POLICY AND REGULATORY ISSUES

Policymakers face a conundrum – promoting the adoption of IoT services to reap its many benefits, while safeguarding societal concerns. This will be a balancing act of oversight and regulation from policymakers to drive investment and consumer adoption while ensuring that safety, security, and privacy frameworks are in place. This column will explore critical national and international IoT policy and regulatory efforts as well as take a deeper dive into specific topics of interest.

Introduction

Douglas C. Sicker

The importance of IoT systems is well known to the readers of this publication, as is the importance to secure these systems. This article focuses on one aspect of IoT, its heavy reliance upon wireless rather than wire-based networking. This reliance raises a host of interesting dependencies and vulnerabilities associated with the radio layer. This article highlights these concerns and provides a set of observations for the IoT community as well as for policymakers.

Internet of Things (IoT) Challenges at the Radio Layer

By Dale N. Hatfield and Douglas C. Sicker

Wireless Dependence and Vulnerabilities

The use of wireless connections for IoT devices is pervasive. In many cases, IoT devices such as sensors and actuators could be connected by wire to a core network. However, in many cases the need for mobility, the cost of installation and maintenance of wiring, or simple convenience dictate the use of wireless connections. But when one examines the systems that are being used or proposed for making such connections, they include wireless access technologies such as Wi-Fi, Zigbee, Bluetooth, SigFox, LoRa, 6LoWPAN, 4G/LTE (NB-IoT) and various 5G implementations. In short, the future of IoT is synonymous with the use of wireless or Radio Frequency (RF) links for connections between devices as well as the balance of the network.

The convenience and other benefits of utilizing wireless links in IoT are overwhelming, but in at least one respect, the implications are troubling for a technology upon which our nation and other nations are increasingly reliant. The fundamental problem is that wireless-based systems are inherently open to physical/radio layer disruptions to a much greater extent than wire-based systems. These disruptions include jamming, spoofing, sniffing (intercepting), and unintentional interference at the radio layer of the protocol stack.[1] Unlike attacks on a wired-network, no penetration of the physical network is required to attack a wireless link. A wireless signal is effectively available for exploitation to anyone in a nearby area. Hence, an attack can be accomplished at a distance using other radio transmitters/receivers to jam or spoof signals or, in the case of sniffing, to intercept the signals on wireless paths or links.

To prevent such attacks at the RF Layer, one could, with no humor intended, put the receivers in a metal box (a Faraday Cage) to prevent the damaging signals. But doing so would obviously block the desired signal, say a voice or data message from a first responder, and render the system ineffective. In short, to allow a wireless-based system to carry out its intended function, it must be open, in the sense that the signal is available to any other system operating at the proper frequency, and because of this, it might be vulnerable.

Wireless services of all kinds are at risk. For example, short-range Bluetooth communications between an IoT device and its control node could be (1) jammed by sending an interfering signal that disrupts the link; (2) spoofed so that the device connects to a rogue node, not the intended one, thus facilitating all kinds of mischief associated with man-in-the-middle (MITM) cybersecurity attacks; and (3) sniffed (passively intercepted) so that both meta-data and user information can be intercepted without detection.

Examples of longer range networks are Commercial Mobile Radio Systems (CMRS), such as 4G/LTE and 5G, which can not only be jammed but are also subject to spoofing and sniffing attacks. Spoofing and sniffing in this instance includes International Mobile Subscriber Identity-catchers, or IMSI-catchers, which are capable of a number of modes of attack including communications interception ("eavesdropping") and location tracking. Although IMSI-catchers have legitimate uses in law enforcement and homeland security applications, they can also be acquired and operated by individuals with nefarious motives.

An example of a still longer radio link subject to disruption is a ground station communicating with a receiver in a geostationary satellite thousands of kilometers away. The disruption could be produced, for instance, by a perpetrator generating a high-power jamming signal to disrupt the Telemetry, Tracking and Command (TT&C) system that is critical to satellite "housekeeping" operations. Even more disruptive, perhaps, are the well-publicized incidents that involve the jamming and spoofing of GPS/GNSS Positioning, Navigation and Timing (PNT) signals with potentially severe consequences militarily, commercially, and scientifically. Moreover, the precise timing signals themselves are used in the synchronizing of digital communications signals used in IoT systems, among many others. This can dramatically increase the impact of GPS/GNSS disruptions.

Further Observations

The following observations provide additional context for the wireless vulnerabilities discussed in the previous section:

• First, while there are a plethora of significant efforts by different federal agencies to address cybersecurity vulnerabilities in commercial settings, they rarely consider RF Layer jamming, spoofing, and sniffing attacks explicitly and, if they do, it is often a narrow, perfunctory or even dismissive handling. Instead, they focus on the upper layers of the protocol stack. That is, they worry about such threats as (a) spoofing attacks on email applications while ignoring spoofing attacks at the RF Layer, or (b) Denial of Service (DoS) attacks at the upper levels of the stack while ignoring "Denial of Spectrum" attacks at the RF Layer.

