***Disclaimer:*** *The following document shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal position of IEEE. The following views should be considered the personal views of participating individuals rather than the formal position of IEEE.*

**Development of Proposal for end-to-end Security and Privacy by Design for the Iot**

**Authors | Editors**  
 **Date**

[Your title can make the difference between a great white paper and a good white paper. Spend time crafting a title that will grab your readers’ attention and entice them to read and share your white paper.

**Tips:**

* **Review the following questions in preparation for title brainstorming:** Who is your target audience? What are their greatest pain points, needs and/or interests that are being addressed by this white paper? What are you providing in this white paper that your audience cannot get elsewhere? What are the key Google search terms that you’re looking to target/own as a result of this white paper and its related [Content Marketing Pyramid](http://www.curata.com/blog/the-content-marketing-pyramid-are-you-hungry-for-content/)?
* **Grab their attention with a bold title**, but don’t be too risqué. Ensure that your title represents what is truly in the white paper. And remember, focusing on your audiences’ needs versus your own will keep you on a track to success.
* Unless you work in a highly technical industry, **avoid buzzwords** and stick to clear and easy to understand language.
* **Abide by standards in your industry**, but don’t sacrifice the opportunity to differentiate your white paper through the title.
* **Consider** [**search engine optimization**](http://www.curata.com/blog/seo-survival-guide-10-tips-for-content-marketing-success/) as part of title creation.
  + Tap into tools such as [Google Keyword Planner](https://adwords.google.com/KeywordPlanner), [Ubersuggest](http://ubersuggest.org/) and [Buzzsumo](http://buzzsumo.com/).
  + Optimal title length for search engines: “Google typically displays the first **50-60 characters** of a title tag, or as many characters as will fit into a 512-pixel display. If you keep your titles under 55 characters, you can expect at least 95% of your titles to display properly.” [[Moz](https://moz.com/learn/seo/title-tag)]
* **Keep your title short, simple and to the point**. As they say, less is more. Do take the time to create a shorter, more powerful title. Having trouble shortening your title?. . . break it down into sections with a colon, or insert a subtitle that can be more descriptive.
* **Analyze what white paper titles already exist in your industry**. (e.g., by your competitors) Determine what types of titles have been most successful (e.g., Google search, social shares), and what aspects have helped set those white papers apart from the others. You may decide to emulate some of the attributes of the best titles, but don’t be afraid to take a chance and be unique.]

**ABSTRACT OR EXECUTIVE SUMMARY**

[The abstract provides another opportunity to grab your readers’ attention, and convince them that your white paper is worth their time to read. Similar to the white paper title, much time should be spent developing a clear, concise and hard-hitting abstract.

Tips:

* **Write the abstract after you have completed your white paper**.
* **Use a direct structure format for creation of your abstract**. That is, include in this abstract the most attention-getting findings, insights and recommendations from the white paper.
* **Keep it short, simple and to the point.** A commonly recommended length is 150 to 250 words.
* **Put abstract on the title page**. Then, you can use the title page as a separate sheet for your sales team to send to prospects. Add a call-to-action linking to the full white paper and save it as a PDF.
* **Ensure that the abstract answers the following questions:**

1. What is included in this white paper? (e.g., what audience pain or need is trying to be solved)
2. Why should I read this white paper? Give your audience a reason to take time out of their busy schedule to read your white paper.
3. What are the white paper’s conclusions and recommendations?

* **Ask someone to review your abstract**. Preferably someone that knows your audience and has a strong attention for detail.]

**TABLE OF CONTENTS**

**INTRODUCTION 6**

**BACKGROUND/PROBLEM STATEMENT 7**

**SOLUTION 8**

**CONCLUSION 11**

**ADDITIONAL RESOURCES 12**

[Develop an outline prior to beginning the writing process. The outline will eventually take form as its shorter, more succinct cousin, the Table of Contents. The outline will provide a map and related trails that will keep you on the correct path to meet your originally laid out objectives. It will ensure that your messaging and content are on-target, and the information flows in an easy to follow manner for your readers. The following tips and subsequent section examples provide a good starting point.

Tips:

* **DON’T SKIP THE OUTLINE.** Yup, the first tip is that you shouldn’t skip the process of creating an outline. Yes, it will take time and delay start of the writing process; however, it will save you an enormous amount of time in the long run, and more importantly, ensure that you have a better final product.
* **Target your audience’s needs.** It is of the utmost importance that you create a white paper that is focused on the readers’ needs, interests and/or pain points. Take a non-egocentric approach to your content creation, minimizing the attention that you spend on your company and its products. In most cases, there are plenty of other formats to provide company or product-specific information to your audience. (e.g., data sheets) For additional tips on how to align with audience needs, refer to [“The Four Steps to Content Marketing Enlightenment”.](http://www.curata.com/resources/ebooks/4-steps-to-content-marketing-enlightenment)
* **Collaborate with your team for creation of the outline.** As the foundational design of your white paper, modifying your course at this stage will be much easier than having to change direction once the white paper is written. Therefore, include team members as part of development and review of the outline to ensure that your white paper plan is on target. Here are some tips about [collaborating across your organization.](http://www.curata.com/blog/content-marketing-crowdsourcing-across-your-organization/)
* **Plan on many revisions.** Creation of an outline is an iterative process. Don’t hesitate to modify its design during the process.
* **Maintain flexibility.** Although the outline is intended to be the map or architecture for writing your white paper, maintain the flexibility to adjust your outline as necessary once writing begins.
* **Map out sections and subsections.** It is important to break up your text into several sections, including section headers and subheads within each section. This increases readability and allows your reader to skim through the document and absorb the sections that are most relevant to their business.

The below sections provide just one example of how to structure a white paper.]

**INTRODUCTION**

**Introduction:**

Scope: The purpose of this paper is to present a set of well investigated guidelines and best practices which others can use as a basis for standards, certifications, laws, policies and product ratings.

Audience: The paper targets corporate and governmental policy makers, industry experts, and standard setting bodies. Highly technical information will be cited in footnotes and appendices.

Definition of IoT: A wired or wireless network of uniquely identifiable connected devices which are able to process data and communicate with each other with or without human involvement.

