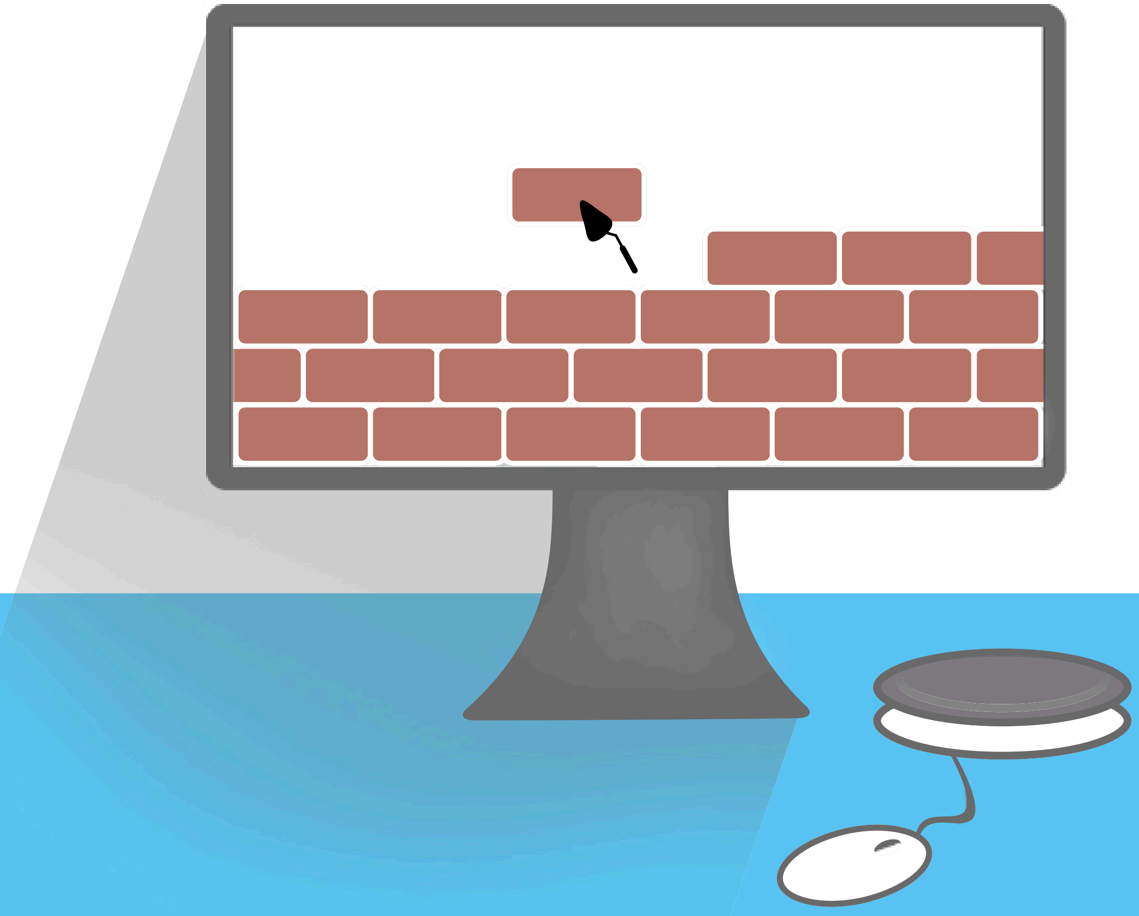
THE IMPORTANCE OF SECURITY RESEARCH

FOUR CASE STUDIES



DECEMBER 2017

CENTER FOR
DEMOCRACY
& TECHNOLOGY

The Importance of Security Research:
Four case studies

How hacking automotive vehicles, medical devices, voting machines, and internet of things devices makes them safer.

Authors: Joseph Lorenzo Hall, Apratim Vidyarthi, and Benjamin C. Dean

1. Introduction

Security researchers and security research are commonly referred to, respectively, as “hackers” and “hacking.” Such words can bring negative connotations to mind, such as hoodie-wearing miscreants in dark rooms lit only by the glow of a computer monitor. This stereotype is far from the truth. Certainly, there are malicious individuals out there attacking computer systems and networks for a variety of motives every day. However, security research and security researchers are an increasingly important component of protecting against such attacks, as well as proactively assessing flaws in the fabric of our digital infrastructures and fixing them.

