SYNOPSYS®

WHITE PAPER

Securing Next-Gen 5G and IoT with Defensics Fuzz Testing

Expansion of the Internet of Things

The evolution of 5G technologies continues to drive advancement in Internet of Things (IoT) devices and their applications. Businesses and homeowners are using the IoT to make commercial and residential buildings more energy-efficient, comfortable, and convenient.[1] Door locks, appliances, thermostats, and smoke detectors are controlled by smart technologies and enabled by 5G connectivity. Cities are using the power of IoT to improve traffic management and other functions, yielding more efficient, effective, and safe communities.[2] Self-driving cars and trucks use dozens of connected devices to safely navigate roadways in a variety of traffic and weather conditions. Conventional vehicles utilize IoT connections to monitor performance and manage computerized systems.[3] By 2025, experts predict there will be 3.74 billion IoT mobile connections in the world, and more than 64 billion IoT devices by 2026.[4]

Security Challenges Today and Tomorrow

However, in addition to enabling superior performance and efficiency, 5G expands the attack surface of applications and devices that run on it. Security breakdowns and exploits on the internet and in public networks have always been dangerous and costly, but IoT and 5G technologies will bring new, unknown attacks as well.

Recent IoT exploits include headline-grabbing incidents such as

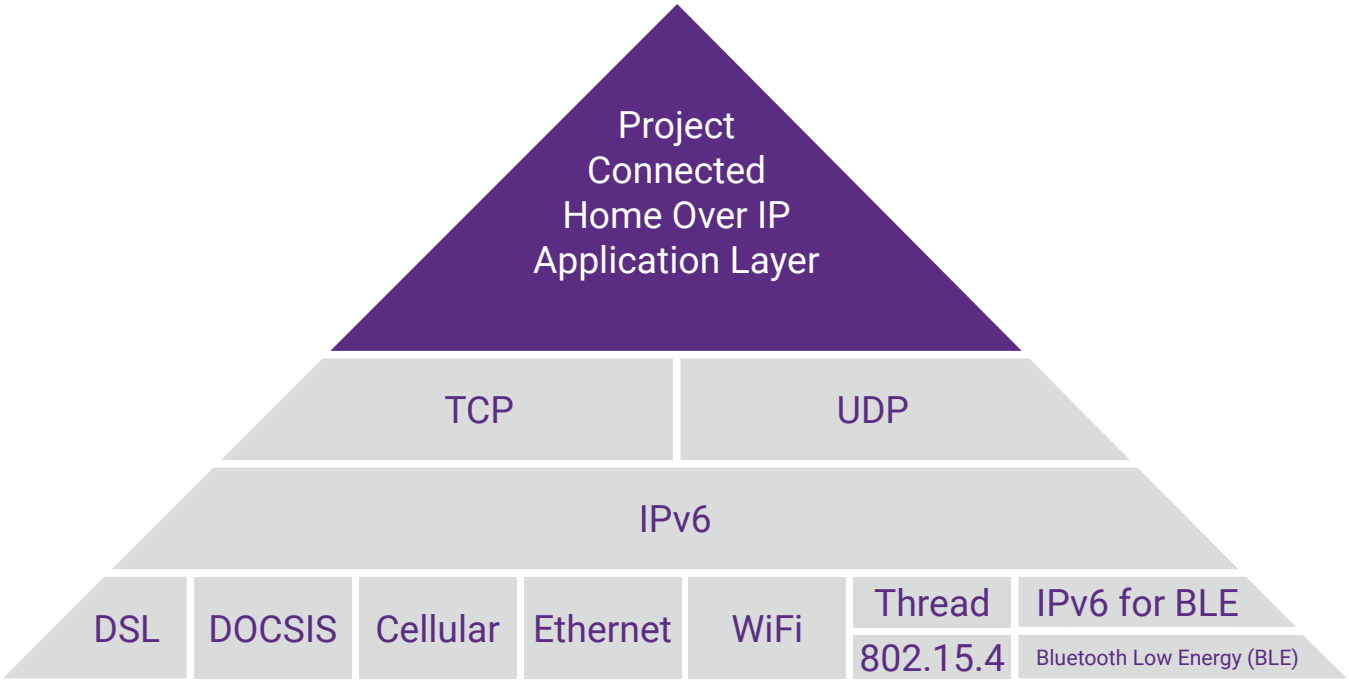
- **The RabbitMQ, EMQ X, and VerneMQ vulnerabilities** in open source message broker applications. The Synopsys Cybersecurity Research Center (CyRC) uncovered input that caused each message broker to consume large amounts of memory, resulting in the application being terminated by the operating system.[5]
- **The BlueFrag vulnerability,** a Bluetooth flaw in Android that affects automotive software.[6]
- **The Kr00k vulnerability,** which affects the 802.11 WPA2 protocol.[7]
- **The Ripple20 vulnerability** affects protocols such as IPv4, IPv6, ICMPv4, DNS, ARP, DHCPv4 and v6, and TCP.[8]
- **AMNESIA:33,** a set of 33 vulnerabilities that impact four open source TCP/IP stacks (up, FNET, picoTCP, and Nut/Net), which collectively serve as the foundational components for millions of connected devices worldwide. These vulnerabilities primarily cause memory corruption, allowing attackers to compromise devices, execute malicious code, perform denial-of-service attacks, and steal sensitive data.[9]
- **BleedingTooth,** a collection of three vulnerabilities in Linux kernel's Bluetooth implementation. By chaining these vulnerabilities, a Google engineer was able to achieve zero-click remote code execution in the target machine.[10]

