A Study of the Advances in IoT Security

Andrew Dean and Michael Opoku Agyeman
Department of Computing, University of Northampton, Northampton, United Kingdom

***Abstract*— The Internet-of-things (IoT) holds a lot of benefits to our lives by removing menial tasks and improving efficiency of everyday objects. You are trusting your personal data and device control to the manufactures and you may not be aware of how much risk your putting your privacy at by sending your data over the internet. The internet-of-things may not be as secure as you think when the devices used are constrained by a lot of variables which attackers can exploit to gain access to your data / device and anything they connected to and as the internet-of-things is all about connecting devices together one weak point can be all it takes to gain full access. In this paper we have a look at the current advances in IoT security and the most efficient methods to protect IoT devices.**

Keywords*— *Hardware, IoT, Security, Efficiantcy

I. Introduction

The internet-of-things is how physical devices interconnect together and is made up of billions of devices which use wireless technologies to communicate. The IoT world is growing rapidly with an estimated 8.4 billion connected devices in 2017 with is an increase of 31% and is expected to grow by another 33% by 2018.

Category	2016	2017	2018	2020
Consumer	3,963.0	5,244.3	7,036.3	12,863.0
Business: Cross-Industry	1,102.0	1,501.0	2,132.6	4,381.4
Business: Vertical-Specific	1,316.6	1,635.4	2,027.7	3,171.0
Total	6,381.8	8,380.6	11,196.6	20,415.4

Fig. 1. IoT Devices (Millions of Units) source : Gartner (January 2017)

IoT works by receiving data from there surrounding in the physical world using sensors sensors, processors and communication hardware and then act on the data. These devices are often called “smart” devices and can talk to other devices using commination standards. And then act of the data received. Fig. 2. Shows an example on how a smart fridge works on the IoT platform using a sensor (Perception layer) to detect the current temperate which can then be sent using WIFI (Network layer) to a mobile device and displayed on a app (application layer) which could be used to change the desired temperature to send back to the fridge to act on.

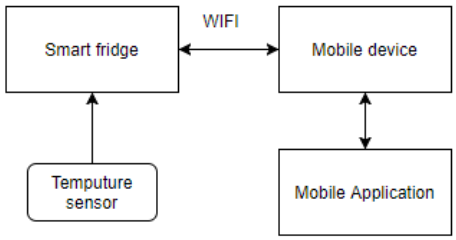

Fig. 2. Smart Fridge IoT

The internet-of-things is very vast which covers a range of domains, which have specific architectures based on their needs. IoT Technology has a lot of real world applications in a wide range of fields such industry automation which can streamline the manufacturing process and optimize efficiency.

II. IoT Archutecture

A. Layers

The IoT architecture can be split into three basic layers, however they can change based on the use case’s as some industry solutions may require further layers.

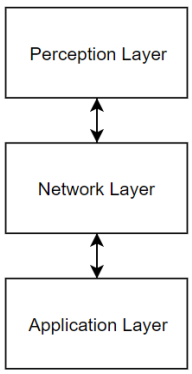

Fig. 3. IoT Layer Diagram

B. Preception

The perception layer is made up of physical devices such as your sensors and actuators which interact with other devices and the physical world to both send and receive data to other devices using wireless technology. [1] This layers objective is to collect all the information from its sensors and actuators. Which can be sent to the network layer.

C. Network

The network layer handles the data been sent between smart devices as well as network devices and servers and can be also used to transmit and process perception layer data into a readable format for the receiving device. Some say this is where the Internet-of-things happens as it bridges the cyber and physical world which allows them to interact with each other, this layer uses a range of technologies (Routers, switches, cloud computing) which processes and directs the data to the specific application layer where the data can be read. many communication technologies are uses to transmit the data which can depend on the deployment of the perception layer, but this includes more than just WIFI as other wireless technologies can have advantages such as Bluetooth for collecting a consolidating data from short ranges or RFID. [1]

D. Application

The application layer which can also be called the business layer delivers specific services to the users, and receives the data from the sensors/actuators from the perception layer after being translated into a readable format by the network layer. The application layer can then use this data to provide services or perform operations based on the data received. This layer can analysis and store the data received to create predications or see trends which could be invaluable for a company to see the current and future states of their products/devices. [1]

III. ENABLING TECHNOLOGIES

A. Hardware Platforms

There is an abundance of IoT hardware platforms and development kits available, Fig. 3 shows a few of the most popular and recent released and you can see the specifications vary quiet a lot because there designed for handling different solutions.

