CONSTRUCTING A KNOCK ACTIVATED LOCKBOX – THE "TAP BOX"

THE CYBER AND PHYSICAL SECURITY CONCERNS OF THE "TAP BOX"

A Thesis Prospectus
In STS 4500
Presented to
The Faculty of the
University of Virginia

In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Electrical Engineering

Yusuf Cetin

October 31, 2022

Technical Project Team Members
Zachary Hogan
Fayzan Rauf
Will Sivolella

Advisors
Catherine D. Baritaud, Department of Engineering and Society
Harry C. Powell Jr., Department of Electrical and Computer Engineering

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

For centuries, material goods have been valued by humans so much that owners often go to great lengths to ensure their possessions are not stolen. Money, gold, and written secrets are just some of the tangible objects that can have detrimental effects if found in the wrong hands. Combating theft is a constant battle which requires clever and strong systems to keep attackers out. One method is by using electronics, and as technology accessibility increases and Internet of Things (IoT) devices multiply, using electronically powered systems for security is becoming more prevalent in commercial products. According to IoT Analytics, the number of connected IoT devices has reached 14.4 billion globally (Hasan, 2021). While these devices ensure security and make lives easier, they still exhibit flaws. Even being connected to the internet is a risk, as cyber attackers are increasingly more capable of infiltrating devices on any home network. Nest cameras, for example, have repeatedly been a target of hackers, and other smart home devices alike are susceptible due to lack of basic security protocols within firmware (Whittaker, 2020). Therefore, ensuring the impermeability of a device like a lockbox is paramount when designing such a product. One solution is to disguise the box as to not draw attention to it as a holder of valuables in the first place, effectively hiding in plain sight. This can be done by enclosing the system in a common household object, such as a book. Furthermore, the device can implement a unique method of access, differing from a traditional keypad method for entry, by using a knocking sequence only known by the owner. Through these features, a lockbox device can be constructed.

The technical and STS research topics that will be explored in this paper include the electrical and physical design and construction of the actual box and the large-scale societal effects of implementing this project as an IoT device in the real world. The transformation of the genesis of the idea into high-level electronic design and eventually to a final product will be

described in great detail in the technical section, as well as the methods that were established and heavily revised during this process. The STS research section of this paper will focus more on the security impacts that such a technology could have, mostly through the lens of cybersecurity. These topics are loosely coupled, as the basic functioning product was determined first before technical work began. Upon deliberation of an interesting, meaningful product, cybersecurity issues were viewed as secondary since Wi-Fi connectivity of the device was an intentionally rudimentary feature to be added. Therefore, considering a possible cyber-attack on the device was not included in the technical scope of the project, deeming the technical and STS topics distantly related.

The project was carried out by myself, Yusuf Cetin, my group members Zachary Hogan, Will Sivolella, and Fayzan Rauf, and with the guidance of Professor Harry Powell in the Department of Electrical and Computer Engineering and graduate TA Ashish Gawali. To tackle specific components of the project, individual responsibilities were delegated to each group member, and allowed for parallelization of pertinent tasks to take place. Each group member was proficient in different fields necessary to the project, being the reason that they were assigned their specific role. I am working on the printed circuit board layout and electronic design components, Will is constructing the physical box and helping with electronic design, Zac is spearheading the software development, and Fayzan is helping Zac as well as aiding in physical component selection. The Gantt chart on page 3 in Figure 1 represents the most up to date timeline given our time constraints. Given the hard deadline of December 12th, this visual helped our group to stay on track.