In this report, we compare four areas in which computers and networks are playing an increasing role: automobiles (Section 2), medical devices (Section 3), voting machines (Section 4), and Internet of Things (IoT) devices (Section 5). We show that the efforts of security researchers have been instrumental in finding and fixing flaws in these systems, such as vulnerabilities and bugs[1] that could have resulted in serious harm, economic loss, and loss of trust in digital infrastructure.

We also describe the complicated results of disclosing flaws. A security researcher does not simply find a flaw, tell the manufacturer, and have the manufacturer fix it. Where we can, we assess if a given flaw was fixed and how long it took to fix. As covered in a past CDT report, there is a complex set of laws and private incentives that might make it difficult for a researcher to engage a manufacturer and for the manufacturer to quickly fix a reported flaw.[2]

While we try to be detailed in the examples cited in each section, this is not a comprehensive list. There are simply too many bugs and flaws that either go undetected or that might be detected and undisclosed or disclosed privately. Instead, these case studies make clear that security research is a necessary and important element of a robust, dynamic cybersecurity ecosystem – one that moves quickly to fix design and implementation flaws in systems that mediate our lives every day. While many

[1] Throughout this report, the term ‘flaws’ is used to encompass bugs and vulnerabilities.
[2] The Center for Democracy & Technology, “‘The Cyber’: Hard Questions in the World of Computer Security Research,” (March 2017), *available at:* https://cdt.org/insight/the-cyber-hard-questions-in-the-world-of-cybersecurity-research/.

of the examples we discuss were not fixed quickly, it is clear from this evidence that we must be very wary of discouraging security research.

2. Automotive Vehicles

Cars have become computers on wheels. They include complex computerized and networked electronics, engine control units (ECUs), and telematics control units (TCUs), amongst many other digital features. Increasingly, features related to sensing and automation are being added (e.g., laser-based sensors for object sensing (LIDAR) and semi-autonomous driving subsystems). Integration of these features should improve vehicle safety, efficiency, functionality, and usability.

The development of internet-connected systems in cars creates new security and privacy risks. As the complexity of the software and hardware systems in cars increases, so too does the number of possible security flaws. Cars are directly responsible for the safety of their occupants, for other people on the road, and for pedestrians. With the move to increase computerization and networking, existing software flaws are imported into the motor vehicle context. Furthermore, as cars are increasingly connected to centralized cloud providers, new risks of systemic failure may emerge in the event of cloud outages. The features used to track cars, so as to autonomously guide them through traffic, can also permit the monitoring of the vehicle's occupants – both their location and communications – if privacy-enhancing safeguards are not in place.

2.1 Examples of Automotive Security Research

The automotive vehicle sector has already experienced incidents linked to computerized and internet-connected system malfunction or hacking. Flaws can be relatively simple, which can cause informational and privacy harms, for example, flaws that expose a vehicle's location over time or a driver or passenger's entertainment preferences. More serious flaws may also result in vehicle theft, performance degradation and resultant damage to the car, serious injury to occupants or bystanders, and unnecessary costs or losses to stakeholders of markets that rely on movement of people and goods.

Over the past decade, there have been numerous reports about various forms of flaws in motor vehicles. These flaws often have security researchers involved directly in their investigation, disclosure, and mitigation. Unfortunately, for a variety of reasons, either additional security research does not take place or the findings of security research are not sufficiently acted upon.

Vulnerabilities in wireless connectivity: In 2015, security researchers found flaws in Chrysler, Dodge, and Jeep vehicles that use the UConnect system. Vulnerabilities in this system allowed a malicious actor to turn off the engine, unlock the car, and control the steering wheel, brakes, transmission, and acceleration.[3] After these flaws were discovered by independent security researchers Charlie Miller

[3] Greenberg, A. (2015, July 21). Hackers Remotely Kill a Jeep on the Highway—With Me in It. *WIRED*. Retrieved from

and Chris Valasek, and disclosed in a chilling video, Chrysler recalled more than 1.4 million vehicles.[4] Chrysler cars, unlike other brands, could not be updated wirelessly, so owners had to bring these vehicles in for service. The end result was that not all systems were updated.[5] [6] It is notable that similar flaws were found by academic security researchers years earlier, using investigations conducted in more controlled experimental conditions – on closed tracks or in laboratories – and were not acted upon.[7]

General Motors (GM) cars have used a similar wireless connectivity system called OnStar. Security researcher Samay Kamkar developed OwnStar, which compromised the OnStar system, thereby identifying the potential for malicious actors to unlock the car, track its whereabouts, and start the vehicle remotely.[8] This flaw affected more than two million cars, and it took GM five years to patch the system.

