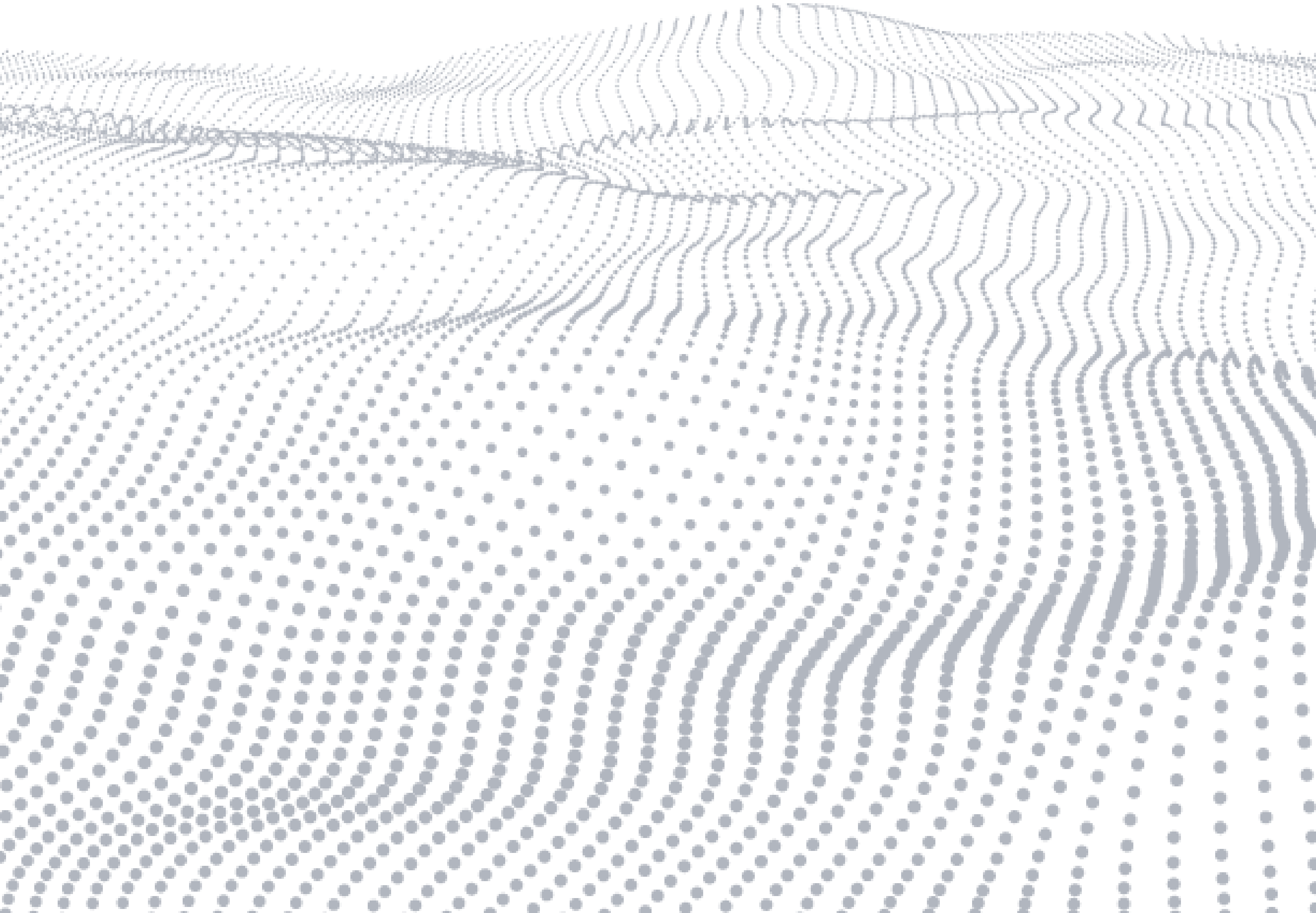
WHITE PAPER

Securing 5G and IoT With Fuzzing



The pervasiveness of wireless communications

Wireless communications are all around us. Our smartphones, Wi-Fi-enabled laptops, and Bluetooth headsets permeate the environment with electronic signals. They let us talk, text, email, view videos, and perform other operations remotely. And now, perched on the cusp of the third decade of the 21st century, wireless communications are set to take a great leap forward with the fifth generation of mobile network communications, more commonly known as 5G. But it's been a long and winding road to this point. So let's revisit it briefly.

