at the Mobile Edge Server
Security Use Cases for Mobile Edge Cloud (Reference. NGMN)

- Storage of Sensitive Security Assets at the Edge
- Third party applications on the same platform as network functions
- User Plane attacks in Mobile Edge Computing Environment
- Exchange of Sensitive Security Assets between core and Mobile Edge
- Trust establishment between functions at the core and at the edge
- Subscriber authentication within the visited network
- Secure storage of credentials to access IMS network
- Access to 5G core over non-3GPP network access
- User plane data security over less trusted 3GPP network accesses
- Management of credentials to access non-3GPP network access
Mobile Edge Cloud – Use Case
Storage of Sensitive Security Context at the Mobile Edge

- Sensitive security assets are compromised at virtualized functions at the edge.
- An attacker could maliciously reuse them to gain connectivity or carry out a spoofing, eavesdropping or data manipulation attack.
- Sensitive Security Assets stored at the mobile edge should be encrypted.
- Threat to sensitive assets while temporarily decrypted also needs to be addressed.

IOT type applications require low latency, faster authentication and hence, need security context to be stored at the edge of the network.

Recommended Solutions:
1. Virtual Firewalls at MEC
2. Encryption at the Edges
3. IDS/IPS to detect and mitigate spoofing and eavesdropping
4. Data Plane
Mobile Edge Computing – Use Case
Third Party Applications and Network Functions Co-exist

- These applications may exhaust resources that are needed by network function

Recommended Solutions:
- Run both the edge computing applications and the network function(s) in robustly segregated virtual machines.
- Assign higher priorities for NFV applications
- Intelligent VM Resource allocations
Mobile Edge Computing – Use Case
Exchange of sensitive Assets between Core and Mobile Edge

- Sensitive Security Assets exchanged with the mobile edge should be encrypted so that these assets are not compromised.

1. Virtual Firewalls at MEC
2. Encryption at the Edges
3. IDS to detect and mitigate spoofing and eavesdropping

VNFs in the Network Slices:
- vEPC
- vHSS
- vS/PGW-C
- vMMF
- vP-CSCF
- vS-CSSCF
- vHSS

MEC Server

5G Core

Network Slices:
1. Network Slice 1
2. Network Slice 2
3. Network Slice 3
4. Network Slice 4

Control Plane

D Plane

Data Plane

Internet

Recommendations:
- An attacker could maliciously reuse them to gain connectivity or carry out a spoofing, eavesdropping or data manipulation attack.

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Consistently low latency application may require very fast authentication procedures at attachment or during handover.
This may force subscriber authentication to be done entirely within the visited network.

Persistent caching of old SAs by both the UE and visited network weaken security.
There is risk of an old key leaking and being abused.

User plane latency can be minimized by re-using an old security association (SA), while in the meantime running AKA and acquiring a new security association.

Recommended Solutions:
1. Encryption at the Edges
2. IDS/IPS to detect and mitigate spoofing and eavesdropping
3. Timely expiration of temporary SAs
### Opportunities

- Scalability by way of separation of control plane and data plane
- Flexible QoS for different types of applications
- VNF and other Third Party Applications can co-exist
- On demand resource utilization
- Increase the possibilities for multiple providers and multi-function networks to collaborate on a system

### Challenges

- Denial of Service to other slices
- Exhaustion of security resources in other slices
- Side Channel Attacks Across Slices
- Impersonation attacks against a Network Slice instance within an Operator Network
- Impersonation attacks against different Network Slice managers within an Operator Network
- Sealing between slices when UE is attached to several slices
Security Use Cases for Network Slicing (Ref. NGMN)

- Denial of Service to other slices
- Exhaustion of security resources in other slices
- Side Channel Attacks Across Slices
  - Controlling Inter-Network Communications
  - Instantiation time Impersonation attacks against Network Slice Manager
  - Impersonation attacks against a Network Slice instance within an Operator Network
  - Impersonation attacks against different Network Slice managers within an Operator Network
- Different Security Protocols or Policies in different slices
- Hybrid Deployment Model
- Sealing between slices when UE is attached to several slices
Network Slicing - Use Case
Side channel attacks across Network slices

If an attacker can observe or influence how code runs in functions in slice-1, she/he may be able to affect the running of code in functions in the slice-2 VM, or extract information about the running of code in slice-2.

This may allow side channel attacks – in particular, timing attacks – that extract information about cryptographic keys or other secrets in slice-2.