	Processor	Clock speed	System Memory	Flash memory	voltage
Arduino Yun	Atheros AR9331	16Mhz	2.5KB	32KB	5V
Raspberry Pi 3 B+	Broadcom BCM2837	1.2GHZ	1GB	SD card (-32gb)	5V
ESP8266	Tensilica L106 32-bit microcontroller	80MHZ	64KB	94KB + 16MB external	3.3V
Beaglebone Black	AM335x ARM® Cortex-A8	1GHZ	512MB	4GB	5V
Intel Edison	22 nm Intel® SoC	500MHZ	1GB	4GB	3.3 – 4.5V
Netduino 3 wifi	Cortex-M4	168MHZ	164 + kb	1408KB + 2GB SD	3.3 – 5V
UP Squared	Celeron N3350	2.4GHZ	2GB	32GB	5V

Fig. 4. IOT Hardware Platforms

The devices with lower specifications would be ideal for solutions with smaller tasks which would require less processing power and will come with a lower cost making them more efficient then using a device with high specifications.

B. Communication

IOT to work needs a way to send to send the data between devices to both gather the needed data and receive instructions based on the sent data. Depending on the deployment of the device it could use a range of commutation technologies and there are both short and long-range standards.

Name	Frequency	Range	Examples
RFID	13.56 MHz	10cm - 200m	Road tolls, Building Access, Inventory
EnOcean	315 MHz, 868 MHz, 902 MHz	30 - 300m	Wireless switches, sensors and controls
NFC	13.56 MHz	< 0.2 m	Smart Wallets/Cards, Action Tags, Access Control
Bluetooth	2.4GHz	1-100m	Hands-free headsets, key dongles, fitness trackers
WIFI	2.4 GHz, 3.6 GHz	100m +	Routers, Tablets, etc
Weightless	470–790MHz	Up to 10km	Smart meters, traffic sensors, industrial monitoring
GSM	850 - 900MHz	n/a	Cell phones, M2M, smart meter, asset tracking

Fig. 5. IoT Commication standards

Fig. 5. Shows some of the most used communication standards as well as some deployed examples. All come with pros and cons such as RFID which is ideal for very close proximity commutation but lacks any security so is vulnerable to data hijacking, but the attacker would need to be very close to do so which makes it impossible to do long range attacks.

C. Cloud solutions

Cloud solutions are very important to the internet-of-things as it allows ubiquitous access to a shared pool of resources, all the devices in the perception layer can using the network layer send the information to be analysed and accessed by the application layer.

Provider	model	capture	visualization	Analytics

Amazon web services	IaaS	Yes	Yes	Yes
Google cloud	IaaS	Yes	Yes	Yes
Windows azure	IaaS	Yes	Yes	Yes
Rackspace Open Cloud	IaaS	Yes	Yes	No
Engine yard	PaaS	Yes	No	No
Red hat Open shift	PaaS	No	No	No
Heroku	PaaS	No	Yes	Yes
Salesforce	SaaS	No	No	Yes
Microsoft office 365	SaaS	Yes	No	Yes
Google apps	SaaS	Yes	No	Yes
Zendesk	SaaS	No	No	Yes

Fig. 6. Cloud Providers

There are some different types of cloud computing which suit different solutions Fig. 6. Shows some of the most used providers as well as their features.

1) IaaS

Infrastructure as a Service is a model is where an organization/business will rent out specific services needed for there solution and is usual a "pay as you go" basis. This means you will only pay for what you use unlike other services which your rent all their services for a fixed price even if you don't use some.

2) PaaS

Platform as a service is designed to streamline the development process by shifting the system management to the provider and offering pre-configured components for businesses/organization to use such as Databases/ application servers / programming languages.

3) SaaS

Software as a service is a cloud service which offers software on demand which are hosted and managed by the provider and is normally a subscription and can improve communication and team collaboration.

IV. IoT Device Constraints

A. Power Consumption

Devices are built for a purpose and will be designed based on that purpose. And the more a device must do such as store/collection information will add to the power consumption. Adding extra security to a device will require more power then the original design, implementation methods such as encryption will increase the power needed to complete the same operation.