5G is poised to make another performance leap with one-tenth the latency, and hundreds of times the capacity, of its immediate predecessor, 4G

Mobile network technology

In the 1980s, mobile network wireless communications had humble beginnings. First-generation handsets, weighing 2 pounds (0.91 kg) and affectionately nicknamed "bricks" for their heft and dimensions, placed the first analog cellular calls.[1] During the 1990s, second-generation digital phones not only made calls but also exchanged Short Message Service (SMS) text messages.[2] By the early 2000s, 3G (third-generation) phones that supported the Wireless Application Protocol (WAP)[3] and primitive attempts at surfing the mobile web[4] made their way to early adopters. By the time iPhone and Android smartphones were introduced, circa 2007–2008,[5] true mobile broadband speed and throughput had arrived with the fourth generation (4G) of wireless telecommunications.[6] Now, 5G is poised to make another performance leap with one-tenth the latency, and hundreds of times the capacity, of its immediate predecessor, 4G.[7]

IEEE 802.11: Continual evolution and convergence with 5G

Mobile network technology was not the only kind of wireless communications evolving during this period. In 1997, its short-range cousin, Wireless Fidelity (Wi-Fi), was standardized by the Institute of Electrical and Electronics Engineers (IEEE) LAN/MAN Standards Committee (IEEE 802) as the 802.11 wireless protocol for local wireless networks.[8] The 802.11 protocol provided the indoor wireless cornerstone that the coming smartphone revolution would build on. But by itself, 802.11 had only partial success, with throughput just up to 2 Mbps and limited range.

By 2003, the 802.11b and 802.11g versions of Wi-Fi promised up to 54 Mbps and an extended range of 50 meters,[9] prompting the release of many Wi-Fi-enabled computers that were forecast to reach a critical mass of 10 million units by 2006.[10] Ever since then, Wi-Fi has made wireless communications ubiquitous in everyday life: at work, home, coffee shops, and airports, and even on the go in cars, buses, trains, and airplanes. The use cases seem virtually unlimited. With Wi-Fi calling and other Wi-Fi innovations since 2015,[11] the consistent growth of wireless communications has kept up the pace as new types of devices and applications extend its usefulness.

The family of Wi-Fi standards has continued to evolve, with increases in range, speed, and throughput with each iteration. The latest release, Wi-Fi 6 (IEEE 802.11ax), came out in 2019 with a theoretical transfer speed of 10 Gbps.[12]

Even with all the achievements of cellular and Wi-Fi technologies to date, the era of pervasive wireless communications is just beginning. Emerging technologies are poised to leverage both 5G and Wi-Fi. Enter the Internet of Things (IoT), which has started to expand wireless communications exponentially, with machine-to-machine (M2M) communications and sensors in the smart grid, autos and trucks, the doorbell in your house, even the clothes you wear.[13]

5G cellular mobile communications

5G will revolutionize many industries, with up to 100 times the speed, 100 times the capacity, and 10 times less latency compared to 4G LTE. 5G enables 10 Gbps downloads—about 600 times faster than 4G.[14] Note that 5G is not a single technology but a constellation of technologies.[15] The higher performance of 5G requires the support of new techniques, such as multiple-input multiple-output (MIMO) antennas, and new spectrums, such as millimeter wave. This new spectrum will require many more wireless access points, some only the size of a smoke detector.[16] In addition, spectrums currently being used by 3G and early 4G networks will need to be repurposed to provide connectivity in rural areas.