IoT devices have also proven to be susceptible to botnets because many use the popular Linux operating system, which has kernel vulnerabilities.

The recently disclosed SweynTooth set of Bluetooth Low Energy (LE) vulnerabilities has also disrupted IoT devices.

Industry Standards

The Matter protocol has emerged in recent years as the framework of choice for connectivity standards. It is supported by major players such as Apple, Samsung, Amazon, and Google, and its aim is easing connectivity and interoperability across disparate devices. Matter encompasses multiple layers in the network stack and offers simplicity, reliability, and security built into its design. By building on internet protocol (IP), Matter enables communication across smart devices, mobile applications, and cloud services.



Matter Technology Stack (Thread, Wi-Fi, and 802.15.4 directly relate to IoT and wireless communications)

3GPP and O-RAN

Other groups creating industry standards include

- The Third Generation Partnership Project (3GPP), a global network of companies that develops protocols for mobile communications
- The O-RAN Alliance, a worldwide community of mobile operators, vendors, and academic institutions that strives to make radio access networks more intelligent, open, and fully interoperable

Telecom equipment manufacturers that develop the hardware and software for the core network or the radio access network are required to follow 3GPP or O-RAN specifications.

Defensics Generational Fuzzer

Defensics® 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. Defensics takes a systematic and intelligent approach to negative testing that allows organizations to ensure software security without compromising on product innovation, time to market, or operational costs.

Defensics Builds Security into 5G

The Defensics fuzzer and Bluetooth LE package of test suites work together to check the security of IoT devices. For example, Defensics can test a device's susceptibility to crashing by using the Bluetooth LE SMP Client test suite to send an unexpected public key. It can also 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.

Defensics can also test IoT devices using test suites for MQTT Client, MQTT Server, IPv6, 802.11 WLAN, Zigbee, and others to proactively protect them from denial-of-service attacks.

Fuzz testing has also proved effective in discovering and fixing botnet security flaws. A Synopsys R&D team—the same team that used Defensics to discover the Heartbleed encryption vulnerability in 2014—uncovered three Linux kernel vulnerabilities using the Defensics fuzzer and the NFS3 Server test suite.

Defensics includes about 300 prebuilt, generational test suites that ensure quick time to fuzz, relieving users of the burden of creating manual tests. Synopsys continually updates Defensics test suites for new input types, specifications, and requests for comments in support of current and emerging technologies.

