5G, Security, and You

By: Nir Kshetri and Jeffrey Voas

Kshetri, Nir and Voas, J. (2020). "5G, Security, and You", IEEE *Computer,* 53(1) 62 - 66.
https://doi.org/10.1109/MC.2020.2966106

Abstract:

As the increased capacity of 5G has changed the process of viewing, managing, and controlling data security, it also brings added security concerns.

Keywords: mobile computing | data security management | 5G mobile communication | computer crime | artificial intelligence | government | smart phones | computer hacking

Article:

The world's major economies have already launched or are planning to launch 5G cellular service. By October 2019, China's Huawei had secured more than 50 contracts in 30 countries.[1] ZTE had already won 35 commercial 5G supply contracts.[2]

The security features of 5G are not fully understood, which engenders trust concerns.[3] Because it is so new, organizations have been curious about 5G and security. Governments have also taken a conservative and cautious approach to 5G deployment. A report from the European Union (EU) noted that 5G deployment may lead to scenarios where hostile states or other nefarious actors could take control of critical infrastructures and systems such as power grids, oil and gas refineries, transportation systems, pipeline operations, smart vehicles, police communications, and even home appliances. Foreign 5G vendors have been viewed as untrustworthy. One report argued that foreign 5G suppliers may face pressure from their governments to facilitate cyberattacks serving their home countries' national interests.[4] In this article, we review several security features of 5G.

5G Security

5G does have security features. For instance, network virtualization can minimize the use of physical hardware to run networks and perform network functions. In this way, it may be possible to minimize cyberattacks.[10] 5G providers can use authentication systems to identify different devices, such as smartphones, sensors, and kitchen appliances, and thus customize security updates.[10] In addition, application providers are developing systems that provide end-to-

end data encryption. In 2018, about half of all Internet traffic was encrypted, and this percentage is expected to increase.[11]

However, due to 5G being somewhat novel, many security vulnerabilities are unknown. One group of researchers has already identified 11 different vulnerabilities with 5G protocols.[12] Nefarious actors could potentially exploit these vulnerabilities to expose a 5G user's location; downgrade their service to older generation (for example, 4G) data networks; track calls, texts, and online activities; and engage in other harmful acts.[13] For instance, by using inexpensive software-defined radios, the researchers were able to engage in service downgrade attacks, which can switch the service from 5G down to 4G or put the device into a limited service mode. By doing this, the device's international mobile subscriber identity number could be revealed unencrypted.[12]

Table 1. The key security features of 5G.

5G feature	Explanation	Implications for security
Speed and latency	Higher speeds are available: up to 10 GB/s of 5G (https://www.fiercewireless.com/europe/itu-outlines-5g-roadmap-towards-imt-2020) compared to 100 Mb/s for 4G (https://news.itu.int/5g-nordic-baltic-economies/). Lower latency is provided: 1–2 ms (0.001 or 0.002 s) compared to the average 50 ms (0.05 s) of 4G.	• Bad actors can download data faster from devices they break and increase the potential scale of denial of service attacks. • Technical impact may be amplified.
Data transmission and storage	Collected data are likely to be stored at the edge instead of being transported to a more central location.	• Edges may not have the same level of security as central locations. • Nefarious actors can install backdoors in mobile base stations to intercept/manipulate data from the radio access network's access points.
Use of SDN, AI, and ML	SDN, AI, and ML are used to provide specific capabilities for varying use cases and ensure given levels of speed and latency.	• Early generation AI may contain security vulnerabilities. • If an SDN controller is compromised, hackers may gain access to devices they control.
Network slicing	A single network can provide varieties of heterogeneous services	• It is possible to offer different and flexible levels of security depending on user needs.
Devices connected	A wide range of devices (for example, home appliances, industrial automation equipment, cars, laptops, and televisions) exists compared to mainly cellular phones in 4G	• The attack surface may increase. • Inexpensive connected devices often lack security features.
Nature of use cases supported	More specialized use cases are supported.	• Hackings on critical activities can have extremely adverse consequences. • Technical impact may be amplified.

SDN: software-defined networking; AI: artificial intelligence; ML: machine learning.