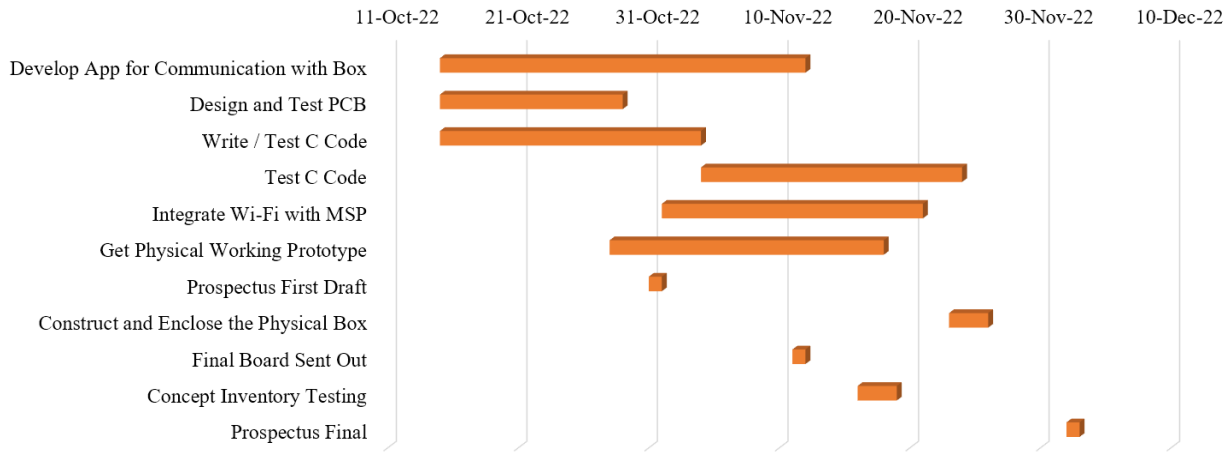

Figure 1: Gantt chart of project. Technical tasks to be completed starting from early October when actual work on the project had been started. Parallelization is shown with overlaps (Cetin, 2022).

CONSTRUCTING A KNOCK ACTIVATED LOCKBOX – THE "TAP BOX"

The technical purpose of this project is to provide a robust, unique, and more secure solution for material valuables storage. As mentioned in the introduction, constructing a lockbox with an inconspicuous enclosure, and knocking pattern mechanism as a method of access will be how this is achieved. Enclosing the entire system into a seamless 3D printed tissue box will ensure minimal hacker detection of there even being a device to breach. The main component of the box, however, will be the knock mechanism as a method for access inside.

The working principle of the mechanism is that a user knocks in a specific sequence on the box, upon which, if correct, will result in the box unlocking, allowing access to its contents, which will be a small space given the physical space restriction. This project, although a seemingly novel idea, has been created by various hobbyists on the internet, proving that it is workable. One of which, implemented as a drawer lock, used various components such as a microcontroller, solenoid lock, a piezoelectric sensor, and a power supply. The piezoelectric sensor took knock sounds as an input, which is processed by the microcontroller, an Arduino, and if correct, results in the unlocking of the solenoid lock (Hoefer, n.d.). The design utilized

one piezoelectric sensor, which differs from our project, which uses two. This is to ensure an extra layer of security that will prevent potentially listening intruders from inputting a stolen knock sequence. To design and create a box version of the mentioned project, much of the same parts will be used, except physically condensed due to the space constraint of the given household object, a tissue box, as shown and labelled in Figure 2.

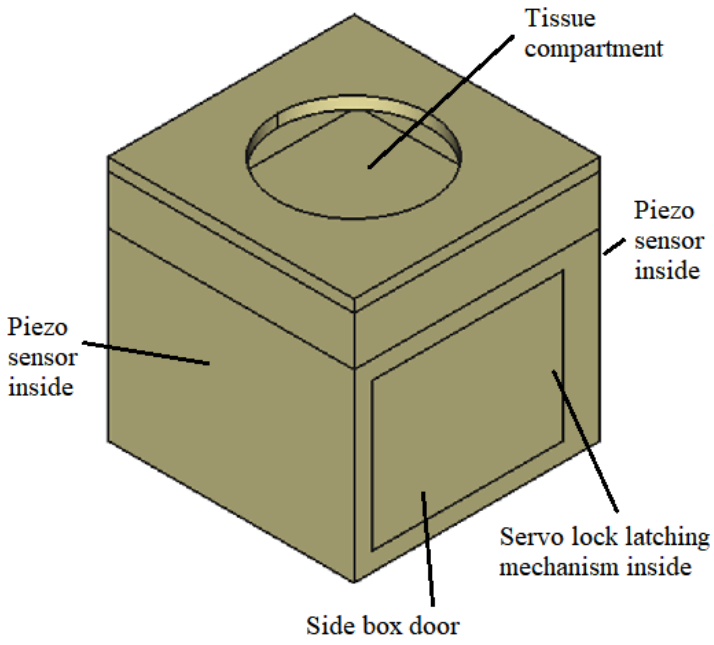

Figure 2: 3D model of the "Tap Box". A tissue box as the enclosure of choice is shown. Because the box will need to be as discreet as possible, a mock tissue compartment will be built in. The door will only unlock upon the correct sequence of knocks, sensed by the piezoelectric sensors of each side of the box. This is made possible by the controlled servo motor behind the door through a latching mechanism (Cetin, 2022).