1. Avoid co-hosting on the same HW slices that have very different levels of sensitivity, or very different levels of vulnerability to influence by an attacker.
2. Deploy proper isolation mechanism so that: observing or influencing how code runs in one VM should not allow an attacker to influence or deduce anything about how code runs in another VM on the same HW.
## 5G Ecosystem – Massive Undertaking – (Not a complete List)

<table>
<thead>
<tr>
<th>5G Standards/Forum</th>
<th>Sample 5G Vendors</th>
<th>Sample 5G Research</th>
<th>Sample 5G Operators</th>
</tr>
</thead>
<tbody>
<tr>
<td>3GPP</td>
<td>NOKIA</td>
<td>5G LAB Germany</td>
<td>AT&amp;T</td>
</tr>
<tr>
<td>ETSI</td>
<td>HUAWEI</td>
<td>AT&amp;T</td>
<td>Verizon</td>
</tr>
<tr>
<td>IETF</td>
<td>SAMSUNG</td>
<td>GMD Fokus</td>
<td>KDDI</td>
</tr>
<tr>
<td>IEEE</td>
<td>INTEL</td>
<td>5G LAB Berkeley</td>
<td>Telefonica</td>
</tr>
<tr>
<td>ATIS</td>
<td>ERICSSON</td>
<td>Stanford</td>
<td>DoCoMo</td>
</tr>
<tr>
<td>NGMN</td>
<td>ALTIOS</td>
<td>Brooklyn Poly</td>
<td>Bell Canada</td>
</tr>
<tr>
<td>WWRF</td>
<td>National Instruments</td>
<td>Rutgers WINLAB</td>
<td>Telus</td>
</tr>
<tr>
<td>5GPP</td>
<td>Arraysys</td>
<td>ON Labs</td>
<td>Orange</td>
</tr>
<tr>
<td>ITU</td>
<td>NEC</td>
<td>GA Tech</td>
<td>Vodafone</td>
</tr>
<tr>
<td>FCC</td>
<td>Cisco</td>
<td>Kings College</td>
<td>BT</td>
</tr>
<tr>
<td>5G Ensure</td>
<td>KeySight</td>
<td>University of Surrey</td>
<td>T-Mobile</td>
</tr>
<tr>
<td>Open Source</td>
<td>Phazr</td>
<td>Others ...</td>
<td>Telecom Italia</td>
</tr>
<tr>
<td>(ONF, Linux Foundation,</td>
<td></td>
<td></td>
<td>Sprint</td>
</tr>
<tr>
<td>ONOS, ODL)</td>
<td>Others ...</td>
<td></td>
<td>Telecom Italia</td>
</tr>
</tbody>
</table>

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
IEEE 5G and Beyond Initiative

  - Active Participation from 18 Societies and Organizational Units
    - Communications Society
    - Computer Society
    - Solid States Circuits
    - Signal Processing
    - Vehicular Technology
    - Technology and Engineering Management
    - Antenna Propagation Society
    - Instrumentation & Measurement
    - Power and Energy Society
    - Electromagnetic Compatibility Society
    - Intelligent Transportation Society
    - Microwave Theory and Techniques
    - IEEE Standards Association
    - Educational Activities
    - Future Directions
    - Consumer Electronics
    - Council on Radio Frequency Identification
    - Aerospace and Electronic System Society

- Identified Working Groups and Projects for 2016/2017
IEEE 5G and Beyond

IMS 2017 INTERNATIONAL MICROWAVE SYMPOSIUM
4 - 9 JUNE 2017 HONOLULU, HAWAI'I

IEEE MTT-S and IEEE ComSoc are offering a special joint 5G Summit at IMS2017.
June 5-6 2017, Honolulu, Hawai'i

Click to learn more!

What's New
- Feature Article
  - How 5G Could Bring Internet Access to Remote Areas

Technology Spotlight
- Collaboration is Critical for 5G Network Slicers

Useful Links
- Join the IEEE 5G Initiative Team
- Call for Volunteers
- IEEE 5G Summit
- 5G Talks: Read Q&A Interviews with IEEE experts
- Infographic: On the Road to 5G

IEEE International 5G Summit
9G Summits in 2017
- Lisbon, Portugal
  - Monday, January 29, 2017
- Delhi, India
  - Thursday, February 9, 2017
- Shanghai, China
  - Monday, September 18, 2017
- Cape Town, South Africa
  - Monday, September 18, 2017
- Beijing, China
  - Monday, December 11, 2017
- Mexico City, Mexico
  - Monday, December 11, 2017