Table 1 shows how key features of 5G relate to security. First, 5G cellular networks have higher bandwidth and lower latency. Verizon reported maximum 5G download speeds of 1.1 GB/s in Chicago[14] compared to average 4G download speeds in the United States of from 15.3 MB/s to 28.8 MB/s depending on the time of the day.[15] A downside to this is that if hackers break into a

device connected to 5G, they may be able to download personal data and other information much faster than on 4G.[5] Cybercriminals may take advantage of 5G's low-latency and high-bandwidth capabilities to increase the potential scale of a distributed denial of service (DDoS) attack. Faster speeds may also lead to greater functionality for attackers. Huge amounts of data flow from machine to machine, artificial intelligence (AI), the Internet of Things (IoT), and other sources could lead to amplified technical impacts.[6]

Second, 5G is likely to employ edge computing, which involves colocating computing, storage, and networking functions closer to where the data are generated instead of transporting them to more centralized locations. This is done to reduce costs and the amount of power required, conserve bandwidth, and enhance performance in terms of latency. Edges may not have the same level of security as a centralized location. Nefarious actors can also install backdoors in mobile base stations to intercept and manipulate data from the access points of the radio access network (RAN). It is not easy to detect hackers' activities in this situation. For example, the systems could appear to be operating normally even if cybercriminals are copying and manipulating data.[7]

Third, AI and machine-learning (ML) tools are often employed to manage software-defined networking (SDN) and network slicing[16] and enable high speeds and low latency.[17] The earlier generation of AI used for this purpose may not be mature enough for 5G and thus contain security vulnerabilities.[7] If an SDN controller is compromised, a hacker may be able to gain privileged access to the devices it controls.[18] The hacker may be able to cause substantial damage to the connected devices.

Fourth, using SDN, a single network may provide a variety of heterogeneous services or "slices" with specific capabilities for varying highly tailored services for different needs. Each slice may be uniquely purposed and thus may need individual security capabilities. For instance, public safety communication systems such as 911 may need higher levels of security than online gaming systems.[19]

Fifth, a wide range of devices, such as home appliances; industrial automation control devices; cars; televisions; shipping containers; tiny climate monitoring sensors; and laptops, next-generation tablets, and smartphones, are likely to be connected to 5G. A working party developing 5G standards has specified at least 1 million devices per square kilometer. The attack surface may increase with the number of inexpensive connected devices because not enough consideration is given to security in designs. For example, it is not practical to install a firewall on most such devices due to insufficient memory. According to Gartner,[5] the number of IoT devices will increase from 14.2 billion in 2019 to 25 billion by 2021. IoT devices account for 16% of traffic but 78% of mobile malware.[20] Financial and practical considerations may prevent the owners of these devices from securing them.

Sixth, unlike previous generations, 5G will support more specialized use cases such as e-health and connected autonomous vehicles. Security issues in some of these cases have greater risks. For instance, the magnitude of the economic and social costs of hackings targeted at activities such as autonomous vehicles and remote surgery could be great.[8]

5G, Business, And Government

5G supports new architectures, business models, and actors and creates additional vulnerabilities. Cybersecurity models need to adapt to satisfy requirements related to authentication, accountability, and nonrepudiation.[21]

Table 2 presents generalized findings concerning organizations' perceptions of 5G security, which appear to have led to a somewhat negative assessment of 5G and may have slowed down its adoption. Organizational concerns in most of the surveys reported are related to the nature of 5G. For governments of some major developed countries, concerns associated with Chinese 5G players such as ZTE and Huawei are clearly visible and prevalent. Countries such as the United States, Australia, and New Zealand have banned Huawei's 5G equipment.[26] In December 2018, the Japanese government also banned both Huawei and ZTE from network hardware procurement.[27]

Table 2. Surveys of 5G security perspectives.

Survey conducted by	Conducted/ released in	Major findings
Ericsson's 5G Readiness Survey	2017	• 79% of respondents from industries stated that security and privacy concerns were a barrier to 5G adoption. • Security ranked as the third most essential feature in 5G services.[21]
Multinational law firm Osborne Clarke	January 2019	• 74% responded that security and privacy concerns hindered the adoption of the IoT and 5G in the energy sector.[22]
Business Performance Innovation Network and A10 Networks	May 2019	• 84% of mobile respondents expected 5G would significantly increase security and reliability concerns.[23]
Reuters' survey of Japanese films	May 2019	• 88% would favor domestic telecom carriers for 5G.[24]
OpinionMatters' survey of more than 250 chief information and security officers in Singapore	September 2019	• 98% expressed security concerns about 5G deployments. • Among these respondents, 55% thought that 5G will allow more destructive cybercrime activities and 54% believed 5G will create more cyberattack opportunities.[25]

In May 2019, the U.S. Department of Commerce blacklisted Huawei by adding it to the entity list.[28] This means that U.S. firms cannot do business with Huawei without obtaining a government license.[8] To place more restrictions on Huawei and ZTE, in October 2019, the U.S. Federal Communications Commission (FCC) put forward a proposal that bans companies receiving government money from purchasing equipment or services from these firms. The FCC argued that if Huawei's 5G equipment operates in sensitive locations such as near a U.S. military base, China could ask Huawei to install a secret backdoor or malware, and U.S. officials may not be in a position to know about it.[29]