Vulnerabilities in Keyfobs and Locking Systems: Audi, BMW, Toyota, and Ford cars had serious flaws in their key fob systems. These systems could be compromised with little effort, allowing for cars to be remotely started and, therefore, stolen.[9] Swiss and German researchers discovered these issues; however, over three years later, no existing fix for these issues has been provided.

Researchers at the University of California, Santa Clara (UCSC) found that Toyota Priuses and Chevrolet Corvettes could be unlocked, started, and vital statistics like fuel levels could be modified through software and hardware manipulation.[10] There are approximately 3.8 million 2010 Priuses on the road,[11]

https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[4] Cobb, S. (2015, July 29). Cybersecurity and manufacturers: what the costly Chrysler Jeep hack reveals. *WeLiveSecurity*. Retrieved from https://www.welivesecurity.com/2015/07/29/cybersecurity-manufacturing-chrysler-jeep-hack/

[5] Luckerson, V. (2015, August 6). How the Jeep Hack Reveals Tesla's Biggest Advantage. *Time*. Retrieved from http://time.com/3987360/tesla-hack/

[6] Despite the ability for such cars to be updated over the air, this is no panacea: a perpetual connection to the internet also introduces the risks of malware, hacking, and other risks that arise with the internet, especially if car companies are careless with their software implementation.

[7] Koscher, K., Czeskis, A., Roesner, F., Patel, S., Kohno, T., Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S. (2010). Experimental Security Analysis of a Modern Automobile. In *2010 IEEE Symposium on Security and Privacy* (pp. 447–462). https://doi.org/10.1109/SP.2010.34; Checkoway, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czekis, A., Roesner, F., Kohno, T. (2011). Comprehensive Experimental Analyses of Automotive Attack Surfaces. In *Proceedings of the 20th USENIX Conference on Security* (pp. 6–6). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=2028067.2028073; Rouf, I., Miller, R., Mustafa, H., Taylor, T., Oh, S., Xu, W., Gruteser, M., Trappe, W., Seskar, I. (2010). Security and Privacy Vulnerabilities of In-car Wireless Networks: A Tire Pressure Monitoring System Case Study. In *Proceedings of the 19th USENIX Conference on Security* (pp. 21–21). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1929820.1929848.

[8] Greenberg, A. (2015, September 10). GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars. *WIRED*. Retrieved from https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/

[9] Greenemeier, L. (2015, July 28). Recall Shows That a Hack Attack on Car Controls Is a Credible Threat. *Scientific American*. Retrieved from https://www.scientificamerican.com/article/recall-shows-that-a-hack-attack-on-car-controls-is-a-credible-threat/

[10] Wagner, D. (2015, October 29). Car Hacking Research Accelerates At UC San Diego. *KPBS Public Media*. Retrieved from http://www.kpbs.org/news/2015/oct/29/car-hacking-research-accelerates-uc-san-diego/

[11] Worldwide Sales of Toyota Hybrids Top 6 Million Units. (2014, January 14). *Toyota USA Newsroom.* Retrieved December 14, 2017, from

along with approximately 14,000 2013 Corvettes.[12]

Independent security researcher Ken Munro discovered that the Mitsubishi Outlander's TCU had a vulnerability that allowed the car to be unlocked.[13] No patch has yet been issued to rectify the situation as Mitsubishi claims that this vulnerability is not a direct threat to consumer security. Approximately 50,000 Outlanders were on the road in 2013.[14]

Vulnerabilities in Mobile Apps Connected to Vehicles: Independent researcher Troy Hunt discovered that the Nissan Leaf could be remotely started and the owner's personal information could be accessed through the car's mobile app.[15] The company immediately responded by shutting down the application, thus removing the path for the vulnerability.

3. Medical Devices

Some types of medical devices are increasingly connected to the internet. Functions could be as complicated as remote operation machines, which allow doctors to perform surgical procedures on their patients from afar, or as simple as blood refrigeration units, which are responsible for maintaining the environmental conditions for blood storage. Additionally, hospital networks are increasingly connected to the internet, which creates risks of system outages or data loss due to accidental or malicious acts.