The MSP432, a microcontroller, will serve as the brains of the system, responsible for the processing of input voltage data and control of the output lock. In addition to this base mechanism, a Wi-Fi module will be connected to the MSP432, providing secondary mobile access to the owner if the knock pattern is forgotten or faulty. Maintaining power to the system will be provided with the use of a rechargeable battery, in conjunction with a printed circuit board (PCB) that allows for power regulation to all components of the project. Extensive embedded coding of the MSP432 will be required to provide the most robust product possible.

Although straightforward at first glance, this project requires tackling a multitude of different problems, with new issues arising as the process continues. Being a portable, battery-powered system, the nagging dilemma of energy conservation of all components must be weighed and optimized accordingly. Therefore, a power budget was made with the following components as primary sources of power drain: MSP432 microcontroller, CC3120 Wi-Fi module, operational amplifiers, and the servo motor. These components are located at the output of the linear voltage regulator, which takes our battery's 9.6V and converts it to a usable standard of 3.3V. To combat wasted power draw during the idle state of the device, the MSP432 and CC3120 Wi-Fi module were set to low power mode in software and were programmed to "wake up" when a knock is detected (Jolly, 2021). The operational amplifiers, used in filtering and amplifying of the piezoelectric signals were chosen to be the lowest current drawing models, which significantly reduces their power consumption. Finally, the servo motor was driven with an N-channel MOSFET acting as a switch, meaning current to the servo could be supplied with the MSP432 as necessary, and the servo would be off otherwise. All these methods of power constricting allow the project to drain the battery at a slower rate, thereby prolonging time between recharges and reducing wasted energy.

Another technical issue that is apparent is the physical restriction of both the PCB and the tissue box enclosure. The PCB will be directly mounted onto the microcontroller and therefore must not have an area larger than the MSP432. This means that components must be surface mount components rather than through-hole, saving a considerable amount of physical space. All of the subsystems of the project, which includes the circuit boards, servo motor, and piezoelectric sensors, must also fit into the enclosure that is built, and will allow for a space to

store valuables. The encapsulation and interconnects between all of these systems is neatly represented in the high-level block diagram in Figure 3.