Since Huawei is in the U.S. Department of Commerce's entity list, Google cannot supply Android services, updates, or apps to Huawei 5G handsets.[9] Huawei decided to delay the sale of its 5G-enabled Mate 30 smartphone series in Europe, which is its largest market outside China. The company noted that the value and usability of these 5G smartphones would be reduced without Google apps.[2]

The alarms raised about Chinese firms by countries such as Australia, the United States, Japan, and New Zealand have also triggered security fears among EU countries.[9] EU officials have expressed concerns related to the use of China-originated 5G technologies in critical infrastructures and systems, such as road and rail management, and even household devices. The director of the Czech National Cyber and Information Security Agency, Dusan Navratil, argued that Chinese laws require companies such as Huawei to cooperate with intelligence services, and, therefore, using Huawei products in critical systems might pose national security threats for the Czech Republic.[30]

Negative news stories and government pressure have resulted in bias against foreign 5G suppliers. For instance, most Japanese companies favor domestic carriers for 5G (Table 2). In January 2019, the British telecom company Vodafone, which operates in 26 countries, decided to pause the use of Huawei equipment in certain networks in European countries due to security concerns.[31]

In summary, 5G is changing how data security is viewed, managed, and controlled. 5G offers a new attack surface and more targets for nefarious actors. Be on guard.

References

1. E. Kania and L. Sheppard, "*Why Huawei isn't so scary foreign policy*," Oct., 2019. [Online]. Available: https://foreignpolicy.com/2019/10/12/huawei-china-5g-race-technology/
2. L. Tao, "ZTE steps up 5G network gear deployment overseas as capital spending in China is set to decline," *South China Morning Post*, Oct., 2019. [Online]. Available: https://www.scmp.com/tech/gear/article/3035254/zte-steps-5g-network-gear-deployment-overseas-capital-spending-china-set
3. E. Feng and A. Cheng, "China's tech giant Huawei spans much of the globe despite U.S. efforts to ban it," *NPR*, Oct., 2019. [Online]. Available: https://www.npr.org/2019/10/24/759902041/chinas-tech-giant-huawei-spans-much-of-the-globe-despite-u-s-efforts-to-ban-it
4. Bloomberg, "Hostile state takeover tops Europe's list of 5G rollout worries," *Data Center Knowledge*, Oct., 2019. [Online]. Available: https://www.datacenterknowledge.com/security/hostile-state-takeover-tops-europe-s-list-5g-rollout-worries
5. N. Huber, "A hacker's paradise? 5G and cyber security," *Financial Times*, Oct., 2019. [Online]. Available: https://www.ft.com/content/74edc076-ca6f-11e9-af46-b09e8bfe60c0
6. M. Kuo, "The quest for 5G technology dominance: Impact on US national security," *The Diplomat*, Jan., 2019. [Online]. Available: https://thediplomat.com/2019/01/the-quest-for-5g-technology-dominance-impact-on-us-national-security/
7. T. Wheeler and D. Simpson, "Why 5G requires new approaches to cybersecurity," *Brookings*, Sept., 2019. [Online].

Available: https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

8. J. Leonard and I. King, "Five months after Huawei export ban, U.S. companies are confused," *Los Angeles Times*, Oct., 2019. [Online]. Available: https://www.latimes.com/business/story/2019-10-24/huawei-export-ban-us-companies-confusion

9. M. Peel, "EU eyes tougher scrutiny of China cyber security risks," *Financial Times*, 2019. [Online]. Available: https://www.ft.com/content/3d13c208-0545-11e9-99df-6183d3002ee1

10. J. Marinho, "*What's new in 5G security? A brief explainer*," Ctia, Washington, D.C., June, 2019. [Online]. Available: https://www.ctia.org/news/whats-new-in-5g-security-a-brief-explainer

11. P. Rogers, "Cisco expert on building and securing 5G networks of tomorrow," *Intelligent CIO*, Sept., 2018. [Online]. Available: http://www.intelligentcio.com/africa/2018/09/10/cisco-expert-on-building-and-securing-5g-networks-of-tomorrow/

12. S. R. Hussain, M. Echeverria, I. Karim, O. Chowdhury, and E. Bertino, "5GReasoner: A property-directed security and privacy analysis framework for 5G cellular network protocol," in *Proc. ACM Conf. Computer and Communications Security (ACM CCS)*, Nov.11–15, 2019, London, pp. 669–684. doi: 10.1145/3319535.3354263. [Online]. Available: http://www.documentcloud.org/documents/6544575-5GReasoner.html

13. L. H. Newman, "As 5G rolls out, troubling new security flaws emerge," *Wired*, Nov., 2019. [Online]. Available: https://www.wired.com/story/5g-vulnerabilities-downgrade-attacks/

14. K. Hall, "Median speeds for UK 5G four times faster than 4G, but still way behind US and South Korea," *Register*, Oct., 2019. [Online]. Available: https://www.theregister.co.uk/2019/10/28/first_look_into_5g_reveals_median_speeds_up_to_four_times_faster_than_4g/