To highlight the degree of vulnerability here, note that hospital networks – like most networks – are vulnerable to malware, such as ransomware and viruses.[16] A number of past incidents demonstrate the potential consequences of this vulnerability. The Hollywood Presbyterian Medical Center suffered a ransomware incident in 2016.[17] In 2011, the Gwinnett Medical Center in Lawrenceville, Georgia was unable to admit non-emergency patients for three days after a virus crippled its computer system, underlining that these kinds of infestations are not merely annoyances but events that can cause critical patient care outages. Similar cases of ransomware have also been reported around the world, particularly in relation to the WannaCry ransomware outbreak in mid-2017.[18] [19]

http://corporatenews.pressroom.toyota.com/releases/worldwide+toyota+hybrid+sales+top+6+million.htm

[12] The End of the 2013 Corvette - What Did They Build Most? (2013, March 12). *Corvette Blogger*. Retrieved December 14, 2017, from http://www.corvetteblogger.com/2013/03/12/the-end-of-the-2013-corvette-what-did-they-build-most/

[13] Lee, D. (2016, June 6). Mitsubishi car alarm system "hacked." *BBC News*. Retrieved from http://www.bbc.com/news/technology-36444586.

[14] Export Shipments by Region. (2013). *Mitsubishi Motor Corporation.* http://www.mitsubishi-motors.com/content/dam/com/ir_en/pdf/fact/2013/fact_2013_07.pdf

[15] Kelion, L. (2016, February 24). Nissan Leaf electric car hack revealed. *BBC News*. Retrieved from http://www.bbc.com/news/technology-35642749.

[16] Ransomware is a type of malware which encrypts data on a device or in a database and only decrypts the data if a ransom is paid.

[17] Cuthbertson, A. (2016, February 18). Hacked hospital ransom payout 'incentivises criminals.' *Newsweek*. Retrieved from http://www.newsweek.com/hacked-hospital-ransom-payout-incentivises-criminals-428133.

[18] Reel, M., & Robertson, J. (2015, November). Hospital Gear Could Save Your Life or Hack Your Identity. *Bloomberg*. Retrieved from

3.1 Examples of Medical Device Security Research

As the variety and number of internet-connected medical devices increases, so too does the risk of malfunction due to unintended actions or malicious actors exploiting the vulnerabilities in these devices. Particularly in a medical context, these incidents could result in illness or death. Such incidents are already occurring, and security researchers – in some cases because they have a direct relationship to a given class of medical devices given their own health concerns – are increasingly responsible for finding, disclosing, and pioneering workarounds that can potentially render such flaws harmless.

Implantable Medical Devices: Insulin pumps transmit dosing information to the device. An incorrect dosage could give rise to a serious medical incident, including the possibility of death. Dosage could potentially be disrupted either due to malicious actions or due to inadvertent software malfunction. Jay Radcliffe, providing a briefing at Black Hat in 2011, determined that many insulin pumps have minimal user-adjustable controls. Due to manufacturers wishing to prevent tampering, these pumps can be (re)programmed to cause an overdose of insulin, resulting in potentially serious adverse health outcomes.[20] In similar analyses by Radcliffe years later, on newer insulin pumps, he found additional flaws, requiring users to either discontinue the use of the provided wireless remote control and/or apply a manufacturer update that limits the maximum dose of insulin applied.[21]

Implanted defibrillators and pacemakers deliver regular stimulation to the heart in order to maintain regular heart-beating. Unfortunately, these devices may possess vulnerabilities that make them susceptible to malicious software attacks, ransomware, or accidental malfunction. For instance, Barnaby Jack, a renowned security researcher, demonstrated how a pacemaker may be hacked so as to deliver a fatal shock to a patient.[22] The flaw was discovered in April 2015, although no current patch for it has as of yet been released.

Durable Medical Equipment: Drug infusion pumps are bedside devices that administer a precise dosage of a drug to a patient. Security researcher Billy Rios determined that multiple drug infusion pumps are susceptible to a flaw that can lead them to deliver the wrong dosage. The flaw exists because of the way in which they update their firmware, allowing the maximum dosage for patients to be raised to potentially fatal levels.[23] Hospira, the main company which faces this problem, was warned by the researcher but did not take any specific action. The FDA has released alerts about the firmware

http://www.bloomberg.com/features/2015-hospital-hack/

[19] Anthony, S. (2017, May 12). Massive ransomware attack hits UK hospitals, Spanish banks. *Ars Technica*. Retrieved from https://arstechnica.com/information-technology/2017/05/nhs-ransomware-cyber-attack/

[20] Basu, E. (2013, August 3). Hacking Insulin Pumps And Other Medical Devices From Black Hat. *Forbes*. Retrieved from https://www.forbes.com/sites/ericbasu/2013/08/03/hacking-insulin-pumps-and-other-medical-devices-reality-not-fiction/

[21] Beardsley, T. (2016, October 4). R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump. Retrieved December 14, 2017, from https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/

[22] *Id.*, at fn 18.