Beyond performance increases, the greatest benefit of 5G will be its ability to serve vastly more devices compared to 4G LTE. For example, Ericsson forecasts that more than 20 billion IoT devices will be connected to the internet by the end of 2023, all depending on 5G for this connectivity.[17]

The greatest benefit of 5G will be its ability
to serve vastly more devices compared to 4G LTE

5G and Wi-Fi 5G: What's the difference?

With so much hype around 5G and all the different networks, it might be hard to tell what 5G actually means. Let's clear this up. The "G" in cellular 5G stands for "generation." By contrast, the "G" in so-called Wi-Fi 5G stands for "gigahertz" and refers to the secondary 5 GHz band used by Wi-Fi. So other than the "G" in their names, Wi-Fi 5G and cellular 5G have nothing in common.[18]

But whatever the name, cellular 5G appears here to stay. According to some reports, by 2023, 50% of all new phones will be 5G handsets.[19] Others forecast that by the end of 2020, nearly two-thirds of organizations will deploy 5G.[20] But 5G also encompasses IoT devices, which are significant for organizations, with 59% of those deploying 5G also planning to use it for IoT devices, enabling up to 1,000 sensor-enabled IoT endpoints per square kilometer.[21]

The Internet of Things and connected applications today and tomorrow

As the future linchpin of cellular technology, 5G enables hosts of IoT devices and their connected applications. Some are with us today. Others seem more conceptual.

Smart IoT devices at home could turn on lights, lock doors, and even turn off the dryer with 5G-connected applications.[22] Wearables such as Apple Watches and Fitbits could track health data and report it to apps in near real time with 5G.[23] In the smart city of tomorrow, 5G-enabled IoT functionality in stoplights and atmospheric monitors will ease congestion and determine when industry should shut down to curb air pollution. Already, smart parking meters alert when spots open up, adjusting rates for peak hours.[24] Today, some cars offer an in-car Wi-Fi experience, known as "the connected car," enabling up to 10 devices in a car to be online simultaneously, courtesy of 5G bandwidth.[25]

Security challenges today and tomorrow

In addition to providing superior performance, 5G expands the attack surface of apps and IoT devices that rely on this next-gen network. There will be unknown, novelty attacks in addition to known security exploits. Security breakdowns and exploits on the internet and in public networks have always been dangerous and costly. Past IoT exploits include major headline-grabbing incidents such as these:

- **The Mirai botnet distributed denial-of-service (DDoS) attacks** in 2016 and 2018 used brute force techniques to take over IP cameras, home routers, and other Linux-based IoT devices using default passwords, which are rarely or never changed. Using these IoT devices, Mirai took a large part of the U.S. offline for hours, including high-profile sites such as the New York Times, Spotify, and Reddit.[26]
- **The NotPetya ransomware attack** on PCs, servers, and network-attached storage devices in 2017 spread quickly[27] and caused $10 billion in corporate losses. The combined losses at Merck, Maersk, and FedEx alone exceeded $1 billion. Of course, 5G networks did not exist at the time, but the attack illustrates the high cost of such incursions.[28]

Some wireless vulnerabilities are akin to proofs-of-concept with the potential for significant disruption if exploited in the wild.

4G LTE security exploits

Impersonation attacks in 4G networks (IMP4GT) exploit a vulnerability in the way that mobile devices and base stations authenticate and communicate with one another. This vulnerability enables hackers to fake a base station or impersonate a mobile phone user and device and charge services or send false location information (potentially incriminating innocent people).[29]

Man-in-the-middle (MitM) attacks can occur on 4G LTE where an attacker has set up a network sniffer, or fake base station, to capture the device information of connected devices in an area that can exceed 300,000 square meters. Attackers can tell if a device is Android, iOS, or IoT. Then they can alter the data and settings on these devices, before security is applied, to prevent handovers and roaming or just drain battery life.[30]

Wi-Fi security exploits

The Wi-Fi Protected Access II (WPA2) network security protocol has been around for more than 15 years but is considered unsecure because it allows any device to intercept connections of other devices on the same Wi-Fi network. Zero-day vulnerabilities have been found in WPA2, including KRACK (key reinstallation attack), which enables eavesdropping on Wi-Fi network traffic.[31] Fortunately, test suites to fuzz the WPA2 protocol and TLS authentication are available.