Interconnection of uniquely identifiable with embedded computing within the internet infrastructure. Primarily physical things with actuators. [Chachich] Differentiate from web of things.

Footnote: We define Internet of Things (IoT) broadly, to include Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and Cyber Physical Systems (CPS). IoT devices may or may not be accessible by Internet Protocol (IP). They may or may not have a human in the loop. [Stankovic, 2014] http://www.intercom.virginia.edu/~stankovic/psfiles/IOT.pdf

System model and terminology: There are several reference models which can be used as a basis for conceptual consistency and common terminology. In this paper we use [Cisco](http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)'s model.

http://cdn.iotwf.com/resources/71/IoT\_Reference\_Model\_White\_Paper\_June\_4\_2014.pdf

Sample paper: https://www.automotiveisac.com/best-practices/

Tips for writing an Introduction:

* **Set up the problem**, need or pain point right up front.
* **Grab your readers’ attention** in the first sentence or two. Strive to make a great first impression. (e.g., a controversial and/or bold statement)
* **Use data to support your point(s).**
* **Provide additional detail** than what was included in the Abstract, but avoid going into too much detail: Save the details for later sections in the white paper.
* **Introduce a framework** that may be used throughout the white paper or may even provide background into the topic.
* **Indicate the objective(s)** of the white paper, as well as what specifically will be included in subsequent sections. Providing a map or structure to the white paper in the introduction will help your audience follow your thought process and understand how the white paper is organized to achieve its objectives.]

**BACKGROUND/PROBLEM STATEMENT**

[The introduction provided an overview of the white paper. This section offers the opportunity to expand upon this overview, and thoroughly define the problem statement.

Sample questions to be answered in this section:

* What is currently happening in the market today? (i.e., What’s the current situation?)
* What are companies and/or individuals most struggling with and why?
* What are the specific problems, needs and/or pain points?
* **What are the potential benefits of addressing these problems, needs and/or pain points?** (Answering this question within your white paper will help your readers understand why your solution is of value; and more importantly, it will entice them to continue reading.
* What data points help to support answers to the above questions?
* What frameworks and/or models can be used to enhance readers’ understanding of this information?]

**SOLUTION**

[You’ve already provided a succinct description of the most impactful solutions in the Abstract, as well as an overview of these solutions in the Introduction. This section provides the opportunity to go into the specifics of the solutions.

Tips:

* **Introduce the solution(s)**, including a clear definition and even a framework or model.
* **Provide a detailed description** of each part of the solution. Use subcategories as required to help readers draw distinct boundaries between different parts of the solution. Subcategories will also make it easier for your audience to follow your thought process and absorb the content.
* **Be very clear regarding the benefits of each of the solutions**, including how it specifically impacts your audience.
* **Target your solutions to different segments of your audience**, thereby improving the relevancy of your content.
* **Provide specific, real-world examples to support your solution(s).** These examples provide another opportunity to connect with different segments of your audience. (e.g., providing examples that are targeted for 3 different buyer personas)
* **Create a figure and/or table** as a stand-alone sheet to help readers visualize your solution(s). This sheet can also serve as a stand-alone asset for your readers and/or for your internal sales enablement efforts. A few examples of charts and figures from Curata’s recent studies can be seen below.

**SECTION 1** (Mohammed)

**The IoT definition**

The Internet of Things (IoT) is not clear term in a technology world due to many definitions available over there. IoT can be defined as “**a universal digital language or protocol to connect and exchange data and commands between anything (living and non-living things that have unique identifiers), anytime anywhere to improve the quality of life (QoL) and provide best services without requiring human interaction**”. In fact, IoT doesn’t mean the Internet is the only way to connect things, it can be any other communication standard like Bluetooth, Wi-Fi, IR, RF, ZigBee and etc. Also, cyber-physical system and Internet2 refer to the IoT in some textbooks. The IoT enables physical things to see, hear, data analysis and make a decision in smart way.

**The statement of purpose**

End to end security and privacy present a significant challenge for the IoT implementations due to the lack of common standard and architecture for the IoT security. In heterogeneous networks as in the case of the IoT, it is not easy to guarantee the security and privacy of users. The core functionality of the IoT is based on the exchange of information between billions or even trillions of Internet connection objects. One open problem in IoT security that has not been considered in the standards is the distribution of the keys amongst devices [1]. IETF’s Smart Object Lifecycle Architecture for Constrained Environments (SOLACE) started some work to overcome this problem. On the other hand, privacy issues and profile access operations between IoT devices without interferences are extremely critical. Still, securing data exchanges is necessary to avoid losing or compromising privacy. The increased number of smart things around us with sensitive data necessitates a transparent and easy access control management in such a way that for example one vendor can just read the data while another is allowed to control the device. In this regard, some solutions have been proposed such as grouping embedded devices into virtual networks and only present desired devices within each virtual network. Another approach is to support access control in the application layer on a per-vendor basis [1]. Also, talking about E2E security of IoT leads us to discuss security of middleware layer since most of IoT services are cloud-based (public, private and hybrid).

Although a lot of research has been done in the IoT, there is a need for a lot more efforts for it to mature. The increasing attention of governments and industries to this disruptive technology has led to an extensive range of research projects. Some of the challenges like the overall architecture and security have attracted a lot of attention, while others like availability, reliability, and performance still require more attention.

Therefore, a universal IoT security model including security and privacy is needed to assure interoperability and reliability of IoT.

[1] I. Ishaq et al., “IETF standardization in the field of the Internet of Things (IoT): A survey,” J. Sens. Actuator Netw., vol. 2, pp. 235–287, 2013.

(Mohammed)

<David Richardson>

Are the costs – money, time and social - of the use of these security technologies out of scope for this paper? In general, these are the "why not" - why the currently available solutions are not implemented, and why new security technologies are likely to fail (or not). An obvious example is "Why doesn't everyone use e-mail encryption? The infrastructure for it has been in place for a couple of decades." In that case it is just plain hard to use for the "normal" user, and since those of us who do understand it have to communicate with the ones who don't, we have to avoid encryption. Lately there is also a "terrorist threat" fear that makes the use of encryption stigmatized, which is a clear "social cost", plus American law enforcement has made it clear that by using encryption, we are automatically terrorist suspects.