B. Processing

Processing on a device is also another constraint to implementing better security as the process will need to perform they designed task as well as the security on top of which could involve extra gates/transistors and additional modules to do so.

C. Design

The design of a device is also a constraint as the size of the device could also be a factor which implements extra modules / transistors will influence the devices designs size and complexity. These implementations could include cost and efficacy which could render the solution to be unviable for deployment. By running simulations, the design can be tested and optimized before building which will reduce the cost and make the device more efficient.

V. IoT Device Efficiantcy

Making a deice more efficient has the benefit of making the device not need as much power or resources to do the same job which will as a result decrease the cost.

A. Code compression [3]

Code compression can be used improve a devices performance and power consumption when used with encryption and integrity checking to secure processor memory transactions can reduce the memory footprint as well as providing more information per memory access.

VI. IoT Device Security

With this increase in IoT devices we can see many advantages for both consumers and businesses which streamline a lot of processes, but they can also come with some disadvantages. One of these disadvantages is security & privacy and having our personal data (banking information / location / activity) being transmitted between devices comes with the risk of losing a lot of our privacy. The IoT opens the doors to many malicious hacks who wish to exploit IoT device weaknesses to access our personal information to be used for their own gain.

A. Authentication

1) Noise Insertion [7]

Noise cancelation aim to protect the raw data when its inside the computing unit to avoid an attacker from using side-channel attacks to retrieve the data.

The way this method works is by inserting noise using a key for sensitive data, although this method isn't as secure as encryption it has the benefit of being very lightweight in comparison. By selecting key locations where the data noise is canceled out making it readable you can keep the data secure in the device and eliminate unnecessary overhead.

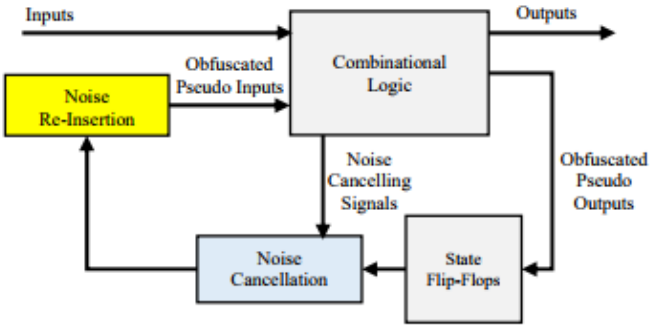

Fig. 7. Noice canselling scheme

2) Logic Locking [9]

Logic locking is a relatively new technique which includes adding extra gates to the design for locking "Key gates" which would change the output and affectively lock the gates correct functionality.

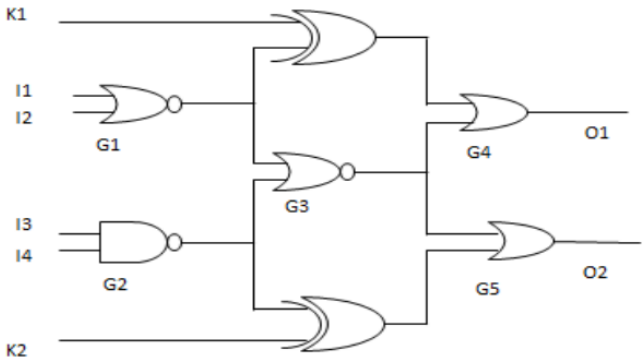

Fig. 8. Logic Locking example

This technique increases the security level over other less secure methods such as IC Camouflaging which is the method of introducing dummy contacts, so an attacker could extract an incorrect net list. In Fig. 7. some XOR gates are used as key gates which need k1 and k2 to be 0 for the process to continued otherwise the output would hide the original output. When comparing logic locking to an older method (OC Cell) there was a dramatic decrease in the delay without compromising the security.

B. Detection & prevention

1) Security Auditing Module [4]

The purpose of the security auditing module proposed as apart of a security architecture is to monitor both internal and external operations to evaluate the devices stability which will prevent device damage, alarm the network of any fatal issues with the device and detect security threats.