[23] Zetter, K. (2015, June 8). Hacker Can Send Fatal Dose to Hospital Drug Pumps. *WIRED*. Retrieved from https://www.wired.com/2015/06/hackers-can-send-fatal-doses-hospital-drug-pumps/.

issue.[24]

An independent security research firm, TrapX Security, found that x-ray equipment and picture archive communication systems are potentially accessible by outside actors.[25] Other medical imaging systems requiring complex electronics (e.g., PET scanners, CT scanners, and MRI machines) have similar flaws. Such systems could be infected with malware and thereby hijacked to gain access to sensitive health data or even so that the device can join a botnet.[26] The storage systems required minimal to no authorization, and did not log access, which makes it difficult to track breaches in the event that they have happened.[27] There are potentially serious privacy and fraud-related risks given the high value of medical data.

TrapX Security also found that blood refrigeration units often have hard-coded passwords embedded by vendors, which are easy to manipulate. This might allow malicious actors to change the temperature remotely,[28] which in turn could result in spoilage of blood units.

4. Voting Systems

The United States has increasingly sought to computerize – and in some cases, network – specific features of our voting systems. The rationale is to make them more usable; accommodate people with disabilities, as well as people with non-English language voting preferences; and tabulate unofficial results much faster than it would take to hand-count complicated ballots. However, the use of computers and computer networks in voting system infrastructure also comes with vulnerabilities in those systems.

While election-related computer and network vulnerabilities have been studied for decades, they have come into particularly stark relief following the 2016 General Election in the United States. At their most basic, flaws in election systems can cause disruption in election processes, leading to long lines or mistakes in ballot contents presented to voters. At their worst, flaws can allow remote attackers a pathway to changing the election outcome from anywhere in the world. Academic researchers have, in some cases, been able to investigate the security of election systems in the past. By contrast, only recently have election systems been the focus of independent security researchers. Election systems

[24] Vulnerabilities of Hospira LifeCare PCA3 and PCA5 Infusion Pump Systems. (2013, May 13). *FDA Safety Communication* Retreived from http://web.archive.org/web/20151121202227/http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm446809.htm

[25] Storm, D. (2015, June 8). MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. *Computerworld*. Retrieved from https://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html

[26] A network of maliciously-controlled computers often used to flood other computers on the internet with more traffic than they can handle.

[27] Zetter, K. (2014, April 25). It's Insanely Easy to Hack Hospital Equipment. *WIRED*. Retrieved from https://www.wired.com/2014/04/hospital-equipment-vulnerable/.

[28] Zetter, K. (2015, November 24). Medical Devices That Are Vulnerable to Life-Threatening Hacks. *WIRED*. Retrieved from https://www.wired.com/2015/11/medical-devices-that-are-vulnerable-to-life-threatening-hacks/.

and voting machines have authentication systems and cryptographic protections. In the past, these protections impeded independent security researchers who wished to investigate these machines. This was because of the potential for application of Digital Millenium Copyright Act (DMCA) anti-circumvention liability to these researchers. The recent DMCA triennial exemption from anti-circumvention liability for voting systems went into effect, thereby permitting more independent security researchers to investigate and thereby contribute to the improved security of these systems.[29]

4.1 Examples of Voting System Research

Flaws in voting systems are unfortunately common. In 2004, academic security researchers obtained[30] a popular voting system, the Diebold AccuVote-TS. This machine had a touchscreen interface that voters would use to make selections. The machine would then record the voter's ballot onto internal memory. This system was found to have serious flaws, notably the unchangeable ("hard-coded") universal password "123456" that allowed complete control over the presentation and recording of the voted ballot. This work was extended a few years later by Princeton researchers who created a virus that could be installed on this system during a primary election by a single individual subverting a single machine. This virus could then spread to all other machines between the primary and general election.[31]

In 2007, the states of California and Ohio were concerned about the security of their voting systems. They commissioned two separate investigations by academic researchers: the California Top-to-Bottom Review[32] and the Ohio EVEREST review.[33] These were the first "white box" evaluations of voting systems, which allowed academic security researchers, under strict confidentiality terms imposed by the voting system manufacturers, access to source code, documentation, and a number of each model of voting system. Access to such information permitted investigation of potential flaws and vulnerabilities.

