Exploring New Ways to Improve Privacy and Safeguard User Data for IoT Devices

Sagar Patadia
Saipriya Sairam
Adiv Sivakumar
Michael Cantwell

Bailey Metz
Michael Afrin
Jolie Beviss

Mercy Barigala
Russell Burkhalter
Rashid Annahas

University of South Carolina
CSCE 522
November 15, 2018

Survey

Currently, 40% of the world's population is considered actively online. By 2020, at least 40 billion more "smart" devices will be launched into our society. These devices will impact our known society in monumental ways, contributing to some of the greatest breakthroughs of mankind. At the same time, however, these devices are at great risk of cyberattack since IoT is just beginning to emerge. Exploits of these devices are being steadily recorded and the estimated costs of cyberattacks on these devices will be 2 trillion dollars by 2020. Sadly, security risk awareness is not present in today's consumer and developer mindset. Despite the fact that so many people and businesses are actively using IoT devices, security standards have not yet been implemented.

Beyond conceptualizing the ideas of secure resolutions, we also need to establish a baseline infrastructure that will provide secure software guidelines for all IoT devices. Furthermore, the debate between whether the answer to secure IoT devices lies within the aspect of hardware or software will need to be assessed in future research. As it stands, an IoT device is readily susceptible to tampering or software security failures which poses great risk of cyberattack.[1]

Limitation 1:

IoT devices have constrained memory and storage and aren't capable of performing complex encryption and decryption quickly enough to transmit data in real-time making them vulnerable to side-channel attacks.

IoT devices are very small. They do not have top of the line hardware and do not have the option to be upgraded. Some IoT devices may not have a RAM size large enough to store all routing information. "Common low-cost IoT devices have significant resource limitations (e.g. 16-32 kB RAM)—both due to cost per device and energy consumption when adding RAM".[2] Flash memory may be a solution to this storage issue, but it also falters before other parts of the device under low-battery circumstances. The previously referenced article refers to the IoT devices having "harsh memory constraints".[2] An issue such as limited memory and storage could cause complex encryption and/or decryption to be slower than ideal.

The limited amount of resources available to IoT devices create a major issue for algorithms attempting to complete complex encryption and decryption methods for these devices in order to achieve privacy. Many researchers have attempted to tackle this problem by looking at different ways of implementing such algorithms so that not a lot of resources are needed for the encryption while others have explored decreasing certificate sizes and changing the handshake process. However, one research group has found a way to achieve fast database querying for cloud data which is often transmitted to IoT devices, sometimes insecurely, making it an integral part of IoT device privacy. Since cloud data is vulnerable to attackers the current method of keeping it secure involves encrypting the data before storing it on the cloud. After querying the database, the IoT device then has to decrypt the data before being able to use it. The problem lies in the fact that decryption is a long and difficult process for IoT devices to complete. Ho et al aim to solve this problem by using a solution that takes advantage of parallel computing.[5] First, the Iot device queries the database for the data it needs. After finding that data, normally the device would have to decrypt each of them one by one. In the parallel processing solution, this process is simplified by dividing the decryption into subparts and decrypting those subparts simultaneously. The net result is a decryption algorithm that is up to 2 times faster than conventional methods and works well with the constrained resources of IoT devices.