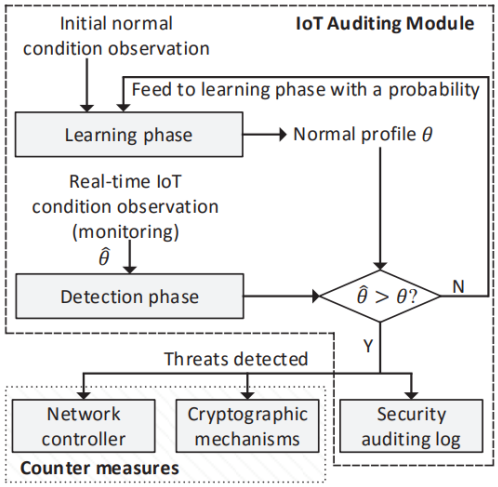

Fig. 9. Security auditing module

Using this module other time can create profiles representing the devices behavior which can be analysed to improve efficiency and detect threats quickly which could prevent loss/compromised data.

2) Attack Detection Unit [8]

The purpose of the attack prevention unit is to detect when a device is under attack and alert the device of this attack, so it can prevent device damage or a compromised device.

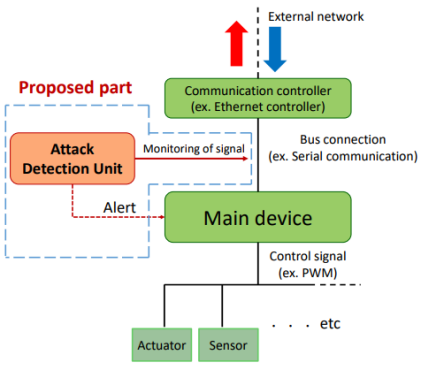

Fig. 10. Attack Detection unit Implimentation

This is done by monitoring the electrical signals from the communication controller which will detect abnormalities in the physical characteristics of the bus communication between the CM and main device. This is not part of the main device it won't interfere with the devices processing power and can be implemented on many devices with a communication controller.

3) Random Canaries Repository [2]

RSR aims to protect against Stack smash attacks which exploit vulnerabilities of the buffer overflow to hijack control of applications. RCR is an enhancement of Stack Smash protector by producing a repository of random values of canary which are used when the application detects an attack the RCR approach increase the difficulty of the attack. To

implement this method no special hardware is needed and can prevent SSA against canary stacks with negligible overhead.

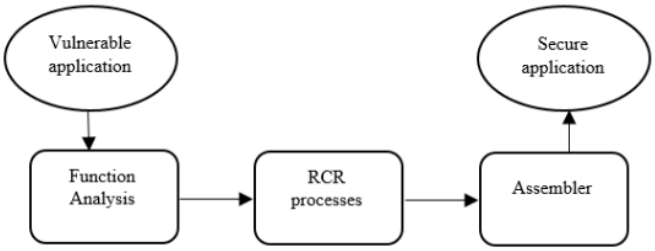

Fig. 11. RCR Approach

Fig. 11 shows the steps of the RCR approach, and in the RCR Processes section the safe code is prepared and the area of random canaries stack at the memory is utilized. Using the time, date and application ID random values are generated an stored in the RCR which can then be copied three times and stored in heap memory. Making the RCR read-only with only "const" variables will prevent attackers form being able to access or alter and as the RCR is a global variable it doesn't need to be referenced in the stack.

C. Isolation

1) Secure sensing [6]

A sensor framework has been suggested based on hardware isolation which will protect the sensors on a device from a compromised application. This is done using the hardware isolation feature on ARM processors, and by deploying a sensor IP into the isolated area which is protected from compromised applications.

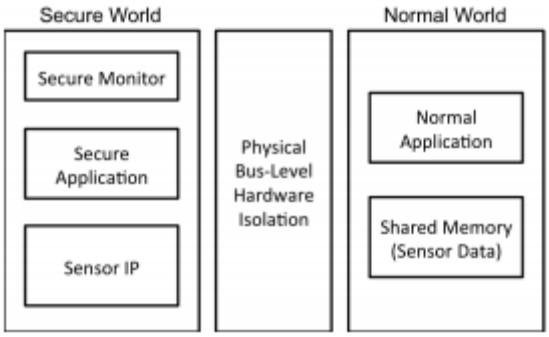

Fig. 12. Secure sensing overview

By deploying shared memory in the normal world which the secure world can access we are able to share the sensors data when needed. The application can then request to the secure monitor in the secure world which can then switch the application mode from normal world to secure world which can verify the request has been authorized. The senor data once the request has been verified and checked for any potential threats can be written to the shared memory which can be read by the normal world.