Since these landmark studies, researchers have focused only episodically on examining voting systems for flaws. Notable cases include the investigation performed on the Sequoia AVC Advantage, which used a powerful hacking technique called return-oriented programming to demonstrate that even

[29] Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies; Library of Congress, Copyright Office. (2017, October 28). 80 Fed. Reg. 65944 at 65956. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2015-10-28/pdf/2015-27212.pdf.

[30] Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system. In *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004* (pp. 27–40). https://doi.org/10.1109/SECPRI.2004.1301313

[31] Feldman, A. J., Halderman, J. A., & Felten, E. W. (2007). Security Analysis of the Diebold AccuVote-TS Voting Machine. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology* (pp. 2–2). Berkeley, CA, USA: USENIX Association. Retrieved from http://dl.acm.org/citation.cfm?id=1323111.1323113.

[32] California Secretary of State. (2007). *Top-To-Bottom Review*. California Secretary of State. Retrieved from http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/.

[33] McDaniel, P., Blaze, M., Vigna, G., Butler, K., Enck, W., Hursti, H., Hall, JL, et al.. (2007). *EVEREST: Evaluation and Validation of Election-Related Equipment, Standards and Testing (Academic Final Report)*. Ohio Secretary of State. Retrieved from http://www.josephhall.org/papers/Academic_EVEREST_Report.pdf.

some of the more potentially secure voting system architectures could be cleverly subverted.[34] Initially, these studies faced some resistance in academic venues due to questions about whether any additional analysis of a voting system above and beyond previous academic treatments would contribute to fundamental knowledge (the merit criteria for academic work). Accordingly, subsequent academic investigations of voting technology focused on newer systems, such as the University of Michigan researchers who (under invitation) mounted an attack against the pilot Washington, D.C. Internet Voting System. This attack allowed them to change the votes on all ballots cast through that system.[35] Non-academic independent security researchers both could not obtain voting systems easily and faced a riskier calculus in terms of potential legal liabilities.

This emphasizes that there has been a lack of academic and independent attention to voting systems in recent years. It is difficult to fund and publish academic work without serious contributions to fundamental knowledge. However, with the interest generated by the 2016 U.S. election cycle and the DMCA anti-circumvention exemption, which was issued in 2015, there is increasing attention by independent security researchers given to voting machines and election systems. Two notable examples are the examination of Georgia's Kennesaw State infrastructure by security researchers Logan Lamb and Chris Grayson[36] and the 2017 DEFCON Voting Machine Hacking Village.[37] In the Georgia case, Lamb wrote a simple computer program that downloaded content from the Kennesaw State University's Center for Election Systems (CES) website. This serves as both the public face and administrative portal for all of Georgia's counties in the maintenance and support of Georgia's uniform voting system. Lamb, and then months later, Grayson, found serious flaws in the website. These flaws allowed access to voter registration records for all Georgia voters and software for the voting machines, ostensibly for counties to download to update the software on Georgia's thousands of very old (15-20 years) voting machines. After a review of CES' procedures and the material discovered by these researchers, the Georgia Secretary of State decided that CES could no longer competently provide services and support for Georgia's voting systems.

DEFCON is the world's biggest hacking conference, held in Las Vegas every August. The conference provides many "villages," which give security researchers hands-on experiences with security-relevant devices and practices (e.g., lock-picking, biomedical devices, and automotive devices). In 2017, for the first time, voting machines were also available. The "Voting Village" showed that within about 24

[34] Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, & Hovav Shacham. (2009). Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. *USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop/Workshop on Trustworthy Elections 2009 (EVT/WOTE' 09)*. Retrieved from http://www.usenix.org/events/evtwote09/tech/full_papers/checkoway.pdf.

[35] Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. A. (2012). Attacking the Washington, D.C. Internet Voting System. In *Financial Cryptography and Data Security* (pp. 114–128). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-32946-3_10.

[36] Zetter, K. (2017, July 14). Will the Georgia Special Election Get Hacked? *POLITICO Magazine*. Retrieved from http://politi.co/2heBRW2.