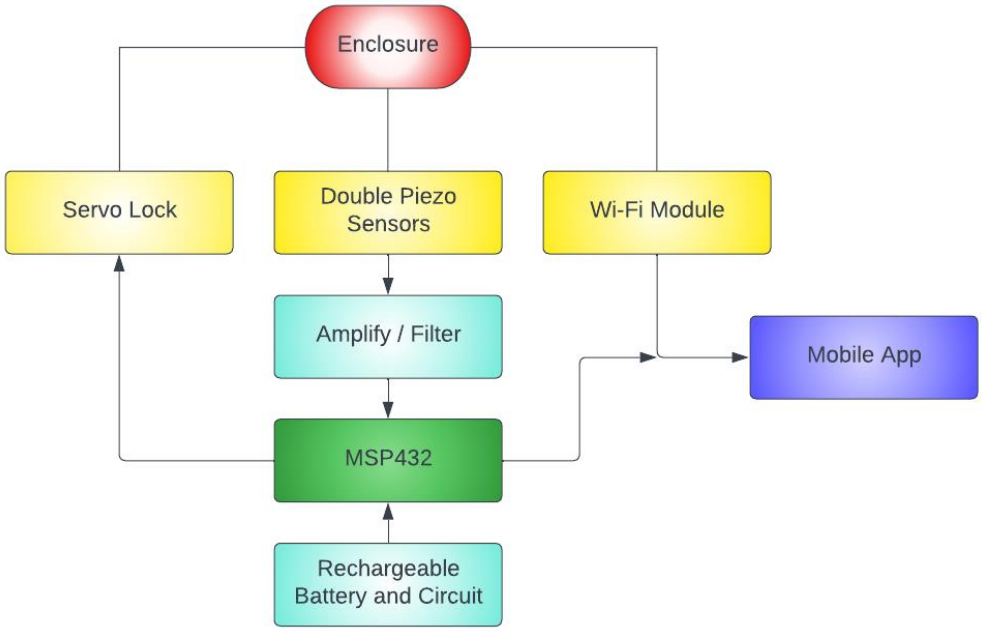

Figure 3: Overall functional block diagram of the "Tap Box". The blue boxes represent systems that will be designed and built, green indicates the microcontroller, yellow shows the electronic peripherals, red indicates the enclosure, and purple shows a software product. The arrows demonstrate roughly current flow and the controlling mechanism at the tail with what it is controlling at the head (Cetin, 2022).

THE CYBER AND PHYSICAL SECURITY CONCERNS OF THE "TAP BOX"

Security is a facet of life that should not be compromised, but of course attackers alter this desired reality. Cyber criminals have gained significant strength in recent years, especially with the advent of widespread IoT devices. Since the knock activated lockbox will be Wi-Fi enabled, the issue of a cyber-attack is especially relevant. As more and more IoT products become commercially available, the concerns that govern their use also apply to this project, if the lockbox were to be widely distributed (Usmonov et al., 2017).

With the unprecedented ravage of the pandemic in early 2020, people were in their homes more, meaning a flourishing of IoT device usage. This influx, however, created the perfect situation for cyber criminals to attack. With more potential entry points into unsuspecting residential internet connections, hackers were able to maximize their intrusion significantly. In fact, according to Forno, Mateczun, and Norris there was a 300% increase in cybercrimes between 2020 and 2021. While IoT is among the major reasons hackers can intrude, ease of monetary gain and low risk of punishment also contribute to malicious intents, catalyzed by the opportunities opened by the pandemic (2022). In turn, governments should be urged to follow the standard best practices and emphasize the demand for cybersecurity jobs. The solutions that arise from continued work on eliminating cybercrimes is vital for the development of effective implementation in the real world of IoT devices. Researching and testing counteractive measures, with deployment of such advancements like honeynets can provide great insight and progress towards making devices as safe as possible. In the technical work carried out by Bernabe, Calero, Skarmeta, and Zarca, honeynets are defined as simulated networks that attract hackers on purpose to study their methods. High-interaction honeypot (HIH) honeynets are even more cloaked to cybercriminals, meaning deeper information can be collected about a hacker with its implementation. However, being a large resource-consuming tool, and having little history with implementation in IoT devices, this technology needs what the researchers were able to devise, an automated framework to deploy a flexible honeynet (2020). Ongoing work such as this is an important step in the direction of securing IoT devices in the broader network.

Although subjectively shocking, none of the United States, except for California, has comprehensive laws governing consumer data privacy with IoT devices. Concerning cybersecurity, the IoT Cybersecurity Improvement Act of 2020 is the only bill that gives some

level of management in the realm of IoT security, although minimal. In California, the California IoT cybersecurity law, SB-327, became effective January 1st, 2020, which requires manufacturers of devices to build in adequate security features, for example, a password setup prior to first use (IoT cybersecurity: Regulating the internet of things, n.d.). Another example of legal mandates exists in the realm of automotive cybersecurity and can be given as described by Burzio, Colajanni, Cordella, Marchetti, and Stabili, with the Society of Automotive Engineering's (SAE) Recommended Practice J3061. This protocol provides a design to end of life framework and guidance for development of cybersecurity measures in physical vehicle systems (2018). Given that the development of these legal measures is only recent, IoT as a security infrastructure still requires work, something that users of the knock activated lockbox should be aware of.

The process of building a sound IoT device in the business realm can be put into a framework that describes the development approach. Applied to IoT technology, Cooper, Coulton, Hands, and Lee describe the concept of New Product Development (NPD) (2019). At its core, NPD defines a market opportunity and results in the delivery of a product addressing this opportunity. Through validating assumptions in a linear fashion, products can be developed based on executive insights, focusing on consultation advice rather than customer thoughts. This process guidance, however, does not accurately describe IoT product creation, rather, a value "constellation" is a better depiction of demonstrating the interaction between customers and producers, as shown in Figure 4 on page 9.