In the case of RFID tags, there is no point to encryption if you are in a warehouse keeping track of boxes, but in the retail store, that same 10 meter range that you need in the warehouse means that someone outside the store can read out every purchase everyone makes, which is a potential threat to e.g. those buying high-priced items, since that high price is a flag for a potential mugger, and that mugger doesn't even need to come into the store.

There is also the case of the INS putting RFID tags into passports, which means that a fairly simple receiver device in the airport customs area can keep track of arrivals and departures – the potential threats of that sort of data capture in a semi-hostile world are astounding. Since this is required by law, it puts every American citizen traveling internationally at risk.

One more case: the "Smart" electric meter, used where the electric company wants to save money on meter reading. Since this is not encrypted, it makes it simple for anyone to read the electric usage of a house or building in small time units. While this doesn't sound like a lot of information, it is "meta-data" of the sort that the US Government collects on e-mail, in that many things can be deduced from it, such as what time the residents get up and leave the house, when they come home, when they are on vacation, and when they are using lots of "grow lights." The first ones are obviously helpful to a potential burglar, and the last one is guaranteed to get a judge to grant a search warrant wherever marijuana is still controlled as a drug – the DEA is not polite society to invite into your house.

A lot of the cost-benefit decisions made by "people" - big generalization, there – are based on the perceived benefits to be gained from privacy vs. The various costs associated with it. From the complete lack of broad acceptance of things like encrypted e-mail, we have to think that privacy is not highly valued, or at least that people are not aware of just how much damage can be done by others' abusing the information that they constantly "leak" through their lack of use of security technologies.

This same economic and social tradeoffs are going to drive the acceptance (or the lack of acceptance) of IoT "best practices", so in many ways these considerations are directly germane to this paper, or at least are part of the environment in which this paper will be read. The problems of IoT security are not purely technical – the Betamax video cassette format was a clear technical win, but the difference between it and VHS did not overcome the various costs associated with it. We are looking at the same sort of issue selling secure IoT as Sony did selling Betamax.

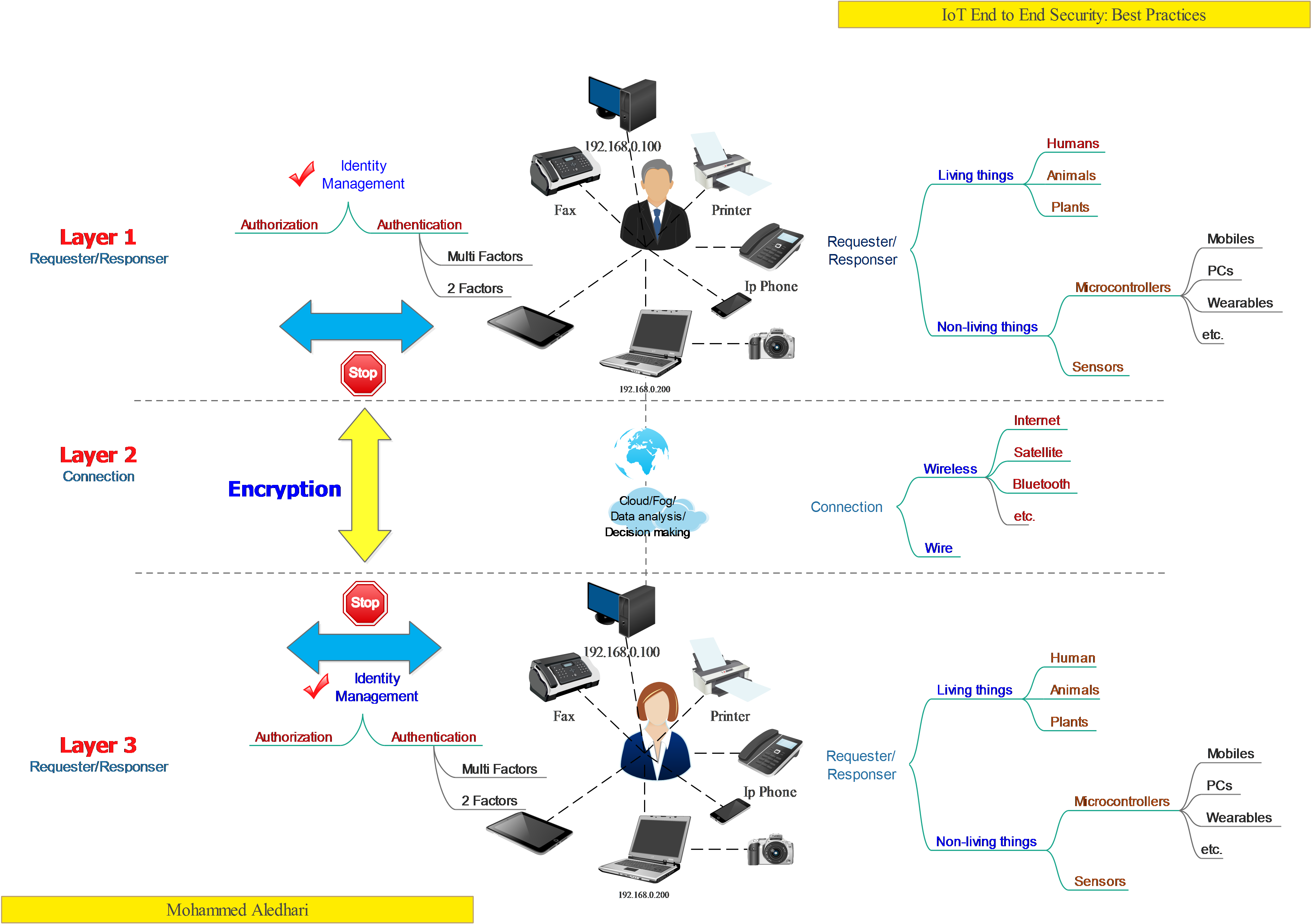
I know that my cultural examples are very much United States-centered, but those are all I have experienced personally.