[37] Blaze, M., Braun, J., Hursti, H., Hall, J. L., MacAlpine, M., & Moss, J. (2017). *DEFCON 25 Voting Machine Hacking Village: Report on Cyber Vulnerabilities in U.S. Election Equipment, Databases, and Infrastructure*. DEFCON. Retrieved from https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

hours, every piece of voting equipment that the organizers were able to procure could be subverted by ordinary security researchers with no privileged information.[38] Notable findings included the complete remote control of the AVS WinVote system, which had been used heavily in Virginia from 2004 until it was decertified in 2015. Remote control of this system allowed an attacker to completely manipulate – in a totally automated fashion – both ballot display and electronic recording of votes. In addition, 650,000 voter records were discovered on voter registration terminals purchased as surplus from a county in Tennessee. This called into question not just the integrity of the devices, but of the procedures used to implement, support, and decommission voting systems.

5. Consumer Internet of Things Devices

The consumer Internet of Things (IoT) sphere, consisting of home and handheld networking devices, constitutes a significant proportion of new internet connected devices. These IoT devices have many flaws that result in malfunction and/or enable malicious actors to easily take advantage of them. This situation is especially concerning because many IoT devices are based on minimal platforms like Arduino and Raspberry Pi, which either are not capable of encryption, which is an important security measure, particularly for personal information, or do not do so by default.[39] [40] Nonetheless, the number of IoT devices continues to grow, with internet connectivity being implemented in everything from lightbulbs to refrigerators. The rate of growth is rapid; in 2012, there were 8.7 billion internet-connected devices; this is projected to grow to 50.1 billion in 2020 – reflecting the magnitude of the security risk that is dawning upon the industry.[41]

5.1 Examples of IoT Device Research

The potentially intimate nature of data to be collected from some of these devices, as well as the risk of personal injury or property damage from the malfunction of these devices, increase the utility of security researchers in this area. A few key use cases can be used to exemplify the risks that IoT devices bring, and the value that security researchers play within the industry.

Light bulbs: Context Security, a security research firm, discovered a flaw in LifeX bulbs.[42] The vulnerabilities posed by these smart bulbs can reveal passwords, usernames, and private information being transported through a wireless network. Researchers also found ways to exploit vulnerabilities in Philips smart light bulbs, which would allow for a chain reaction disabling of all light bulbs of the same

[38] As had been the case with the 2007 academic security evaluations discussed above.

[39] AES Algorithm processing time in Arduino vs Raspberry Pi. Retrieved December 14, 2017, from https://crypto.stackexchange.com/questions/12891/aes-algorithm-processing-time-in-arduino-vs-raspberry-pi.

[40] For example, see: Kumar, U., Borgohain, T., & Sanyal, S. (2015). Comparative Analysis of Cryptography Library in IoT. *ArXiv:1504.04306 [Cs]*. Retrieved from http://arxiv.org/abs/1504.04306.

[41] IoT: number of connected devices worldwide 2012-2025. (2017). *Statista*. Retrieved from https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[42] Wakefield, J. (2014, July 8). Experts hack smart LED light bulbs. *BBC News*. Retrieved from http://www.bbc.com/news/technology-28208905.

type within close proximity.[43]

Smart refrigerators: Pen Test Partners, a security research firm, discovered a vulnerability in a Samsung smart fridge that would allow Gmail – and other websites – login credentials to be accessed because the "device does not validate SSL certificates."[44] Thus, the fridge is vulnerable to man-in-the-middle attacks and also leaks passwords on the wireless network the fridge is connected to. Due to their vulnerabilities, smart fridges have also been found sending out spam when their software was maliciously modified to be part of a botnet.[45]

Smart thermostats: TrapX and Professor Yier Jin from the University of Central Florida found that if malicious actors have physical access to Nest thermostats, they can upload custom software onto the devices and take advantage of the unencrypted (potentially private) data stored on those thermostats.[46] This hack required physical access to the device. The manufacturer claimed that such a "jailbreak doesn't compromise the security of our servers or the connections between our devices and our servers."

Baby monitors: Rapid7,[47] a security research firm, found many poor security practices in baby monitors such as "default passwords and a lack of encryption."[48] Some manufacturers, like Philips, have released advisories to their customers due to similar issues. The New York City Department of Consumer Affairs has released an investigation and an alert due to these issues.[49]

Smart alarm systems and locks: Researchers at the University of Michigan successfully created malware targeting home security/alarm systems. Their custom software granted the researchers access to the PIN; allowed them to remotely control the blinds, lights, and other connected home functionalities; and even turn on the fire alarm.[50] Many security systems face such problems, including ADT and Vivint. These devices are vulnerable due to their susceptibility to jamming, and due to their transmission of unencrypted signals on wireless networks.[51] In another case, a maker of high-security

[43] Ronen, E., Shamir, A., Weingarten, A. O., & O'Flynn, C. (2017). IoT Goes Nuclear: Creating a ZigBee Chain Reaction. In *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 195–212). https://doi.org/10.1109/SP.2017.14.