15. M. Potuck, "US average 4G download speeds ranked 47th among 77 countries in large-scale study," *9to5Mac*, Feb., 2019. [Online]. Available: https://9to5mac.com/2019/02/20/4g-speeds-us-performance/

16. SDxCentral, LLC, "*Topic hub: Artificial intelligence*," Denver, CO. Accessed on: Dec.20, 2019. [Online]. Available: https://www.sdxcentral.com/big-data/artificial-intelligence/

17. M. Robuck, "AT&T turns up AI for drones, load balancing, 5G build out," *FierceTelecom*, Sept., 2019. [Online]. Available: https://www.fiercetelecom.com/telecom/at-t-turns-up-ai-for-drones-load-balancing-and-5g-build-out

18. J. Kirk, "*What's riding on 5G security? The Internet of Everything*," BankInfoSecurity, Princeton, NJ, Jan., 2018. [Online]. Available: https://www.bankinfosecurity.com/whats-riding-on-5g-security-internet-everything-a-10618

19. G. Reddig, "*In 5G we trust: Why flexible security is a 5G business essential*," Nokia blog, Helsinki, Finland, Dec., 2018. [Online]. Available: https://www.nokia.com/blog/5g-we-trust-why-flexible-security-5g-business-essential

20. T. Mann, "*Nokia VP: 5G security risks are huge*," SDxCentral, LLC, Denver, CO, Oct., 2019. [Online]. Available: https://www.sdxcentral.com/articles/news/nokia-vp-5g-security-risks-are-huge/2019/10/

21. "*5G security - scenarios and solutions*," Ericsson, Stockholm, Sweden, White Paper, 2015. [Online]. Available: https://www.ericsson.com/en/white-papers/5g-security-scenarios-and-solutions

22. P. Gordon, "*Cyber threats continue limiting IoT and 5G adoption, report*," Smart Energy International, Rondebosch, South Africa, Jan., 2019. [Online]. Available: https://www.smart-energy.com/industry-sectors/cybersecurity/data-protection-osbrne-clarke-gdpr-cybersecurity-iot-5g/

23. M. Alleven, "With new 5G revenues come security concerns: Survey," *FierceWireless*, May, 2019. [Online]. Available: https://www.fiercewireless.com/wireless/new-5g-revenues-come-security-concerns-survey

24. T. Kajimoto, "Japanese firms prefer to use 5G networks of domestic carriers," *Reuters*, May, 2019. [Online]. Available: https://www.reuters.com/article/us-japan-companies-5g/japanese-firms-prefer-to-use-5g-networks-of-domestic-carriers-idUSKCN1SS30C

25. E. Yu, "Most Singapore firms experienced data breaches, worried over 5G deployments," *ZDNet*, Oct., 2019. [Online]. Available: https://www.zdnet.com/article/most-singapore-firms-experienced-data-breach-worried-over-5g-deployments/

26. "Japan bans Huawei and ZTE networking hardware," *Industry Herald24*, Oct., 2019. [Online]. Available: https://www.industryherald24.com/japan-bans-huawei-and-zte-networking-hardware/

27. J. Horwitz, "Japan bans Huawei and ZTE 5G networking hardware: Will Canada be next?" *Venture Beat*, Dec., 2018. [Online]. Available: https://venturebeat.com/2018/12/10/japan-bans-huawei-and-zte-5g-networking-hardware-will-canada-be-next/

28. "*Entity List*," Bureau of Industry and Security, U.S. Department of Commerce, Washington, D.C., 2019. [Online]. Available: https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list

29. S. Pham, "Huawei and ZTE could lose what little business they have in the United States," *CNN Business*, Oct., 2019. [Online]. Available: https://www.cnn.com/2019/10/29/tech/fcc-huawei-5g-ajit-pai/index.html

30. R. Muller, "Czech cyber watchdog calls Huawei, ZTE products a security threat," *Reuters*, Dec., 2018. [Online]. Available: https://www.reuters.com/article/us-czech-huawei/czech-cyber-watchdog-calls-huawei-zte-products-a-security-threat-idUSKBN1OG1Z3

31. G. Hutchens, "Huawei poses security threat to Australia's infrastructure, spy chief says," *Guardian*, Oct., 2018. [Online]. Available: https://www.theguardian.com/australia-news/2018/oct/30/huawei-poses-security-threat-to-australias-infrastructure-spy-chief-says

Nir Kshetri is a professor of management in the Bryan School of Business and Economics at the University of North Carolina at Greensboro. Contact him at nbkshetr@uncg.edu.

Jeffrey Voas is the editor-in-chief of *Computer*. He is an IEEE Fellow. Contact him at j.voas@ieee.org.