</David Richardson>

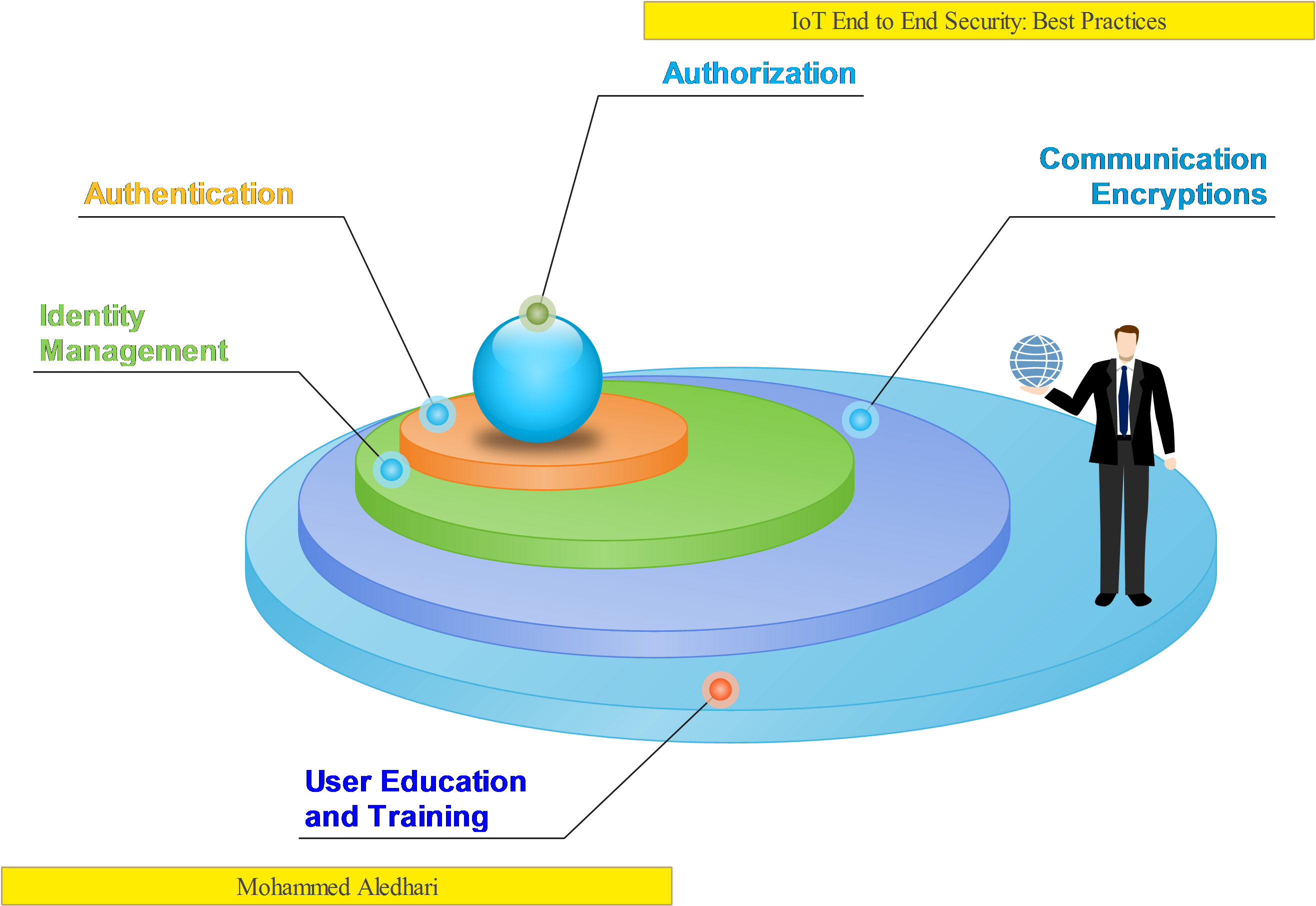
**KEY FINDINGS**

lacking of protocol standardizations for the IoT considered a big challenge because most of these protocols were developed by specific vendors, and these vendors typically promote their own protocol choices, don’t clearly define their assumptions, and ignore the other alternatives. so focusing on standardization will help in creating a solid secure model for IoT.

**FIGURE 1.1**



**FIGURE 1.2**



**The definition – a suggestion (Sukanya Mandal)**

Since 1991, after WWW was formed, internet has changed the way long distance communication was conducted, it created new ways to share and acquire knowledge. It changed the way awareness was spread across communities. It was a great leap when people from different parts of the world were able to connect with each other through internet to share, learn and care.

But then, **what is internet** ?

Internet is “*a global network connecting millions of embedded hardware devices (computer, smartphones, tablets) providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols*.”

And now, the next term – **Things**….

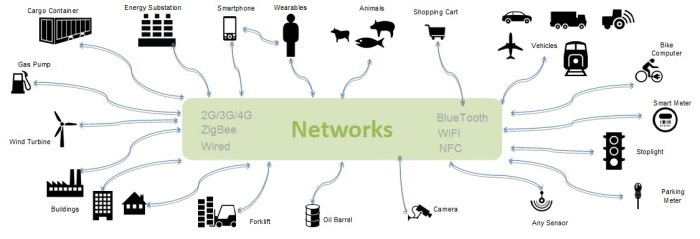
Today, an average household has more devices at home which are connected to internet than the number of people at home.

Each device that is on the internet is identifiable with a unique ID – that is the IP address.

The IP address is string of characters and numbers which help identify a device, locate the device on the network and route the internet traffic.

And hence, “*Things refers to any physical objects with a device that has its own IP address and can connect to a network also send/receive data via a network.*”

Things can be us – humans, animals, buildings, energy stations, smartphones, tablets, bicycle, sensors, cameras, vehicles, health monitoring devices etc.

 **illustration of ‘things’**

Merging Internet and Things – making them work hand in hand, we land up to a powerful technology The **Internet of Things (IoT).**

Today we have many other devices apart from smart phones and computers which have the capability to connect and communicate through internet like garage door opener, internet connected sprinklers, water quality sensors, ATM machines, Electricity and utility meters, cars and other vehicles, Medical and Health monitoring device and many more.