Support of Next-Generation Core Cellular Communications and IoT Technologies

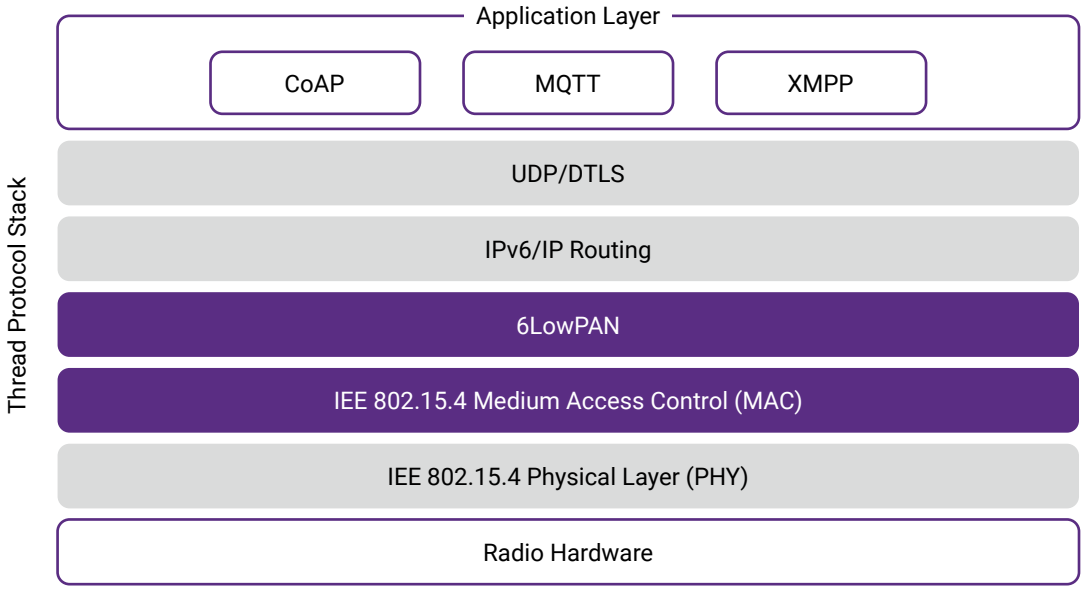
Most network equipment manufacturers and service providers have started investing in 5G. Even for the current generation of cellular infrastructure, the underlying 3G/4G protocols still in use are within the scope of 5G—especially in nonstandalone mode, as the 5G connection is anchored to an LTE eNodeB base station and will require fallback to LTE networks for partial operation.

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

Thread Protocol

The Thread protocol is a Thread Group–defined full-stack solution for wireless personal area networks (WPANs). The protocol is designed for smart home and smart building applications where an IP-network is preferred.

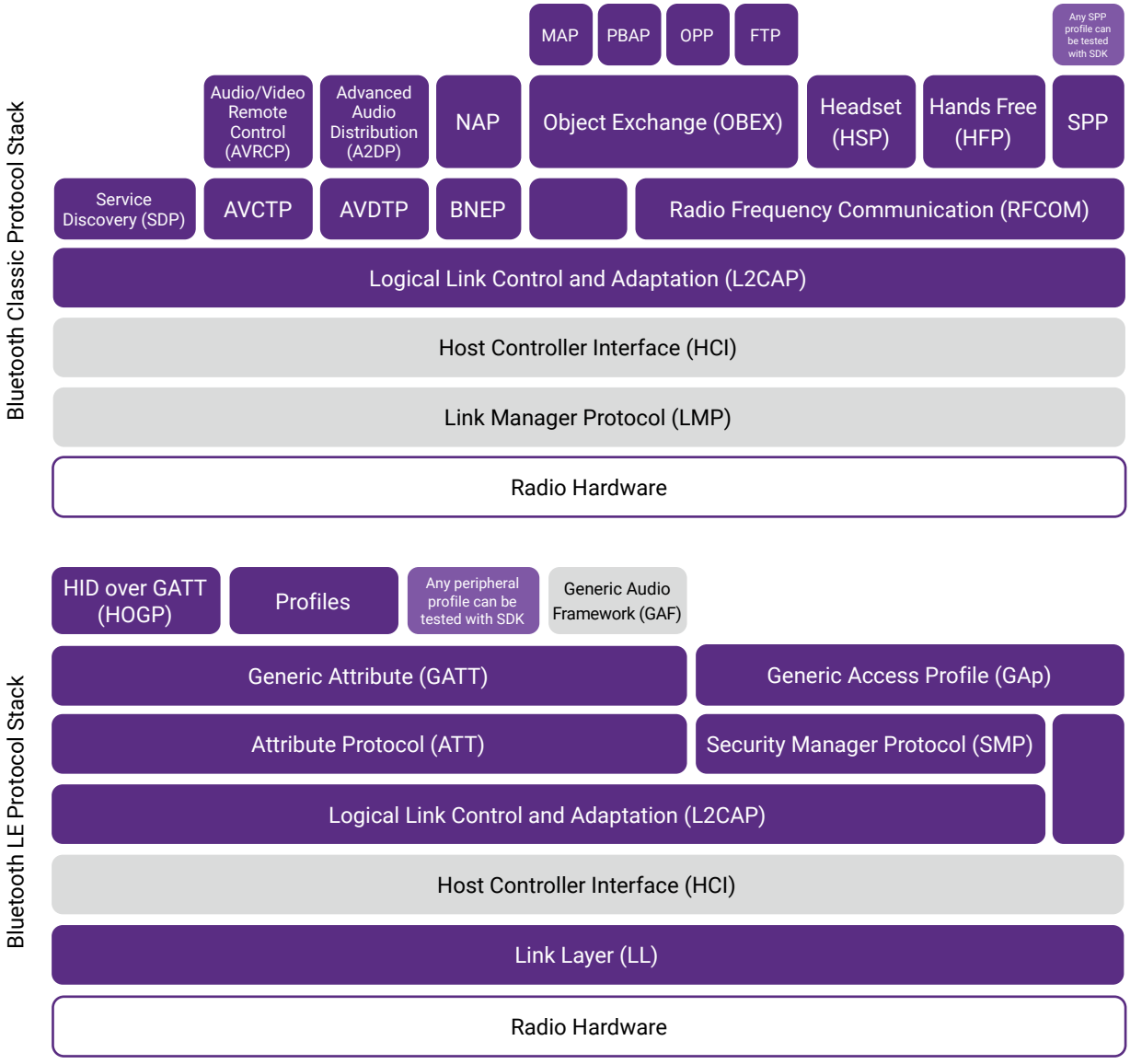
- The Defensics Thread bundle includes two test suites.FuzzBox Thread MAC for testing the IEEE 802.15.4 medium access control (MAC) layer on a Thread device
- FuzzBox Thread 6LoWPAN for testing the 6LowPAN layer (a compressed version of the IPv6 protocol) on a Thread device