[44] Leyden, J. (2015, August 24). Samsung smart fridge leaves Gmail logins open to attack. *The Register*. Retrieved from https://www.theregister.co.uk/2015/08/24/smart_fridge_security_fubar/.

[45] Fridge sends spam emails. (2014, January 17). *BBC News*. Retrieved from http://www.bbc.com/news/technology-25780908

[46] Tilley, A. (2015, March 6). How Hackers Could Use A Nest Thermostat As An Entry Point Into Your Home. *Forbes*. Retrieved from https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/

[47] Stanislav, M., & Beardsley, T. (2015). *Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities*. Rapid7. Retrieved from https://www.rapid7.com/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf

[48] Cuthbertson, A. (2016, January 29). Are hackers spying on your baby? *Newsweek*. Retrieved from http://www.newsweek.com/search-engine-sleeping-babies-420967

[49] Consumer Alert: Consumer Affairs Warns Parents to Secure Video Baby Monitors. (2016, January). Retrieved December 14, 2017, from http://www1.nyc.gov/site/dca/media/pr012716.page

[50] Fernandes, E., Jung, J., & Prakash, A. (2016). Security Analysis of Emerging Smart Home Applications. In *2016 IEEE Symposium on Security and Privacy (SP)* (pp. 636–654). https://doi.org/10.1109/SP.2016.44

[51] Zetter, K. (2014, July 23). How Thieves Can Hack and Disable Your Home Alarm System. *WIRED*. Retrieved from https://www.wired.com/2014/07/hacking-home-alarms/

electromagnetic locks threatened researchers at independent security firm, IOActive, after they had detailed serious security shortcomings in those locks, allowing an attacker to modify the “authorizations” stored on the electronic key to allow arbitrary access to other locks.[52]

Fitness monitors: Security researchers at Fortinet discovered an easy way to inject malware into Fitbit’s devices in less than ten seconds.[53] However, Fitbit was reluctant to define such a vulnerability as one that would allow malware to spread, and denied the initial vulnerability.

6. Conclusion

This paper has provided a rich set of examples where security researchers have played a critical role in the identification and reporting of flaws and vulnerabilities in automotive vehicles, medical devices and hospital networks, voting and election systems, and a multitude of consumer IoT devices. In many cases, the implications of these shortcomings are serious, including potential physical harm and death, theft or loss of device control, disruption or outcome changes in government election processes, and eavesdropping on and/or tracking users.

There is a growing need for greater scrutiny of the security of these technologies as they continue to proliferate throughout society. Unfortunately, more security researchers are unable to play a greater role in this area – or, at least, are less likely to concentrate in this area – due to chilling effects. This is because of the uncertainty and potential illegality of their well-intentioned research, under the DMCA – for circumvention of access controls – and the Computer Fraud and Abuse Act (CFAA) – for accessing systems over networks, which were put in place to prohibit maliciously-intended activities, not the sleuthing of well-intentioned researchers and tinkerers.[54] Security researchers also face a general atmosphere of suspicion and ill-will from the companies that produce and sell these defective products, leading to serious legal threats and, in some cases, lawsuits.

As the use of these products in our societies increases, and the risks from their defects also increase, changes to these laws would permit security researchers to play a greater role in managing these risks. With a clearer picture of what legal risks security researchers face, we would potentially learn much more about pervasive insecurity of the digital fabric of society, and hone efforts focused on fixing vulnerabilities, as well as entire classes of vulnerabilities, for good.

[52] Zetter, K. (2015, May 6). With Lock Research, Another Battle Brews in the War Over Security Holes. *WIRED*. Retrieved from https://www.wired.com/2015/05/lock-research-another-battle-brews-war-security-holes/

[53] Dent, S. (2015, October 21). Fitbit trackers can be hacked in “10 seconds” (update: Fitbit disagrees). *Engadget*. Retrieved from https://www.engadget.com/2015/10/21/fitbit-tracker-bluetooth-vulnerability/

[54] *Id.*, CDT, note 1.