All the interconnection of these uniquely identifiable computing devices within the existing internet infrastructure can be termed as Internet of Things or in short IoT.

Hence, **IoT can be defined as** :

*A network of physical objects or ‘things’ that can interact with each other to share information and take action.*

OR

*The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure.*

**SECTION 2**

Actors – identify the actors

Frameworks – identify existing frameworks including cybersecurity tap-in resources and make suggestions of how to interoperate. Suggest new approaches for IOT

Jurisdictions – some jurisdictions are safer that others for data privacy and security

Policies that have an impact on security and privacy in IOT – identify policies or non-policies that allow the flourishing of the IOT technology. Identify deterrents.

**KEY FINDINGS**

**FIGURE 2.1**

**SECTION 3**

Minimizing and controlling the attack surface – This subparagraph can encompass IOT system and network segmentation, segmentation of functions, separation of information; identify aspects of authentication, encryption, communication and interoperability.

**KEY FINDINGS** (Lucian)

# III. Minimizing and controlling the attack surface

## *A.* *Attack surface in the context of IOT*

Within the context of cyber systems the attack surface represents the services and areas of potential exposure to breaching attacks or vulnerability exploit. By minimizing or controlling the areas via which known or unknown vulnerabilities can be exploited, the risk of penetrating the system decreases and system security increases.

An area of system exposure is a potential exploit link or attack vector which might entice an attacker to pursue breaching the system or interfere with its functionality. By successfully pursuing an exploit link the attacker might have access to other known or unknown system vulnerabilities. In general, the severity of a vulnerability cannot be fully assessed without being evaluated in the context of the attack vectors in which can be exploited.

In particular, IOT systems include sensing components which might represent an extension to the attack surface. The meddling with their sensing capabilities may cause damage to system safety. Despite the apparent potential increase of attack surface, the IOT sensing systems poses the significant advantage of being able to use more defense vectors and fusioned data for a more effective defense against any type of attack. Hence is of significant importance that for critical sensing systems, redundancy, data fusion and semantic decision making be in place in order to mitigate vulnerabilities and improve the safety and security of the system. The exploit links on these components might include interfering with the sensing components e.g. pinpoint a laser to a camera, RFID jamming, localized temperature change etc. however, those require in general a more localized presence in the area of attack; therefore, a more localized attack on the sensing capabilities might yield more information about the attacker than a remote cyber breach.

IOT systems are cyber systems and hence operated by software modules which run most hardware components and are present at all levels of the architectural stack. The attack vectors on those software modules are multiple and include network, human, hardware interface like USB, hard drive etc. There are many available tools either freeware or paid on the web that allow pursuing various exploit links for various systems and components. There are also less known or classified tools that can exploit very specific particularities and vulnerabilities of components or systems.

In order to improve system security and minimize risk, the attack vectors should be assessed and the vulnerabilities reduced. While a complex system might include many known or unknown bugs and vulnerabilities those may not pose an immediate security risk if there is no exploit link available. While no system is immune to breaches and vulnerability exploit, the risk can be managed by implementing a risk strategy and framework which can monitor those aspects in real time, assign the color of severity to the security problem at hand(see NIST) and deal with it accordingly.

According with *IBM Security Services 2014 Cyber Security Intelligence Index* is that “over 95 percent of all incidents investigated recognize “human error” as a contributing factor. The most commonly recorded form of human errors include system misconfiguration, poor patch management, use of default user names and passwords or easy-to-guess passwords, lost laptops or mobile devices, and disclosure of regulated information via use of an incorrect email address. The most prevalent contributing human error? “Double clicking” on an infected attachment or unsafe URL.”

As such the “human error” vector is of significance when dealing with IOT systems security and privacy.

One problem that arises with IOT components is that it may be hard to patch once in the field e.g. a firmware running a security camera etc. While a system for detecting, flagging and updating the obsolete firmware is advisable, it might not be always possible or available and hence, taken proper actions to limit exposure to attacks becomes more important.

The following sections present practices of importance which should be taken in order to minimize the attack surface on IOT systems.

## *B.* *Network segmentation*

In a general way, the segmentation is the process in which a larger system is segmented in multiple smaller subsystems or layers. In the context of security the idea is that by segmentation a system should become more resilient as a vulnerability exploited on one sub-segments might be contained and not spread or affect the whole system. The same logic applies to the privacy of the system wherein the privacy of segmented data is higher than if the same data reside in a non-segmented fashion. A layered approach adds the benefit of using very simple and limited services at the external layer which represent a reduced external attack surface while more complex services are hidden within the internal layers.

By definition IOT systems include a networking component which allow data to be transferred between modules. The networking can be used to communicate with sensors via wired or wireless connections, for cloud connection or to transfer information between IOT nodes.

It has been proven that IOT systems should not rely solely on network security to assume that they operate in a safe environment. While an intruder gains access to the network through one of the attack vectors mentioned above so it does to any vulnerable or insecure IOT devices or systems. Examples include unsecured home networked monitoring cameras, unsecured or vulnerable control systems, point of sale, ATMs etc. Using authentication and encryption for smart IOT devices is therefore important. Also, having a smart firewall to restrict and control the network traffic to and from the outside world is also important for these devices and fits in overall concept of network segmentation. As a general security rule which applies to IOT is that any IOT device should expose to the outside world only a very limited number of services which can be used through a secure and authenticated connection like TLS, VPN etc. while all the other non-relevant services (e.g. platform OS services) should be disabled or restricted.

IOT low end devices have in general limited computing capabilities due to the fact that they are either very low power or low cost. Hence, those devices cannot use sophisticated encryption and authentication algorithms and therefore might be more vulnerable to impersonation or man in the middle attacks. In general, those low end devices use an access point or gateway to connect to the network backbone isolating the segment of low end devices - e.g. RFID gateways, PLC controllers etc. Therefore, the access point or gateway security should be strong and act as a bastion between the network backbone and the low end sensor segment. The security of low end devices networks should also rely on semantic technologies which use semantic intelligence and data fusion to detect security breaches. These includes detecting sensor de-doubling, location anomalies, anomalous values or any other fusion elements. One critical advantage of low end sensors is that they can be replaced more often, sometimes as often as a visit to a store or the airport and therefore, in the unlikely case of a sensor compromise, there is no long term damage to security or privacy - e.g. a spoofed bank card can do so much damage as opposed to the more critical breach of the ATM machine which acts as a gateway or access point for the ATM card.