Internet of Things consists of the unification of a wide variety of devices. Some of these include, but aren't limited to, miniaturized devices, data analytics, and Cloud. IoT infrastructure encompasses a range of devices suitable for small scale setting (e.g., homes) to a large scale (e.g., transportation systems). As a result, feedback control system(use feedback where a part of the output signal is returned back to the input to diminish errors and increase stability) requires real-time performance. Our point of focus for the real-time issue will be in the context of industrial IoT. Closed loop industrial automation introduces rigid end-to-end delay requirements on communication of data. To aid a control loop, the network regularly sends data from sensors to a controller and then sends the control commands to the actuators within an end-to end deadline. Missing this deadline may lead to inefficiency in production, equipment ruination, and many such issues. As one can conclude by this point, real-time IoT requires end-to-end real time performance (e.g. miniaturized devices use real-time embedded systems, data analytics use real-time analytics, and Cloud uses real-time data processing). 'Real-time communication in industrial WSANs is challenging due to their limited bandwidth and multi-hop mesh topologies'.[7] Additionally, WirelessHART (an industrial standard) utilize Multi-channel TDMA to achieve predictability and reliability within in the communication. Communication delays within these networks are impacted by conflicts within transmission. 'Because conflicting transmissions cannot be scheduled in a same time slot, transmission conflicts contribute significantly to the end-to-end communication delays of data flows'.[7] Though many recent studies have been conducted on this issue, there has not been much emphasis on routing algorithms specifically devised for recent industrial WSAN standards. furthermore, they usually ignore transmission conflicts in routing decisions, which negatively impact the capability to meet the delay requirements of many real-time flows.

IoT devices don't have top of the line security and because of the lack of complex encryption as well as the slow nature of the transmitted data, devices become highly susceptible to side-channel attacks. These attacks are attacks that mainly rely on the relationship between the information that is released through a "side channel" and the privacy of that data is compromised. The two ways to mitigate this issue have been to find ways to eliminate or reduce the release of such private information and/or to eliminate the information that ties the secret data to the released data. The solutions to this issue have to make the leaked information seem uncorrelated to the secret data. One way to solve this issue that has been discussed is to the SM9, ECDSA or SM2 algorithms[3]. The issue with this solution is that the attack methods that these algorithms are all used for different attacks. This means there is more effort needed than there should be and the solutions are thus less desirable. It would be smart to find a solution that encompasses the mitigations together so that the problem can be smoothly and quickly fixed.

Limitation 2:
IoT devices don't have the resources necessary to communicate across the network securely and messages are not encrypted before being sent.

There are new IoT devices introduced every day, and they all try to beat their competition by being the smallest, fastest, or most versatile. In doing so, it creates a problem that consumers don't notice, the constriction of resources. Most of the IoT devices have a limited storage, memory, and processing capability. They often need to operate with minimal power usage since most of them are battery operated. Since these devices are so small, they use a fast performing encrypted algorithm, instead of a more powerful and secure algorithm because of the restricted resources. This opens the IoT device to side-channel attacks. IoT devices have to communicate between themselves and a server that either regulates their actions, or coordinates their states. When this communication is sent or received in plain-text, it can be easily snooped on by attackers. If these devices used encrypted communication, they wouldn't be so easily snooped on, but IoT devices aren't known for their incredibly intensive hardware. IoT devices are barebones, to accomplish a simple goal like turning on a light bulb, so they aren't made with powerful computational skills.

A few ideas have been laid out that would encrypt communications through one-time secret keys that are time-based, but they would still require storage and computational power that all IoT devices might not be able to reach currently. Though, it could be used in the future as a base-line for hardware in these devices, but that would require a standard to follow, and that has its own hoops to jump through.

Due to most IoT devices being too small to contain the processing power or memory to handle traditional encryption and decryption of messages, many plain text messages can end up being sent across insecure channels. Increasing the resources in IoT devices would make them less practical, so there must be a more efficient method of securely sending data implemented. The computationally efficient process of digital watermarking may be able to provide this. Digital watermarking embeds the data into the message in a manner that only the authorized recipient can retrieve rather than encrypting the entire message[4]. This secures the link between an IoT device and its network, which can often be an overlooked point of a network's security.