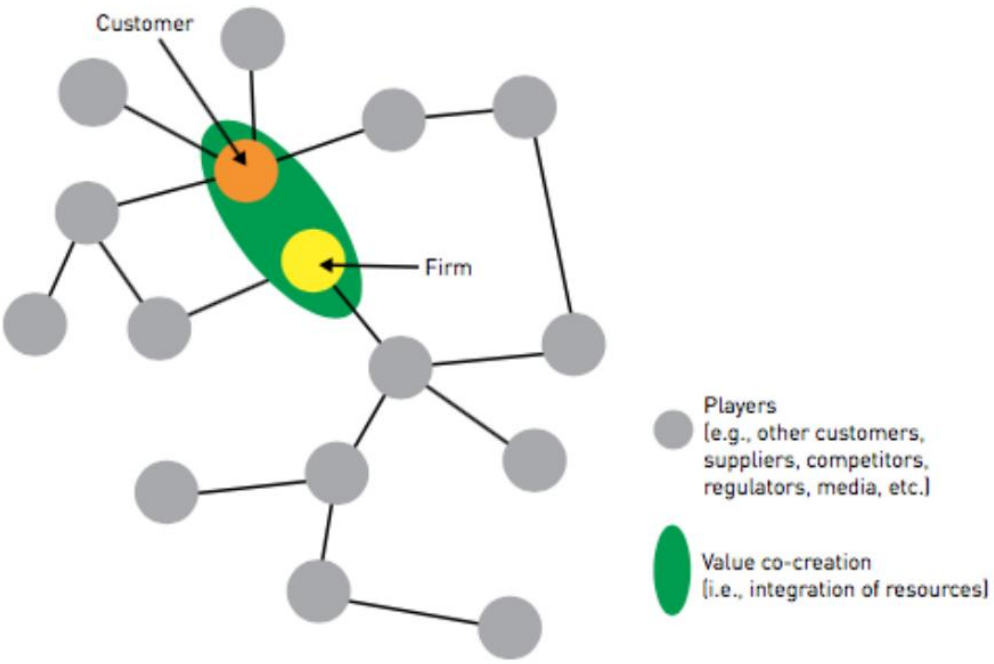

Figure 4: The "value constellation" demonstrating the co-creation of IoT technology with a customer and the production firm. The interconnects are clearly shown as grey nodes, which could correspond to big data, business analytics, and other influences (Cooper et al. 2019).

While cybersecurity is a definite concern for users of the product, a perhaps more important potential flaw of this system is the nature of the access method itself. Using an auditory input as a means of unlocking a lockbox may be creative but comes with certain technical drawbacks. Hackers, if aware that a knock method is being used for entry, can implant listening devices into the owner's home and easily access the box that way, a simpler attack process than more traditional locking methods. Another foreseen weakness of this product is the accidental unlock case. Outside vibrations and noise could potentially trigger an unlock, leading to very undesirable consequences, for both the customer and the creators. Implications of accidental or false positive unlocks could be devastating with high-value assets involved.

Given the connections of the IoT and cybersecurity to society at large, an STS framework can be applied as a summary of this network. With the Social Construction of Technology

(SCOT) model, arrows go in both directions because groups inform the IoT device's activities and the characteristics of the technology, while the product is equally providing value to each group. Business development will facilitate the process of making the product to fulfilling customer needs, all while allowing monetary gain. Government regulations will mandate the technology with current laws, which the technology will also help develop, in a feedback type manner. Manufacturers, of course, play a role in the product as well, who are expected to provide standardized, reliable components. Cybersecurity concerns, as described in detail, allow for the IoT product to develop effectively and will change as the product demands more security measures. Finally, the end user, the most important group, will determine whether a certain IoT product is necessary or up to par with their needs, allowing for revisions and redesigns. These groups govern the development of the IoT device, and the IoT device changes each group's perceptions with its development, as illustrated in Figure 5 below.