In conclusion a layered network architecture with more than one line of defense like firewalls, IOT access points etc. provide more resiliency and security than a flat network and non layered configuration .

## *C.* *Function segmentation*

As expressed before, the human error vector accumulates for most of successful link exploits. By separating the human factor error in IOT systems so the attack surface is significantly reduced. It is hence desirable to separate the input functions that are influenced or operable by human factors from the functions that effectively operate the IOT system.

In general, the human factor intervenes in configuring IOT systems and devices; secure configuration is key in preserving the system security and privacy; at a minimum each system should require authentication before any configuration changes and should enforce changes to any default credentials.

Another segmentation practice, is that the user interface engine e.g. web server and database should not run on the same device or virtual machine that provide sensor control and management. This is advisable in order to eliminate attacks through malicious data entries in the user interface. Instead the configuration should be transferred to IOT devices and controllers through a secure and authenticated transaction from the configuration element to the device itself.

For critical systems as medical devices for example other precautions can be taken as avoiding over the air configurations or updates or ensuring that those updates are done in a predetermined schedule in a controlled environment.

## *D.* *Data segmentation*

The privacy is an important aspect of IOT systems wherein there is a logical separation between sensor or IOT data and personally identifiable data. While the first category is circulated and transmitted more often in IOT systems it is less prone to be used to leak sensitive information if a set of best practices are implemented into the system.

In general, object identification data or sensor data e.g. from RFID tags, credit cards, license plates, bar codes, wearables, appliances etc. doesn’t contain any personally identifiable information; it’s just a way of signaling the presence of an entity or transmitting a set of observations to the IOT managing element.

The IOT system is the one that may link the identification or sensor data to personally identifiable information in order to perform its tasks. Therefore, the link between the identification or sensor data and personally identifiable information should be clearly defined and secured. There shouldn’t be any option that allows an attacker to use solely sensor or identification data in order to gain access to personally identifiable information.

Any system using identification or sensor data for authentication on gaining access to sensitive information should use at least two-way identification or authentication beside that data e.g. RFID + password, biometric + password etc.

One important aspect of the new breath of IOT systems is that they store personally identifiable information on the private or public cloud and less on the IOT devices or gateways. So, in the unlikely event that an attacker gains access to the IOT device or gateway, the personally identifiable information remains safe in the cloud. As the gateway devices use strong authentication and secure cloud services, is then very difficult for an attacker to gain access to the information through this kind of link exploit. Exceptions from this case may consist of smart phones, tablets and other more general computing devices that may act as a gateway for sensor devices(e.g. wearables) while storing or streaming sensor data and unrelated personal information on the smart phone or computing device. Therefore, IOT specialized gateways and devices may provide better security and privacy than a more general unsegmented computing platform. It is also of importance that the IOT system use a reliable and safe cloud environment in order to store private data.

**FIGURE 3.1**

**SECTION 4**

Detection – While IOT systems can be based on a deep stack and architecture they also have additional detection capabilities that can be beneficial for either a self contained deployment or integrated as part of a collaborative framework.

Resiliency – redundancy, failover, backup

**KEY FINDINGS**

**FIGURE 4.1**

**SECTION 5**

Recovery – Identify self healing and recovery options

Controlled information sharing – how to control the sharing of information; based on settings preferences etc. Foil pattern detection.

**KEY FINDINGS**

**FIGURE 5.1**

**SECTION 6**

**KEY FINDINGS**

**FIGURE 6.1**

**SECTION 7**

**KEY FINDINGS**

**FIGURE 7.1**

**SECTION 8**

**KEY FINDINGS**

**FIGURE 8.1**

**CONCLUSION**

[By this point you’ve told them what you’re going to tell them in the Abstract and Introduction; you’ve told them in the Problem Statement and Solution; and now you need to tell them what you told them. The Conclusion provides the opportunity to:

* Summarize the objectives of the white paper.
* Review the problem statement(s).
* Highlight the solutions and their value for your audience. Be clear regarding how these solutions address the problem statement(s).
* Finish with a strong statement. (e.g., a vision of future solutions; how your audience can develop new solutions on their own; where your audience can go for addition information and/or resources)]

**ADDITIONAL RESOURCES**

[Provide a list of available resources for your audience. This list may include resources that you have sourced throughout the white paper.]

**FOR MORE INFORMATION**

© 2016 IEEE Internet Initiative, ETAP Internet Technology Policy Community. All Rights Reserved.

For more information, please contact jared.m.bielby@ieee.org

**Additional Tips for Creating White Papers**

* **Formatting & Coloring:** Create a consistent color scheme based on the color of your logo. Use the most dominant color for your section headers. Use a softer version or a shade of gray as the subhead color. Use these same colors throughout all visual elements of your white paper (e.g. charts, graphs or figures).
* **Grammar & Editing:** Ensure that your white paper has been run through several editors for quality control. Once someone downloads your white paper, it is in his or her possession and you are unable to make further edits. Correct spelling and grammar will elevate your message and back up the credibility of your company.
* **Promoting Other Assets:** Use the white paper to link to several of your other content marketing assets. These could be other white papers, eBooks or blog posts. Do ensure that these assets are highly relevant to the topic at hand and focused on answers the audience may need, rather than pushing your company’s product.
* **Curating Expert Content:** Substantiate your message by including content from experts on the topic; either directly getting quotes from these experts or [curating their content](http://www.curata.com/blog/the-definitive-guide-to-content-curation/).Be sure to follow ethical best practices for curating content, such as linking back to the original source, only taking a small portion of the content and adding your own annotation. For a guide to ethical curation, download our complete eBook on the topic: [Content Marketing Done Right](http://www.curata.com/resources/ebooks/content-marketing-done-right)

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Supplementary Materials**

**A. Project Scope**

**1.0 Proposed Action**: "Development of an End-to-end Security and Privacy by Design for IoT":

Create a layered End-to-end Security and Privacy by Design model towards guiding policy.