• Second, while dismissing radio layer attacks in wireless systems may be the right public policy choice in some, if not many, situations, an appropriate risk assessment demonstrating that the threat can be downplayed or dismissed is often missing. Or, if a risk assessment has been conducted, it is not available to (a) organizations or individuals evaluating or imple-

[1] For the purposes of this paper, the term RF Layer is taken to include both electromagnetic radiation and the PHY layer of the OSI protocol stack.

menting a potentially vulnerable system, and (b) independent research groups who attempt to identify and warn appropriate authorities or the public at large of the risk. This could be the case where, for example, a firm is in the process of shifting to an industrial IoT system in a manufacturing plant or in a transportation application.

• Third, even a casual review of trade journal articles, industry conferences and other public sources reveals that there are ongoing, often classified, efforts to solve wireless-based system disruption issues such as jamming, spoofing, and sniffing. While defense agency solutions may well be useful in some commercial settings, they may not be practicable in more consumer-oriented, but nevertheless critical applications including, for example, advanced driver assistance systems, or patient monitoring systems. In such systems, cost and time-to-market considerations may dominate and reduce the attention given to intentional or unintentional RF Layer interference issues.

• Fourth, while encryption can be very useful in solving some of the threats discussed above, e.g., using end-to-end encryption to protect privacy and security of patient data in the Bluetooth example, it does little in terms of someone collecting meta data through sniffing. Nor, even more fundamentally, is encryption useful if the desired signal is disrupted by brute force jamming at the RF Layer before the data even gets into the upper layers of the protocol stack. Additionally, some RF Layer protocols are particularly vulnerable to "smart" or "protocol aware" jamming, which can significantly increase the accuracy of jamming, and make jamming much harder to detect. Moreover, the distance at which jamming is effective may be increased even more if the smart jamming is directed at a control channel of the vulnerable system rather than at payload channels.

Summary and Conclusions

To summarize, this article draws attention to seven points and concerns:

- The future of IoT is synonymous with the use of wireless or Radio Frequency (RF) links for connections between devices and the balance of the network.
- To allow a wireless-based communications network to carry out its intended function, it must be open, therefore vulnerable.
- All types of wireless systems, from the least complex to the most complex, and from the least important to the most important, are vulnerable to jamming, spoofing, and sniffing attacks.
- Major cybersecurity efforts often focus their primary attention on attacks at higher layers of the protocol stack rather than at the RF Layer.
- While focusing attention on higher layers of the protocol stack instead of jamming, spoofing, and sniffing at the RF Layer may be an initially useful choice, a comprehensive risk assessment demonstrating that the RF Layer threats can be safely downplayed or dismissed is often missing.
- Defense agency supported efforts to solve RF Layer jamming, spoofing, and sniffing attacks may be useful in some commercial settings, but they may not be practical in more consumer oriented applications that are cost- and time-to-market driven.
- While strong encryption can be useful in preventing some forms of disruption, they have limited or no usefulness against both brute force and smart jamming attacks.

While this column has focused on the inherent openness of wireless networks and the possibly under-appreciated threats of jamming, spoofing and sniffing attacks on such networks, the intent is not to advocate that more effort and resources be prioritized for these RF Layer vulnerabilities. Instead, more subtly, the intent is to suggest that if RF Layer vulnerabilities are downplayed or ignored in the design and architecting of, say, an IoT system, that this treatment be justified by an appropriately comprehensive risk analysis to create awareness of the risks in not addressing vulnerabilities and what security is gained versus the cost tradeoffs to address any vulnerabilities.

Acknowledgments

The authors would like to acknowledge the leadership and intellectual foundation for this effort provided by our colleague, Dr. Pierre de Vries, who is an Executive Fellow at the Silicon Flatirons Center (SFC) for Law, Technology, and Entrepreneurship at the University of Colorado at Boulder and co-director of its Spectrum Policy Initiative. However, the views, thoughts, and opinions expressed herein belong solely to the authors, and not necessarily to the authors' employer, organization, committee or other group or individual.

Biographies

Dale N. Hatfield is a senior fellow at the Silicon Flatirons Center for Law, Technology and Entrepreneurship and an adjunct professor in the Technology, Cybersecurity and Policy graduate program, both at the University of Colorado Boulder. Prior to joining CU Boulder, he was the chief of the Office of Engineering and Technology at the Federal Communications Commission (FCC). He retired from the FCC and government service in December 2000. Before joining the FCC in 1997, he was the founder and CEO of Hatfield Associates Inc., a Boulder-based multidisciplinary telecommunications consulting firm. He holds a B.S. in electrical engineering from Case Institute of Technology and an M.S. in industrial management from Purdue University. In 2008, h ewas awarded an honorary doctorate by CU Boulder for his commitment to the development of interdisciplinary telecommunications studies.

Douglas C. Sicker (sicker@cmu.edu) is currently the Lord Endowed Chair in Engineering, and a professor in the College of Engineering and School of Computer Science and courtesy appointment in the Heinz College at Carnegie Mellon University. He is also the Executive Director of the Broadband Internet Technical Advisory Group (BITAG). Previously, he was the DBC Endowed Professor in the Department of Computer Science at the University of Colorado at Boulder with a joint appointment in, and director of, the Interdisciplinary Telecommunications Program. He recently served as the chief technology officer and senior advisor for Spectrum at the National Telecommunications and Information Administration (NTIA). He also served as the chief technology officer of the Federal Communications Commission (FCC), and prior to that he served as a senior advisor on the FCC National Broadband Plan. Earlier he was director of Global Architecture at Level 3 Communications, Inc. In the late 1990s, he served as Chief of the Network Technology Division at the FCC.