Secure 5G:
Transforming the Data Sharing Landscape

Summary of Roundtable, hosted by ATARC in December 2022

WHITE PAPER

With higher speeds, superior reliability, and endpoint to endpoint device connectivity, 5G has the potential to transform how the Government operates in the future. Although not fully deployed, 5G is already reshaping how information is shared and is improving how agencies achieve mission critical goals.

Enforcement and defense agencies rely on 5G to train agents and expand data bandwidth in order to meet the needs of video and image transmission requirements. Experts anticipate 5G will transform supply chain, logistics, and battlefield applications, and give AI and IoT applications a major boost across a range of industry use cases.

> Secure 5G is like saying secure the internet. Where do you start?

But as agencies move 5G systems beyond prototyping in the coming years, it is critical they evaluate security and risks throughout the increasingly complex ecosystem of end user equipment, radio access networks, 5G core networks, and edge computing systems.

The Advanced Technology Academic Research Center recently held a roundtable with Federal Government and industry experts to discuss the various challenges and opportunities of achieving secure 5G.

Achieving Secure 5G

When addressing security within 5G, roundtable participants are considering it from several perspectives. Several working groups and labs in both the public and private sectors are working to test any number of threats and scenarios within an increasingly complex ecosystem that could threaten secure 5G connections.

Secure 5G involves addressing threats to infrastructure, supply chain, and networks, while also standardizing policies and environments to ensure a frictionless user experience. Ultimately, agencies want to achieve the many benefits of fast and reliable 5G while operating through trusted networks.

Challenges with Secure 5G

Repeatedly, roundtable participants shared they are looking for use cases to better design and implement secure 5G. With each new use case, agencies can better determine the security and technology required to achieve secure 5G. As the internet of things (IoT) expands and smart cities become the new normal, the only way to secure 5G in an ever-changing and expanding environment will be through automation and machine learning.

Cybercriminals will no longer target users through structured, internet-based email accounts, but through any connected device. Infrastructure, such as connected cities, connected warehouses, and autonomous vehicles are additional interfaces that will need to be secured if connected to a 5G network.

5G enables secure communication, but it also enables an attacker to deliver threats quicker. Compromised content is now delivered faster, and sometimes in a secure manner through compromised certificates, through mobile devices, which can lead to formalized compromise of other networks and devices.

 info@atarc.org

Recent internal research of a participating agency shows that smishing (text message phishing) and phishing attacks on mobile devices already account for 75% of all phishing attacks. While focusing on technology and security is one side of the 5G coin, the other concerns the user and ensuring a frictionless user experience while maintaining utmost security.

Frictionless User Experience

Agencies are looking to Zero Trust for greater authentication opportunities on cloud-based networks, but roundtable participants struggle to know how to deliver this level of secure, on-demand authentication on mobile in a way that is frictionless for the user. Complicating the challenge for many government agencies is a diverse user base connecting to networks across the world.

How do we architect in a frictionless, balanced, secure way?

While the U.S. may have secure 5G standards and policies in place, foreign countries where Federal employees are working may not. Several roundtable participant agencies are working to develop national 5G standards, while partnering with international organizations and foreign countries to ensure the policies are globally protective.

Supply Chain Risk Management

In addition to 5G networks operated by private and foreign entities, agencies are challenged with the security risks of the 5G supply chain. Supply chain issues intersect all aspects of 5G development from software developers and vendors down to the customer. To ensure 5G is secure, agencies must be confident in all aspects of the supply chain, which is an impossible feat without automation software.

Although still a concern, roundtable participants are encouraged by the possibility of a significant improvement in the supply chain with the passage of the Chips Act. When chips are manufactured in the United States under secure regulations, agencies will have confidence that technology or devices connecting to their infrastructure can be better identified and trusted.

Because the landscape changes with such frequency, Federal agencies will need to seek guidance from experts, vendors, and organizations conducting 5G modeling and testing. Roundtable participants foresee a point in the near future where applications themselves will transcend as standalone threat vectors, just like mobile devices have in the past few years.

Next Steps with Secure 5G

As 5G technology advances, the Federal Government and its partners aim to continue testing and modeling ideas and use cases to ensure secure 5G. In a lab environment, new ideas can be tested against standards and new solutions can be affirmed. These proven insights will then help agencies with their buying power and general knowledge in the space.

Agencies can also learn from private 5G efforts and use cases. Several participating agencies recently took a 5G tour of carriers, vendors and labs across the country to learn best practices and develop use cases for the Federal Government.

For events on this and other topics, please see ATARC **Events Calendar**. To learn more about and get involved with the **ATARC Secure 5G Working Group**, reach out to **workinggroups@atarc.org**.