To replace WPA2, in 2018 the Wi-Fi Alliance standards body released the Wi-Fi Protected Access 3 (WPA3) security protocol, which is supposed to be more secure.[32] But despite improved versions of security standards and protocols, there will always be new, unknown attacks, such as the discovery of the Dragonblood vulnerability shortly after WPA3 replaced WPA2.[33]

IoT security exploits

The number of known and still-unknown IoT vulnerabilities is vast, which has huge implications for both the security and safety of certain medical devices. For example, as of March 2020, more than 480 Bluetooth devices were affected by the recently discovered SweynTooth vulnerabilities, which target Bluetooth Low Energy (LE) protocols.[34] These vulnerabilities can cause unexpected public key crashes, where the stack does not expect the public key, and sequential ATT deadlock, when the device cannot handle receiving consecutive ATT request packets without waiting for a response, as two examples.

The environment is target rich for attackers, with forecasts projecting up to 14.6 billion IoT connections by 2022. And because many of these devices include industrial control systems that were not originally intended to connect to the internet, something as straightforward as a network scan can shut down an entire facility.[35]

The case for fuzz testing

Fuzz testing (or fuzzing) can test and exploit the LTE network and help find improper handling of unprotected initial procedures, crafted plain requests, messages with invalid integrity protection, and security procedure bypasses. All these can have far-reaching consequences, from denying LTE services to legitimate users to spoofing SMS messages to eavesdropping on and manipulating user data traffic.

With next-generation 5G leveraging virtualization technologies such as software-defined networking (SDN), hypervisors, and network slicing to run, manage, and scale massive applications and workloads on the network edge, it will become harder to predict and frame the use cases for 5G. Mitigating potential security risks exposed by these new, unknown vectors will also be more difficult.

Fuzz testing can be your first and last line of defense for uncovering new, unknown bugs, vulnerabilities, and crashes that can have severe outcomes.

How fuzzing works

With fuzzing, malformed data is sent to connected devices and applications to surface errors, glitches, system freezes, and weaknesses.[36] Fuzz testing works by sending intentionally malformed inputs to software to see if it fails. Each malformed input is a test case. Failure indicates a found bug, which should then be fixed to improve the robustness and security of the target software.

A fuzzer is a testing program that tests the target software. A useful fuzzer must keep records, produce actionable reports, and provide a smooth remediation process to reproduce failures so that they can be fixed.

Overall, fuzzing is one of the best ways to spot zero-day vulnerabilities that are unknown and have no known workarounds. There are different types of fuzzers. Choosing the most appropriate fuzzer will depend on the goals for testing. For more detailed information on different types of fuzzing, see our white paper What Is Fuzzing: The Poet, the Courier, and the Oracle.