2) Secpage [5]

Secpage is both a hardware and software lightweight architecture which aims to protect the devices memory by providing an isolated memory environment which protects sensitive code and data. This security method provides compromised systems software with a secure isolated and trusted environment to avoid data and code access buy unauthorized users but also provides availability to easy access to pages which don't need to be secure which reduces the overhead of the architecture implementation.

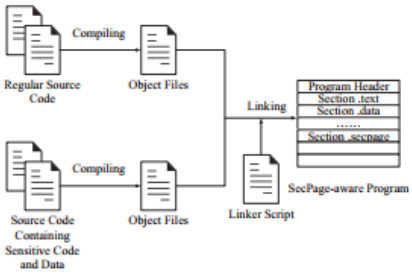

Fig. 13. Building a SecPage aware rogram

VII. Coclusion

Security is an important issue with IoT as we can see, and with IoT expending to a lot of industries and services such as industry and healthcare security will keep being more important to protect sensitive data and devices against damage. The perception layer is obviously the most vulnerable as it is deployed in the real world and normal embedded into a product which could be taken apart and interfered with and as it will normally have a connection other device using the network layer which could be exploited to either steal or send harmful data. With devices normally being constrained by normally cost, design and efficiency it means we can't add the best security without overhead side affect which would make the deployment either unviable or too expensive we need to invest in more lightweight security which can't help preventing attacks. IOT has many benefits but is growing at a rapid pace and some devices are stuck with outdated security leaving them vulnerable to attack and are constrained by the devices processing & power consumption limitations.

References

[1] J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang and W. Zhao, "A Survey on Internet of Things: Architecture, Enabling Technologies, Security and Privacy, and Applications," in IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1125-1142, Oct. 2017.
doi: 10.1109/JIOT.2017.2683200

[2] D. A. H. Shehab and O. A. Batarfi, "RCR for preventing stack smashing attacks bypass stack canaries," 2017 Computing Conference, London, United Kingdom, 2017, pp. 795-800.
doi: 10.1109/SAI.2017.8252186

[3] E. W. Netto, R. Vaslin, G. Gogniat and J. P. Diguet, "A Code Compression Method to Cope with Security Hardware Overheads," Computer Architecture and High Performance Computing, 2007. SBAC-PAD 2007. 19th International Symposium on, Rio Grande do Sul, 2007, pp. 185-192.
doi: 10.1109/SBAC-PAD.2007.40

[4] F. Ye and Y. Qian, "A Security Architecture for Networked Internet of Things Devices," GLOBECOM 2017 - 2017 IEEE Global Communications Conference, Singapore, 2017, pp. 1-6.
doi:10.1109/GLOCOM.2017.8254021

[5] K. Liang, Y. Feng, J. Wei and W. Guo, "SecPage - A Lightweight Memory Protection Architecture," 2016 IEEE Trustcom/BigDataSE/ISPA, Tianjin, 2016, pp. 1917-1922.
doi: 10.1109/TrustCom.2016.0293

[6] M. Ye, N. Hu and S. Wei, "Lightweight secure sensing using hardware isolation," 2016 IEEE SENSORS, Orlando, FL, 2016, pp. 1-3.
doi: 10.1109/ICSENS.2016.7808904

[7] Y. W. Lee and N. A. Touba, "Computing with obfuscated data in arbitrary logic circuits via noise insertion and cancellation," 2017 IEEE Conference on Dependable and Secure Computing, Taipei, 2017, pp. 146-152.
doi: 10.1109/DESEC.2017.8073840

[8] R. Jinnai, A. Inomata, I. Arai and K. Fujikawa, "Proposal of hardware device model for IoT endpoint security and its implementation," 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, 2017, pp. 91-93.
doi:10.1109/PERCOMW.2017.7917533

[9] T. Thangam, G. Gayathri and T. Madhubala, "A novel logic locking technique for hardware security," 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), Karur, Tamilnadu, India, 2017, pp. 1-7.
doi: 10.1109/ICEICE.2017.8192439