IoT devices operate deep within the network, so traditional security measures, such as antivirus, patching, and perimeter defense, are not as effective because the IoT environment is dynamic and operates on multiple devices. IoT devices can interact with other devices through explicit and implicit channels. An example of an explicit channel would be a single app using multiple IoT devices, and an implicit channel would be an IoT light bulb triggering an IoT light sensor. Because of this, both physical and computational components of a device are being exposed to a vulnerability, such as exposed access or exposed account information such as username or password. A proposed solution would be to use a brute-force strategy and list the networked IoT devices, each with a corresponding security context and environment variables. The set of possibilities is represented as a set S, and each state will have a security posture defined. These security postures define the way the network traffic for each device will be dealt with.[12]

Citations

[1] Marcel Medwed. 2016. IoT Security Challenges and Ways Forward. In Proceedings of the 6th International Workshop on Trustworthy Embedded Devices (TrustED '16). ACM, New York, NY, USA, 55-55. DOI: https://doi.org/10.1145/2995289.2995298

[2] Joakim Eriksson, Niclas Finne, Nicolas Tsiftes, Simon Duquennoy, and Thiemo Voigt. 2018. Scaling RPL to Dense and Large Networks with Constrained Memory. In Proceedings of the 2018 International Conference on Embedded Wireless Systems and Networks (EWSN ’18). Junction Publishing, USA, 126-134.

[3] Qi Zhang, An Wang, and Yongchuan Niu. 2018. Side-Channel Attacks and Countermeasures for Identity-Based Cryptographic Algorithm SM9, Security and Communication Networks, vol. 2018, 14 pages. DOI: https://doi.org/10.1155/2018/9701756

[4] Abdelkader Laouid, Muath AlShaikh, Farid Lalem, Ahcène Bounceur, Reinhardt Euler, Madani Bezoui, Habib Aissaoua, and Abdelkamel Tari. 2018. A distributed security protocol designed for the context of internet of things. In Proceedings of the 2nd International Conference on Future Networks and Distributed Systems (ICFNDS '18). ACM, New York, NY, USA, Article 26, 5 pages. DOI: https://doi.org/10.1145/3231053.3231079

[5] Kim Giau Ho, Ly Vu, Nam Hai Nguyen, and Hieu Minh Nguyen. 2017. Speed up Querying Encrypted Data on Outsourced Database. In Proceedings of the 2017 International Conference on Machine Learning and Soft Computing (ICMLSC '17). ACM, New York, NY, USA, 47-52. DOI: https://doi.org/10.1145/3036290.3036299

[6] Chenyang Lu. Real-time Internet of Things. Retrieved November 2, 2018 from https://www.cse.wustl.edu/~lu/talks/isorc17-keynote.pdf

[7] Chenyang Lu. Real-time Wireless Routing for Industrial Internet of Things. Retrieved November 2, 2018 from https://www.cse.wustl.edu/~lu/papers/iotdi18.pdf

[8] Said Ouissal. 2018. It's Time to Redefine Real-Time for IoT. (June 2018). Retrieved November 2, 2018 from https://www.sensorsmag.com/iot-wireless/it-s-time-to-redefine-real-time-for-iot

[9] Thomas Scheffler and Olaf Bonneß. 2017. Manage resource-constrained IoT devices through dynamically generated and deployed YANG models. In Proceedings of the Applied Networking Research Workshop (ANRW '17). ACM, New York, NY, USA, 42-47. DOI: https://doi.org/10.1145/3106328.3106331

[10] Anna M. Gerber. 2017. Top 10 IoT security challenges. (November 2017). Retrieved November 2, 2018 from https://developer.ibm.com/dwblog/2017/iot-security-challenges/

[11] Tianyi Song, Ruinian Li, Bo Mei, Jiguo Yu, Xiaoshuang Xing, and Xiuzhen Cheng. 2017. A Privacy Preserving Communication Protocol for IoT Applications in Smart Homes. 2016 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI) (May 2017). DOI: https://doi.org/10.1109/JIOT.2017.2707489

[12] Tianlong Yu, Vyas Sekar, Srinivasan Seshan, Yuvraj Agarwal, and Chenren Xu. 2015. Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the Internet-of-Things. In Proceedings of the 14th ACM Workshop on Hot Topics in Networks (HotNets-XIV). ACM, New York, NY, USA, Article 5, 7 pages. DOI: https://doi.org/10.1145/2834050.2834095