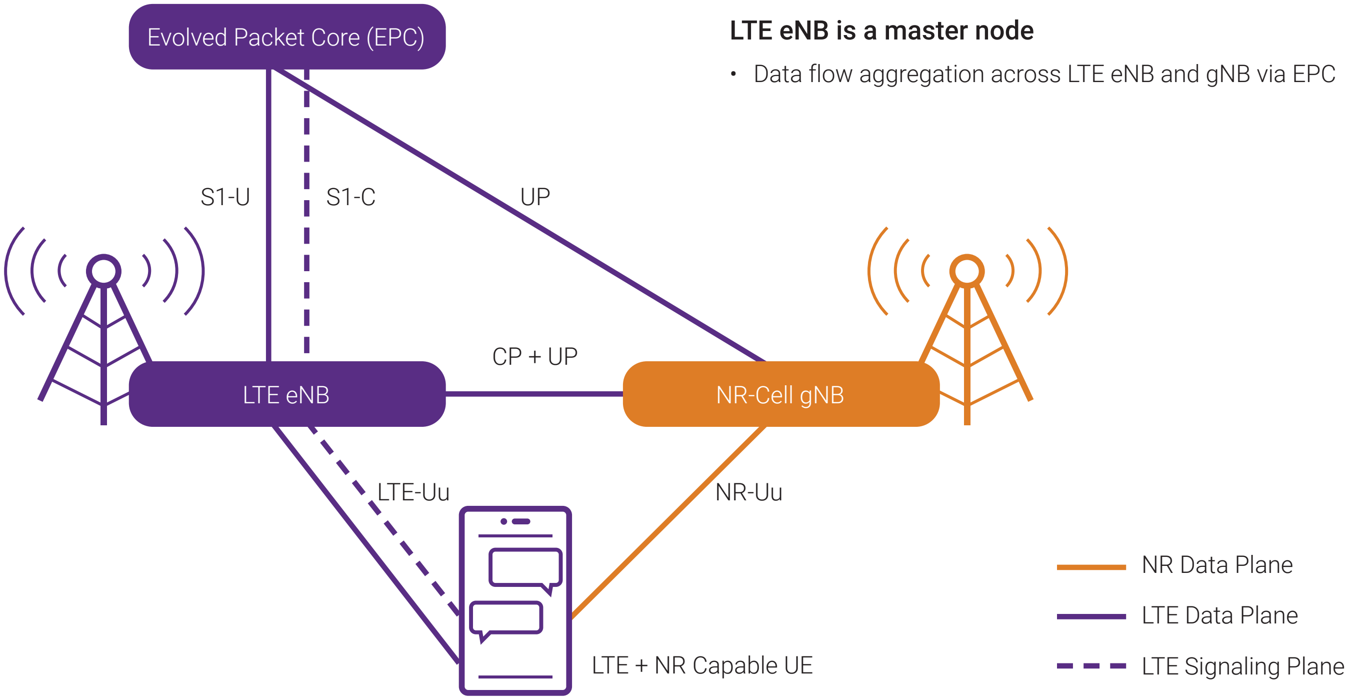
Defensics generational fuzzer

Defensics® Fuzzing is an advanced generational fuzzer geared for enterprises and other organizations that need to discover and remediate security weaknesses in software systems effectively and efficiently. By taking a systematic and intelligent approach to negative testing, Defensics allows organizations to ensure software security without compromising on product innovation, time to market, or operational costs. Defensics builds security into 5G. For example, using a recently added test suite, Defensics can test control plane signaling between a 5G base station and a user device.

The Defensics generational fuzzer is superior to other types of fuzzing and includes close to 300 prebuilt, generational test suites that ensure quick time to fuzz, relieving users from the burden of creating manual tests. Black Duck continually updates the Defensics test suites for new input types, specifications, and requests for comments (RFCs) in support of current and emerging technologies.

Support of next-generation core cellular communications and IoT technologies

Most network equipment manufacturers and service providers have started investing in 5G. Even for the current generation of cellular infrastructure, the underlying 3G/4G protocols still in use are within the scope of 5G, especially in non-standalone (NSA) mode, as the 5G connection is anchored to an LTE eNodeB (eNB) base station[37] and will require fallback to LTE networks for partial operation.[38] See Figure 1.



LTE eNB is a master node

- Data flow aggregation across LTE eNB and gNB via EPC

Figure 1. LTE eNB as master node.

In addition to cellular 4G LTE and 5G, Defensics test suites include a wide range of wireless, Wi-Fi, and Bluetooth test suites that can help in a broad array of core cellular, network, IoT, and media communications testing.

IoT devices and the modern internet

IoT devices form an important part of the modern internet. They depend on a variety of protocols to connect to the internet for critical use cases such as medical devices. But vulnerabilities such as the recently disclosed SweynTooth set of Bluetooth Low Energy (LE) vulnerabilities can impair these devices.[39]

Fortunately, the Defensics fuzzer and Bluetooth LE package of test suites can check the security of IoT devices. For example, Defensics can test an IoT device's vulnerability to crashing by using the Bluetooth LE SMP Client test suite to send an unexpected public key. Or it can test whether an IoT device will freeze, or deadlock, by sending it repeated ATT request packets without waiting for an ATT response using the Bluetooth LE ATT Server and ATT Client test suites.