Bluetooth Protocol

Defensics test suites cover both Bluetooth LE and Bluetooth Classic protocol stacks.

The Bluetooth stack is split into two main components, host and controller. Zephyr OS is an Apache-licensed real-time operating system backed by the Linux Foundation and many big-industry vendors; it is mainly used in embedded and resource-constrained systems. Zephyr's Bluetooth LE controller is used as part of the Defensics Bluetooth LE fuzzing solution. Zephyr's Bluetooth LE stack's lowest layers were fuzz tested using Defensics Bluetooth LE test suites.



Bluetooth Security Exploits

Eight vulnerabilities were discovered in the Bluetooth LE Link Layer and L2CAP implementation. The vulnerabilities can be divided into three high-level categories.

- **Freeze:** This vulnerability makes it possible for an attacker to remotely cause a freeze or assertion failure on a target device by sending malformed input. In the case of a freeze, the behavior of a target device depends on whether assertions are enabled and if the error handler for fatal errors exists. Because a device usually restarts itself in case of hard faults, an attacker can use this vulnerability to restart the device over the air with single packet when exploiting some other vulnerabilities. In some circumstances, freezing may lead to remote code execution.
- **Deadlock:** Some of the vulnerabilities can cause the target device to misbehave in a way that prevents other devices from connecting to it. The target must be rebooted to recover to normal state.
- **Information leak:** This vulnerability makes it possible for an attacker to gain access to potentially confidential information like encryption keys or information about memory layout. This type of vulnerability can also help an attacker bypass mitigation techniques like address space layout randomization.

The Defensics Bluetooth Suites

- Support FuzzBox OS for running tests in a virtualized environment
- Enable traffic capture to support Bluetooth HCI capture when using local HCI device
- Support running multiple Bluetooth test suites in parallel

