**Communications Security, Reliability, and Interoperability**

**Council VIII Working Groups**

**September 2021**

**Working Group 1: 5G Signaling Protocols Security**

*Co-chairs:**Brian Daly, AT&T & Travis Russell, Oracle*

*FCC Liaison:**Ahmed Lahjouji*

The Chairwoman of the FCC directs CSRIC VIII to examine and address security vulnerabilities associated with the newly adopted 5G signaling protocol, Hypertext Transfer Protocol Version 2 (HTTP/2), which, like the SS7 and Diameter signaling protocols considered in earlier CSRICs, is vulnerable to attacks. Researchers have discovered security issues related to the HTTP/2 protocol which could place millions of websites at risk of attack.[[1]](#footnote-2) CSRIC VIII will confirm these vulnerabilities and identify others, assess their potential for harm, and recommend safeguards to harden 5G networks and protect critical business and consumer data from these and other cyber threats. CSRIC VIII will also provide recommendations on how to remediate the risks associated with HTTP/2 and prevent them from carrying over to HTTP/3, the next release of the protocol.

***Milestones****:*

* Report on Security Vulnerabilities in HTTP/2, ***September 2022***
* Report on Best Practices to Mitigate Vulnerabilities in HTTP/2 and HTTP/3, ***June 2023***

**Working Group 2: Promoting Security, Reliability, and Interoperability of Open Radio Access Network Equipment**

*Co-chairs:**Mike Barnes, Mavenir & George Woodward, RWA*

*FCC Liaison:**Zenji Nakazawa*

The Chairwoman of the FCC directs CSRIC VIII to provide recommendations to advance security, reliability, and interoperability of Open Radio Access Network (ORAN) equipment in the United States and what new efforts can be undertaken to support secure and interoperable ORAN design and deployment. The Radio Access Network (RAN) is the final link between the network and the phone. It includes the antennae on towers, buildings, and in stadiums, plus the base stations. When a consumer makes a call or connects to a remote server, the antenna transmits and receives signals to and from the consumer’s mobile phone or other handheld device. The signal is then digitalized in the RAN base station and connected into the network. The introduction of ORAN enables mobile network operators to use equipment from multiple vendors and still ensure interoperability.

CSRIC has previously considered security risks in emerging 5G networks. CSRIC VIII will build on this work and expand it as one part of its exploration of the development and deployment challenges facing ORAN technology, including the extent ORAN technology may increase the threat attack surface and how best to mitigate such security challenges.

Further, CSRIC VIII will consider how the FCC can support the goals of developing and deploying secure, open and interoperable networks when the FCC participates in standards-setting bodies like 3GPP and the Alliance for Telecommunications Industry Solutions.

***Milestones****:*

* Report on Challenges to the Development of ORAN Technology and Recommendations on How to Overcome Them, ***December 2022***

**Working Group 3: Leveraging Virtualization Technology to Promote Secure, Reliable 5G Networks**

*Co-chairs: Micaela Giuhat, Microsoft & John Roese, Dell*

*FCC Liaison:* *Jeff Goldthorp*

The Chairwoman of the FCC directs CSRIC VIII to develop recommendations on how virtualization technology can be used to promote the availability of secure, reliable 5G technologies and services solutions from a diverse market of 5G equipment vendors. Most 5G network product sets are vertically integrated and proprietary – factors that contribute to important communications supply chain risks. CSRIC VIII will develop recommendations for how vendor-agnostic, horizontal stack solutions for 5G can be promoted to foster a diverse, competitive, and more secure 5G environment despite the wider attack surface presented. These recommendations should address ways to provide opportunities for smaller vendors that cannot yet manufacture all parts of a vertically integrated, traditional 5G stack.

In its first report on this subject, CSRIC VIII’s will include recommendations on ways in which funds can be made available to promote virtualized environments that result in improved 5G security and reliability; recommendations on ways to promote and overcome obstacles to the availability of virtualized central units (vCU) and virtualized distributed units (vDU) to increase 5G vendor diversity; best practices for reliability and interoperability that should be used by small businesses that contract or outsource as part of a multi-vendor 5G implementation; and other ways to promote a diverse 5G environment to improve 5G security and reliability. CSRIC VIII will also identify whether any additional work is needed from standards bodies such as 3GPP and ETSI on virtualization issues, such as addressing security risks relating to application programming interface (API) security.

In its second report on this subject, CSRIC VIII will include recommendations on steps that the FCC should take (if any) to help coordinate formal standards, informal standards, and any collaborative open-interface community efforts to ensure interoperability in the virtualized 5G space; recommendations on how the FCC can promote 5G collaborations and innovation labs; recommendations on actions the FCC can take do to build confidence in virtualized 5G solutions using open-source cloud computing software; and any other ways in which FCC can promote a diverse, competitive 5G environment.

***Milestones****:*

* + Report on How Virtualization Technologies can be Used to Promote 5G Security and Reliability, ***December 2022***
  + Report on Recommendations on the Role of the FCC in Promoting the Availability of Standards for More Secure, Reliable 5G Environment Through the Use of Virtualization Technology**, *June 2023***

**Working Group 4: 911 Service Over Wi-Fi**

*Co-chairs:**Mary Boyd, Intrado & Mark Reddish, APCO*

*FCC Liaison:* *Rasoul Safavian*

The Chairwoman of the FCC directs CSRIC VIII to explore the public safety benefits, technical feasibility, and cost of options for making Wi-Fi access points and/or unlicensed spectrum available to the public to facilitate access to 911 services. The ubiquitous nature of Wi-Fi access points suggests that, in the long term, various Wi-Fi solutions could be added to the “toolbox” of 911 connectivity options available to consumers, Public Safety Answering Points (PSAPs), and communications providers, and could complement the broader transition to an IP-based Next Generation 911 environment.