The Defensics fuzzer can also check IoT devices using test suites for MQTT Client, MQTT Server, IPv4, 802.11 WLAN, and other IoT fuzz testing suites to proactively protect them from these and other types of denial-of-service attacks.

IoT devices have also proven susceptible to botnets. That's because many of them use the popular Linux operating system, which has kernel vulnerabilities. But in recent years, fuzz testing has helped discover and fix these security flaws. A Black Duck R&D team uncovered three such Linux kernel vulnerabilities using the Defensics fuzzer and the NFS3 Server test suite. This team is the same one that, in 2014, used Defensics to discover the Heartbleed encryption vulnerability, which affected millions of businesses and consumers.

4G/5G protocols and cellular communications vulnerabilities

Cellular communications in 5G networks will depend on at least a dozen new protocols and almost another 30 protocols found in 4G LTE networks that have 5G enhancements. For example, the Packet Forwarding Control Protocol (PFCP) is a packet protocol introduced in 5G that's also used in 4G/LTE to connect functional elements in mobile core networks to provide 4G and 5G services.

Other important protocols include S1AP/NAS and NGAP/NAS for signaling user devices and providing mobility and session management. With this expansive attack surface, new, unknown vulnerabilities will inevitably occur.

Defensics can use its PFCP Server, PFCP Client, S1AP/NAS Client, NGAP/NAS Client, and other cellular core test suites to act as a malicious base station or user device and send exceptional or anomalous requests to the test target.

Unconventional development life cycles and custom protocols

Do you have an unconventional development life cycle? Black Duck's experienced Professional Services team can help you identify fuzz testing checkpoints, define fuzz testing metrics, and establish a fuzz testing maturity program.

Or maybe you have custom, proprietary protocols and interfaces you need to secure. You can future-proof them against exploits with the Defensics fuzz testing software development kit (Defensics SDK). It provides a fuzzing framework that enables your organization to develop its own test suites for uncommon, custom, or proprietary protocols.

Conclusion

The impending world of 5G-connected apps, societies, and nations has the promise to revolutionize many industries, including telecommunications, industrial control, gaming, and telemedicine. Higher speeds, lower latencies, and greater throughput will enable applications across the internet that until recently only seemed illusory (e.g., virtual reality, augmented reality).

Along with this increased functionality comes an increase in SDN infrastructure and ecosystem complexity that results in an expanded surface area prone to attacks, plus the integration of 5G into legacy networks, including industrial control systems that were never intended to connect to the internet. These legacy networks have many latent security flaws that will open them up to new, novelty attacks when they make the transition to full 5G and edge computing, and when IoT becomes more pervasive.

But in light of its increased security risks, the next-gen 5G network provides an opportunity for governments and businesses to establish a new, more robust quality and security framework. Increased risks have driven organizations like the National Institute for Standards and Technology (NIST) and 3GPP to produce cyber security frameworks that could become best-practices guides for the industry.

To learn more about how to use fuzz testing for your 5G and IoT devices and applications, visit the Defensics webpage.