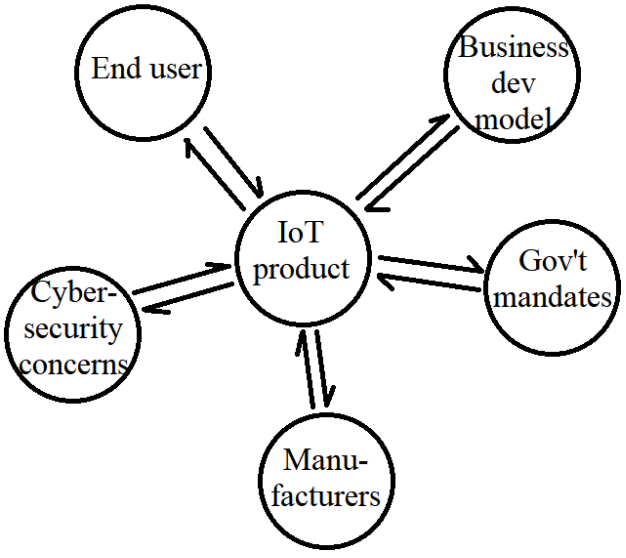

Figure 5: SCOT model for an IoT product. The product at the center transfers and receives value to and from each of the labelled groups (Adapted by Cetin (2022) from Carlson, 2009).

MAKING THE "TAP BOX" A REALITY

The technical aspect of this project addresses the working mechanism for the final product, while the STS topic explores the implications of this device being deployed in the real world. To succinctly describe potential societal effects, cybersecurity as a whole must first be realized and understood. The IoT world is expanding and so are cybersecurity risks. Being able to manage and reduce these risks effectively will allow for less intrusion as well as higher levels of the public's trust in these devices. Especially in the case of a device that stores valuables, security and confidence in the user must be prioritized.

Through careful design decisions, and consideration of the potential societal impacts that this product could have, the construction of the lockbox will be carried out methodically and documented thoroughly. The vision for the end product is a creative, yet useful system to store valuables securely.

REFERENCES

Bernabe, J., & Calero, J., & Skarmeta, A., & Zarca, A. (2020). Virtual IoT honeynets to mitigate cyberattacks in SDN/NFV-enabled IoT networks. *IEEE Journal on Selected Areas in Communications, 38, 1262-1277.* doi:10.1109/JSAC.2020.2986621

Burzio, G., & Colajanni, M., & Cordella, G., & Marchetti, M., & Stabili, D. (2018). Cybersecurity of connected autonomous vehicles: A ranking based approach. *2018 International Conference of Electrical and Electronic Technologies for Automotive*. doi:10.23919/EETA.2018.8493180

Cetin, Y. (2022). 3D model of the "Tap Box". [Figure 2]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Cetin, Y. (2022). Gantt chart of project. [Figure 1]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Cetin, Y. (2022). Overall functional block diagram of the "Tap Box". [Figure 3]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Cetin, Y. (2022). SCOT model for an IoT product. [Figure 5]. *Prospectus* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Cooper, R., & Coulton, P., & Hands, D., & Lee, B. (2019). Value creation for IoT: Challenges and opportunities within the design and development process. *IEEE Xplore*. doi:10.1049/cp.2019.0127

Forno, R., & Mateczun, L., & Norris, D. (2022). The future of local government cybersecurity. *Cybersecurity and Local Government, 201-226*. doi:10.1002/9781119788317.ch12

Hasan, M. (2021, September 22). State of IoT 2021: Number of connected IoT devices growing 9% to 12.3 billion globally, cellular IoT now surpassing 2 billion. IoT Analytics. https://iot-analytics.com/number-connected-iot-devices/

Hoefer, S. Secret knock activated drawer lock. (n.d.). Retrieved September 21, 2022, from https://cdn-learn.adafruit.com/downloads/pdf/secret-knock-activated-drawer-lock.pdf

IoT cybersecurity: Regulating the internet of things. (n.d.). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/iot/inspired/iot-regulations

Jolly, B. (2021). IoT device battery life: Go slow for fast insights into challenging conditions. *2021 IEEE International Midwest Symposium on Circuits and Systems (MWSCAS).* doi:10.1109/MWSCAS47672.2021.9531705

Usmonov, B., & Evsutin, O., & Iskhakov, A., & Shelupanov, A., & Iskhakova A., Meshcheryakov, R. (2017). The cybersecurity in development of IoT embedded technologies. *2017 International Conference on Information Science and Communications Technologies (ICISCT)*. doi:10.1109/ICISCT.2017.8188589

Whittaker, Z. (2020, June 1). After a spate of device hacks, Google beefs up Nest security protections. TechCrunch. https://shorturl.at/cglpB