IEEE 5G Summit in 2016
- Lisbon, Portugal
  - Monday, January 29, 2016
- New Delhi, India
  - Monday, February 9, 2016
- Shanghai, China
  - Monday, September 18, 2016
- Cape Town, South Africa
  - Monday, September 18, 2016
- Beijing, China
  - Monday, December 11, 2016
- Mexico City, Mexico
  - Monday, December 11, 2016

IEEE 5G Summit in 2015
- Lisbon, Portugal
  - Monday, January 29, 2015
- New Delhi, India
  - Monday, February 9, 2015
- Shanghai, China
  - Monday, September 18, 2015
- Cape Town, South Africa
  - Monday, September 18, 2015
- Beijing, China
  - Monday, December 11, 2015
- Mexico City, Mexico
  - Monday, December 11, 2015

IEEE 5G Summit in 2014
- Lisbon, Portugal
  - Monday, January 29, 2014
- New Delhi, India
  - Monday, February 9, 2014
- Shanghai, China
  - Monday, September 18, 2014
- Cape Town, South Africa
  - Monday, September 18, 2014
- Beijing, China
  - Monday, December 11, 2014
- Mexico City, Mexico
  - Monday, December 11, 2014

IEEE 5G Summit in 2013
- Lisbon, Portugal
  - Monday, January 29, 2013
- New Delhi, India
  - Monday, February 9, 2013
- Shanghai, China
  - Monday, September 18, 2013
- Cape Town, South Africa
  - Monday, September 18, 2013
- Beijing, China
  - Monday, December 11, 2013
- Mexico City, Mexico
  - Monday, December 11, 2013
IEEE 5G and Beyond Initiative Structure

Typical Initiative Organization

Steering Committee Co-Chairs
Ashutosh Dutta
Gerhard Fettweis

Staff Program Director
Harold Tepper

Technology Roadmap

Major Project Two

Education Track
- Education Working Group

Publications Track
- Publications Working Group

Web Portal Track
- Web Portal Working Group

Conferences Track
- Conferences Working Group

Standards Track
- Standards Working Group

Content Development Track
- Content Development Working Group

Community Development Track
- Community Development Working Group

Industry Outreach Track
- Industry Outreach Working Group

Project A

Project B
5G Initiative Working Groups

Working Group Scope

**Education Track**
(R. Ting, R. Annaswamy)

Define, develop and manage portfolio of offerings/activities including:
- eLearning Modules
- Tutorials
- Webinars
- Podcasts
- Google Hangouts

**Publications Track**
(C-L. I, G. Li)

Define, develop and manage portfolio of offerings/activities including:
- eNewsletter
- Journal, Transactions
- Magazine
- Supplements to other publications
- Special issues in other publications

**Web Portal and Content Development Track**
(J. Irvine
Alex Wyglinski)

Determine, source and manage content placed on portal
- By-lined articles
- Q&As
- Expert Interviews
- Whitepapers
- Scenarios/Use Cases
- Media Interviews
- Analyst Briefings

**Conferences Track**
(A. Dutta, L. Ladid)

Manage Initiative events
- Conferences
- Workshops

Determine and manage participation in other events
- Patron
- Exhibitor
- Panelist
- Keynote
5G Initiative Working Groups

**Working Group Scope**

**Standards Track**
(A. Gelman, P. Nikolich)
- Manage portfolio of activities including:
  - New projects
  - Workshops for needs definition and connection with technology developers
  - Roundtable program for industry leaders
  - Engagement with SDOs and other external organizations

**Branding/Marketing Track**
(B. Das)
- Develop and source content for posting / publication including:
  - 5G rebranding
  - Messaging
  - Marketing Collaterals
  - Logo Development

**Community Development Track**
(J. Irvine, A. Wyglinski)
- Establish and grow a broad IEEE 5G Community including:
  - IEEE Technical Community
  - Collabratec
  - Twitter
  - LinkedIn
  - Facebook
  - FlipBoard

**Industry Outreach Track**
(M. Lu, M. Condry)
- Drive engagement with industry including:
  - Partnerships
  - Training
  - Career Development
Emerging services are evolving rapidly
• SDN/NFV is an enabler and Foundation for 5G
• 5G-specific application across many verticals adds new security requirements
• Comprehensive security architecture is essential to take care of security challenges
• Security opportunities in this new virtualized environment
• Operators, other verticals (e.g., eHealth, Automotive, Agriculture), VNF vendors and research community need to work together to form a security ecosystem
• Collaboration among Standards and Forums, Testbeds and POCs act as catalyst for Virtualization
Thank you