CSRIC VIII will bring industry stakeholders together to examine a range of technical issues with the goal of promoting consensus in the Wi-Fi ecosystem to support reliable 911 services (voice and text) under normal conditions and when catastrophic events disrupt mobile service.  The primary focus will be to examine and report on security issues including authentication and access control protocols, solutions to automatically activate Wi-Fi Calling on eligible mobile devices when necessary, automatically determining the 911 caller location and call routing issues, 911 call prioritization, identifying missing standards, and timelines and costs for implementing 911 over Wi-Fi solutions.

***Milestones****:*

* Report on 911 Service over Wi-Fi, ***March 2023***

**Working Group 5: Managing Software & Cloud Services Supply Chain Security for Communications Infrastructure**

*Chair:**Rittwik Jana, VMWare*

*FCC Liaison:* *Saswat Misra*

The Chairwoman of the FCC directs CSRIC VIII to review risks to service provider operations from attacks in service providers’ software and cloud services stacks and develop mitigation strategies for these vulnerabilities.  In order to improve supply chain security in the communications industry, the FCC has barred the use of Universal **S**ervice Fund support to pay for equipment and services produced or provided by any company posing a national security threat to the integrity of communications networks or the communications supply chain, and the FCC will be reimbursing providers to remove, replace, and dispose of insecure equipment and services.  Additionally, prior CSRIC work, such as the CSRIC IV Report on Cybersecurity Risk Management and Best Practices (March 2015), and the CSRIC II Report on Cybersecurity Best Practices (March 2011), focused on attacks that mostly affect traffic on the network or attacks on users through the network.

However, recent breaches of trusted vendors of software have exposed risks in other segments of the supply chain that have resulted in previously trusted systems becoming compromised. Specifically, attackers have inserted malware in to signed code with valid, but compromised, digital certificates.[[2]](#footnote-3) These recent breaches have highlighted that the threat is pervasive and extends well beyond the telecommunications network itself to software components and cloud-based services that service providers rely on to manage and operate their networks. Attacks on these operational networks could have a significant impact on emergency 911 calls and national security communications.

The FCC further directs CSRIC VIII to recommend best practices to mitigate the risks for each vulnerability it identifies, considering the matrix of capabilities of large and small service providers, large and small software vendors, and large and small cloud service providers.

***Milestones:***

* Report on Recommended Best Practices to Improve Communications Supply Chain Security, ***September 2022***
* Report on Recommended Best Practices to Improve Supply Chain Security of Infrastructure and Network Management Systems, ***June 2023***

**Working Group 6: Leveraging Mobile Device Applications and Firmware to Enhance Wireless Emergency Alerts**

*Co-chairs: Farrokh Khatibi, Qualcomm & Francisco Sanchez, Harris County Office of HSEM*

*FCC Liaison: James Wiley*

The Chairwoman of the FCC directs CSRIC VIII to identify the software or functional requirements necessary to allow Wireless Emergency Alerts (WEA) software to pull capabilities from other mobile device applications and firmware to enhance the presentation of WEA alert messages. When WEA launched, mobile device manufacturers in collaboration with Commercial Mobile Service Providers that participate in WEA created specific programming procedures and rules for allowing their WEA applications to access and retrieve WEA messages. These programming procedures and rules are not available to third-party developers and do not currently allow the WEA software to interface with other mobile device functionality. This policy protects consumer privacy and the integrity of WEA messages, but also prevents WEA from leveraging many mobile device capabilities that could make WEA’s presentation of emergency information to the public more effective. To provide just two examples, researchers have found that allowing WEA to leverage the mapping capabilities of popular smartphone applications could reduce the amount of time the public spends trying to confirm that an emergency alert is relevant to them before taking action to protect their lives and property. Mobile devices also often contain a suite of accessibility features that, if leveraged in the WEA context, could make the emergency information that WEA messages contain more accessible to individuals with access and functional needs.

CSRIC VIII will bring together Commercial Mobile Service Providers, mobile device manufacturers, software and firmware developers, public safety and consumer group representatives to define an Application Programming Interface for this purpose, including any features necessary to continue to secure WEA messages and protect consumer privacy. In addition to technical issues, CSRIC VIII should also identify any resource constraints or procedural issues that could affect the timely deployment of this Application Programming Interface and recommend appropriate mitigations.

***Milestones****:*

* Report on WEA Application Programming Interface, ***March 2023***

1. The FCC has learned of four main vulnerabilities and attack vectors related to HTTP/2: (1) slow read attacks, which call on a malicious client to read responses very slowly; (2) HPACK Bombs, which are malicious archive files designed to crash the program or system reading them and often disable antivirus software; (3) Dependency Cycle attacks, which exploit a new flow mechanism designed to optimize networks to instead create an infinite loop which cannot be escaped; and (4) Stream Multiplexing Abuse, which uses security flaws in stream multiplexing functionality to crash servers, resulting in a denial of service to legitimate users. [↑](#footnote-ref-2)
2. Dustin Volz and Robert McMillan, *Suspected Russian Hack Said to Have Gone Undetected for Months* (Dec. 15, 2020), <https://www.wsj.com/articles/suspected-russian-hack-said-to-have-gone-undetected-for-months-11607974376>. [↑](#footnote-ref-3)