WLAN Protocol Stack

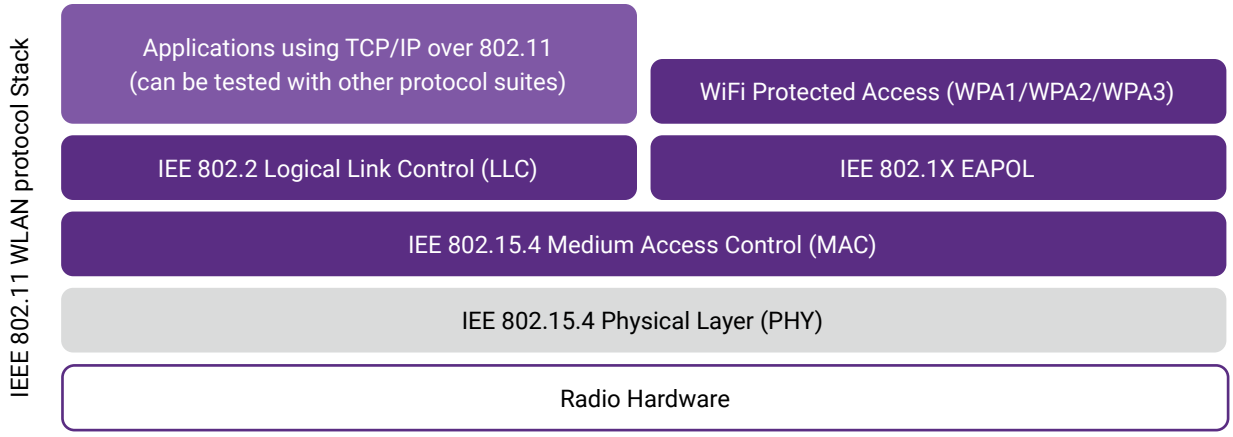
Defensics supports the WLAN protocol stack for Wi-Fi data transmissions.

Defensics WLAN AP FuzzBox package (suite is WLAN client, and test target is AP)

- FuzzBox 802.11 AP for WLAN connection testing
- FuzzBox 802.11 WPA AP for WPA and WPA2 four-way handshake testing
- FuzzBox 802.11 WPA3 AP for WPA3 Dragonfly and four-way handshake testing

Defensics WLAN Client FuzzBox package (suite is AP, and test target is WLAN client)

- FuzzBox 802.11 Client for WLAN connection testing
- FuzzBox 802.11 WPA Client for WPA and WPA2 four-way handshake testing
- FuzzBox 802.11 WPA3 Client for WPA3 Dragonfly and four-way handshake testing



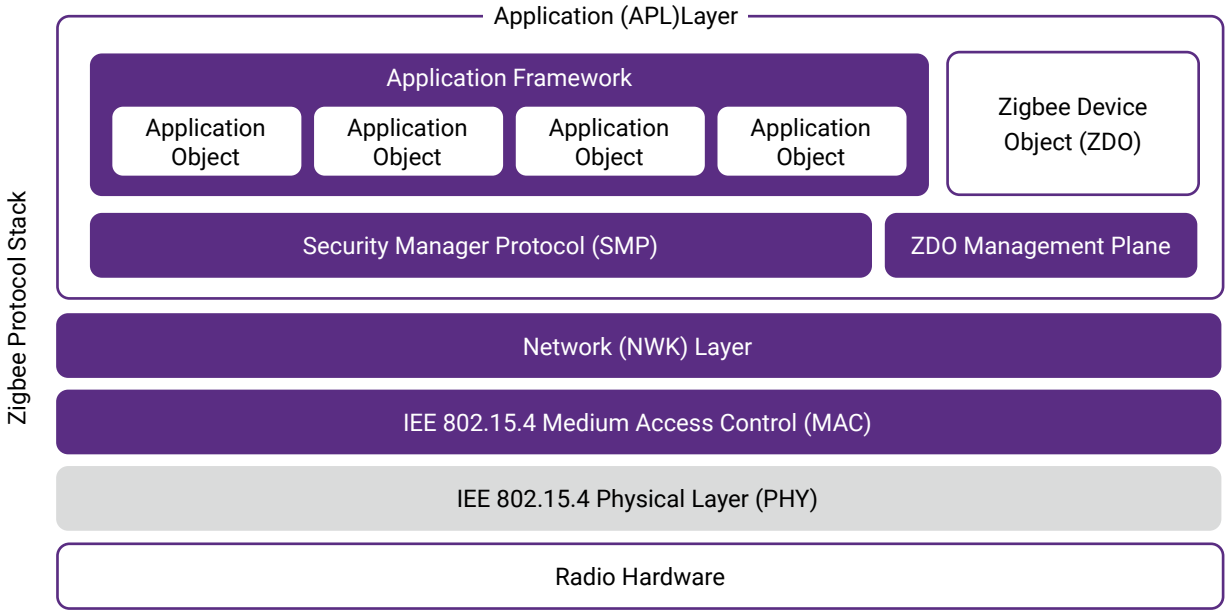
Zigbee Protocol Stack

Zigbee is an IEEE 802.15.4-based specification for wireless mesh networks used by small, low-power digital radios and monitoring devices. Its prominence is expected to increase with the widespread adoption of 5G connectivity.