**1.1 Action Mandate:** Determine how to collaboratively navigate the “cyber‐ecosystem” – the combined domains of Internet, people, processes and technology – towards designing End-to-end Security and Privacy.

**1.2 Goal:** Create a set of well investigated guidelines and best practices so well investigate and thought out that other use it to for their clarifications, laws, and product ratings

**1.3 Timeline for completed deliverable:** 5/hrs. week per participant, first draft due September 15th for a completion date / Final draft of October 15th, 2016

**1.4 Publication options**

IEEE Publication Recommender: <http://publication-recommender.ieee.org/home>

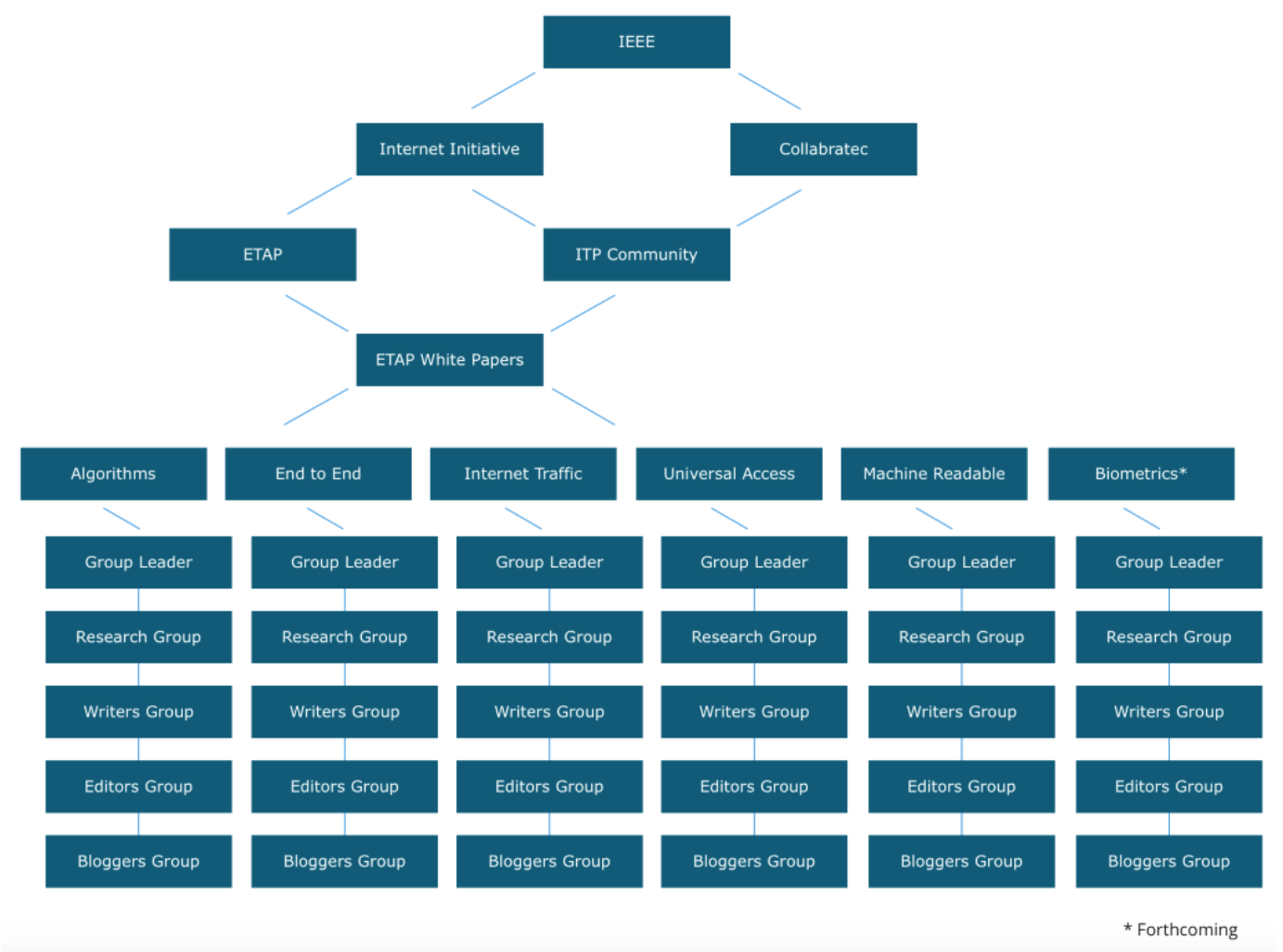
1) **IEEE Archival Journals:** This is our traditional venue for print publications and it could work well for certain papers. Of particular interest would be some of the Open-Access journals so that our readership can reach beyond just those with full access to XPLORE.

2) **Conferences:** For most of our papers there will be several related IEEE conferences. Chris J. can help do outreach to conference sponsors to help facilitate sessions, plenaries, workshops related to papers.

3) **IEEE Internet Initiative (3I) Events:** similar to conferences, we can help organize sessions / speaking roles for White Papers teams and authors at 3I events.

4) **Webinars:** Once the paper is completed, Chris J. can help produce Webinars with paper team members to promote the papers to a wide audience of IEEE members and affiliated non-members.

**1.5 Project Map:**



**B. Contributor Teams**

**2.1 Interest Groups:**

Please enter your Interest Group in interest sub-group column.