Resources

1. GCN, How Much Did the First Handheld Cell Phone Weigh?, Sep. 22, 2011.
2. Techopedia, Short Message Service (SMS), May 28, 2019.
3. Chris Bennett, Wireless Application Protocol 2.0, InformIT, Nov. 9, 2001.
4. NTE, What Is WAP Mobile Web, LoveToKnow, accessed June 29, 2020.
5. Robin Parrish, Which Came First: iPhone or Android?, Apple Gazette, May 3, 2012.
6. Aditi Chakraborty, A Study on Third Generation Mobile Technology (3G) and Comparison Among All Generations of Mobile Communication, International Journal of Innovative Technology & Adaptive Management 1, no. 2 (November 2013).
7. Rahul Gupta, 6 Interesting 5G Wireless Technology Features That Make it Superior to 4G/3G, Guiding Tech, April 4, 2018.
8. CableFree, The History of WiFi: 1971 to Today, May 18, 2017.
9. C. Suresh, V. Vidhya, et al., Wireless Fidelity, International Journal of Research in Computer Applications and Robotics 4, no. 2 (February 2016), pp. 50–59.
10. The Economist, A Brief History of Wi-Fi, June 12, 2004.
11. Chris Neiger, Is Wi-Fi Calling the Future of Wireless?, The Motley Fool, July 12, 2015.
12. Brandon Conroy, What Are the Real Benefits of Wi-Fi 6—Everything You Need to Know, Windows Dispatch, March 8, 2020.
13. Ahlem Saddoud, Wael Doghri, et al., 5G Radio Resource Management Approach for Multi-Traffic IoT Communications, Computer Networks 166 (Jan. 15, 2020).
14. Finley, The WIRED Guide to 5G.
15. Klint Finley, The WIRED Guide to 5G, Wired, Dec. 18, 2019.
16. Wikipedia, Extremely High Frequency, updated June 22, 2020.
17. IoT Business News, Ericsson Forecasts 20 Billion Connected IoT Devices by 2023, Dec. 8, 2017.
18. Colin Berkshire, The Difference Between 5G and 5G, TalkingPointz, April 24, 2019.
19. Rae Hodge, A 5G Phone Boom Is Coming, but Maybe Not Until 2022, CNET, Jan. 22, 2020.
20. Gartner, Gartner Survey Reveals Two-Thirds of Organizations Intend to Deploy 5G by 2020, Dec. 18, 2020.
21. Ibid.
22. Rajesh Mishra, 15 Examples of Internet of Things Technology in Use Today, Beebom, Jan. 31, 2020.
23. Andrew Meola, A Look at Examples of IoT Devices and Their Business Applications in 2020, Business Insider, Dec. 18, 2019.
24. Ibid.
25. AT&T, Connected Car From AT&T—Unlimited Data for Your Car, accessed June 29, 2020.
26. Josh Fruhlinger, The Mirai Botnet Explained: How Teen Scammers and CCTV Cameras Almost Brought Down the Internet, CSO, March 9, 2018.
27. Iain Thomas, Everything You Need to Know About the Petya, er, NotPetya Nasty Trashing PCs Worldwide, The Register, June 28, 2017.
28. Tom Wheeler and David Simpson, Why 5G Requires New Approaches to Cybersecurity, Brookings, Sept. 3, 2019.
29. Ravie Lakshmanan, New LTE Network Flaw Could Let Attackers Impersonate 4G Mobile Users, The Hacker News, Feb. 26, 2020.
30. Karen Epper Hoffman, 5G Inherits Some 4G Vulnerabilities, GCN, Oct. 21, 2019.
31. Charlie Osborne and Zack Whittaker, Here's Every Patch for KRACK Wi-Vi Vulnerability Available Right Now, ZDNet, Oct. 17, 2017.
32. Mohit Kumar, Wi-Fi Alliance Launches WPA3 Protocol With New Security Features, The Hacker News, Jan. 9, 2018.
33. Catalin Cimpanu, Dragonblood Vulnerabilities Disclosed in WiFi WPA3 Standard, ZDNet, April 10, 2019.
34. NetSec.News, More Than 480 Bluetooth Devices Affected by SweynTooth Vulnerabilities, March 5, 2020.
35. Ben Heubl, How to Hack an IoT Device, E&T, June 10, 2019.
36. Techopedia, Fuzz Testing, accessed June 29, 2020.
37. AT&T, 5G Update, accessed June 29, 2020.
38. Telecompaper, 3GPP Approves First 5G Standards, Dec. 21, 2017.
39. U.S. FDA, SweynTooth Cybersecurity Vulnerabilities May Affect Certain Medical Devices: FDA Safety Communication, March 3, 2020.

About Black Duck

Black Duck® offers the most comprehensive, powerful, and trusted portfolio of application security solutions in the industry. We have an unmatched track record of helping organizations around the world secure their software quickly, integrate security efficiently in their development environments, and safely innovate with new technologies. As the recognized leaders, experts, and innovators in software security, Black Duck has everything you need to build trust in your software. Learn more at www.blackduck.com.