Defensics supports multiple layers of the Zigbee protocol stack.

Defensics Zigbee FuzzBox package

- FuzzBox Zigbee MAC for testing the IEEE 802.15.4 medium access control layer
- FuzzBox Zigbee NWK for testing the network (NWK) layer
- FuzzBox Zigbee APS for testing the application support sublayer (APS)



Unconventional Development Life Cycles and Custom Protocols

Synopsys supports atypical software development life cycles (SDLCs) and proprietary protocols and interfaces for any organization. The Synopsys Professional Services team can identify fuzz testing checkpoints, define fuzz testing metrics, and establish a fuzz testing maturity program. The Defensics fuzz testing software development kit (Defensics SDK) provides a fuzzing framework that enables any organization to develop its own test suites for uncommon, custom, or proprietary protocols.

Conclusion

5G technologies are revolutionizing many industries, including telecommunications, transportation, telemedicine, and public infrastructure. Higher speeds, lower latencies, and greater throughput enable applications across the internet that seemed illusory until now (e.g., virtual reality and the metaverse).

But this increased functionality also brings an increase in SDN infrastructure and ecosystem complexity that result in an expanded attack surface. The integration of 5G into legacy networks, including industrial control systems that were never intended to connect to the internet, adds to the complexity. These legacy networks have many latent security flaws that make them vulnerable to new attacks when they make the transition to full 5G and edge computing, and when the IoT becomes more pervasive.

Despite these risks, the next-gen 5G network provides an opportunity for governments and businesses to establish a new, more robust quality and security framework. Organizations such as the National Institute for Standards and Technology and 3GPP have responded to these risks by producing frameworks that are considered best practices for the industry.

Fuzz testing solutions such as Defensics can find security vulnerabilities in the software and devices using 5G networks. Defensics generational fuzzer includes 300 prebuilt test suites, as well as custom suites, to protect organizations from unknown vulnerabilities.

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

Endnotes

1. Pratt, Mary K, "Top 8 IoT Applications and Examples in Business," TechTarget.com, Mar. 30, 2022.
2. Ibid
3. Ibid
4. Meola, Andrew, "A Look at Examples of IoT Devices and Their Business Applications in 2022," Apr. 15, 2022.
5. "Synopsys Discovers Denial of Service Vulnerabilities in RabbitMQ, EMQ X, and VerneMQ," IT Security Guru, Jun. 8, 2021.
6. Fingis, Jon, "Android Security Flaw Lets Attackers Send Malware over Bluetooth,"engadget.com, Feb. 9, 2020.
7. Cimpanu, Catalin, "New Kr00k Vulnerability Lets Attackers Decrypt WiFi Packets," zdnet.com, Feb. 26, 2020.
8. Cimpanu, Catalin, "Ripple20 Vulnerability will Haunt the IoT Landscape for Years to Come," zdnet.com, Jun. 16, 2020.
9. dos Santos, Daniel; Dashevskyi, Stanislav; Wetzels, Jos; Amri, Amine, "Amnesia:33—How TCP/IP Stacks Breed Critical Vulnerabilities in IoT, OT and IT Devices," Forescout Research Labs, 2020.
10. Tung, Liam, "Google Warns of Severe 'BleedingTooth' Bluetooth Flaw in Linux Kernel," zdnet.com, Oct. 14, 2020.

SYNOPSYS®

The Synopsys difference

Synopsys provides integrated solutions that transform the way you build and deliver software, accelerating innovation while addressing business risk. With Synopsys, your developers can secure code as fast as they write it. Your development and DevSecOps teams can automate testing within development pipelines without compromising velocity. And your security teams can proactively manage risk and focus remediation efforts on what matters most to your organization. Our unmatched expertise helps you plan and execute any security initiative. Only Synopsys offers everything you need to build trust in your software.

For more information, go to www.synopsys.com/software.

Synopsys, Inc.
690 E Middlefield Road
Mountain View, CA 94043 USA

Contact us:
U.S. Sales: 800.873.8193
International Sales: +1 415.321.5237
Email: sig-info@synopsys.com