Researcher = RS, Writer =W, Editor = E, Reviewer/Advisor = RA, Blogger/Summaries = BS, Group Leader = GL

Please enter your local time zone according to the Coordinated Universal Time (UTC) in Local time zone column such as:

EST Eastern standard time = UTC – 5, CST Central standard time = UTC – 6, MST Mountain standard time = UTC – 7

Use [this link](http://www.timeanddate.com/time/zones/) to find your local time zone in UTC

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| First & Last Name | Email | Affiliation | Interest sub-group | Time Zone |
| **Mohammed Aledhari** | [mohammed.a.aledhari@gmail.com](mailto:mohammed.a.aledhari@gmail.com) | Doctoral Associate at Center for High Performance Computing and Big Data, Western Michigan University | RS & RA | UTC-5 |
| **Sukanya Mandal** | sukanyamandal06@gmail.com | Software Engg. - Insights and Data | RS, W and BS | UTC+05:30 |
| **Carl Wack** | Jybird47@yahoo.com | ANSI/BoD | RS and W | UTC-5 |
| **George Corser** | gpcorser@svsu.edu | Saginaw Valley State University | GL, W, RA | UTC-5 |
| **Kewei Sha** | Comersha@gmail.com | University of Houston - Clear Lake | RS & RA | UTC-6 |
| **Anna Slomovic** | Anna.slomovic@gmail.com | Independent consultant  Former chief privacy officer | RA | UTC-4 (EDT) or UTC-5 (EST) |
| **Binit Sharma** | binit.sharma101@gmail.com | Freelance Design Engineer, Nepal Innovation Center | RS, RA | UTC +5.45 |
| **Nagender Aneja** | naneja@gmail.com | Universiti Brunei Darussalam | RS and W | UTC+8.00 |
| **Lucian Cristache** | Lucianc@ieee.org | Lucomm Technologies | RS,W,RA | UTC-7 |
| **David Richardson** | DSRich01a@GMail.com | Industrial Controls Engineer | E | UTC-4 (EDT) or UTC-5 (EST) |
| **Rajesh Nighot** | Rajesh.nighot@nebulian.com | Independent Consultant | RS,W,RA | UTC+05:30 |
| **Sandhya Aneja** | Sandhya.aneja@ubd.edu.bn | Universiti Brunei Darussalam | RS and W | UTC+8.00 |
| Ali Kashif Bashir | Ali-b@ist.osaka-u.ac.jp | Research Fellow/Lecturer, Osaka University, Japan. | E, RA | UTC+9 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**2.2 Task Flow:**

The above task-flows follow as such:

1.) The *Bloggers Group* task includes the writing and preparation of summaries and short articles for publication with the Institute and the Internet Initiative Newsletter. They will proceed on the advice and lead of the Editors Group.

2.) The *Editors Group* will take action upon the completion of the tasks of the Writers Group and the Bloggers Group and will edit for publication according to established publication standards.

3.) The *Writers Group* will be advised by the Research Group and will write according to the established research and findings of the Research Group.

4.) The *Research Group* task will include narrowing the scope of issues and aspects that fall within the parameters of the established Goals of the white paper and will provide curated and pointed material for the Writers Group to work with.

5.) The Research Group will proceed on the advice of the *Group Leader,* who will determine direction and scope parameters. The Group Leader will have the final say in all decisions about the white paper.

**2.3 Contributor Teams:**

**Contributor Team One: Research Group (meeting to be determined)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **Affiliation** | Preferred time | Preferred day | **Tasks** |
| Mohammed Aledhari | [mohammed.a.aledhari@gmail.com](mailto:mohammed.a.aledhari@gmail.com) | Doctoral Associate at Center for High Performance Computing and Big Data, Western Michigan University | 6 - 9 P.M.  12 - 5 P.M.  EST/UTC-5 | Mon. - Fri.  Sat. - Sun. |  |
| Sukanya Mandal | sukanyamandal06@gmail.com | Software Engg., Insights and Data | 09:00 P.M - 00:00 A.M IST  06:00 P.M - 00:00 P.M | Mon-Fri  Sat-Sun |  |
| Carl Wack |  |  |  |  |  |
| Kewei Sha |  |  |  |  |  |
| Binit Sharma |  |  |  |  |  |
| Nagender Aneja | naneja@gmail.com | Universiti Brunei Darussalam | 1pm-11pm (Loal)  7pm-11pm(Loal)  UTC+8 | Fri& Sun  Mon-thu,Sat |  |
| Lucian Cristache |  |  |  |  |  |
| Rajesh Nighot |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Contributor Team Two: Writers Group (meeting to be determined)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **Affiliation** | Preferred time | Preferred day | **Tasks** |
| Sukanya Mandal | sukanyamandal06@gmail.com | Software Engg., Insights and Data | 09:00 P.M - 00:00 A.M IST  06:00 P.M - 00:00 P.M | Mon-Fri  Sat-Sun |  |
| Carl Wack |  |  |  |  |  |
| George Corser |  |  |  |  |  |
| Nagender Aneja | Naneja@gmail.com | Universiti Brunei Darussalam | 1pm-11pm (Loal)  7pm-11pm(Loal)  UTC+8 | Fri& Sun  Mon-thu,Sat |  |
| Lucian Cristache |  |  |  |  |  |
| Rajesh Nighot | Rajesh.nighot@nebulian.com | Independent Consultant, Gujarat, India | 8pm to 11pm  (local)  UTC+05:30 | M-F |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Contributor Team Three: Editors Group (meeting to be determined)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **Affiliation** | Preferred time | Preferred day | **Tasks** |
| Jared Bielby |  |  |  |  |  |
| David Richardson |  |  |  |  |  |
| Ali Kashif Bashir | Ali-b@ist.osaka-u.ac.jp | Research Fellow/Lecturer, Osaka University, Japan. | 9:00-22:00 (UTC+9/JST) | M~F |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Contributor Team Four: Bloggers Group (meeting to be determined)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **Affiliation** | Preferred time | Preferred day | **Tasks** |
| Jared Bielby |  |  |  |  |  |
| Martin |  |  |  |  |  |
| Sukanya Mandal | sukanyamandal06@gmail.com | Software Engg., Insights and Data | 09:00 P.M - 00:00 A.M IST  06:00 P.M - 00:00 P.M | Mon-Fri  Sat-Sun |  |
| Mohammed Aledhari | [mohammed.a.aledhari@gmail.com](mailto:mohammed.a.aledhari@gmail.com) | Doctoral Associate at Center for High Performance Computing and Big Data, Western Michigan University | 6 - 9 P.M.  12 - 5 P.M.  EST/UTC-5 | Mon. - Fri.  Sat. - Sun. |  |
| George |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

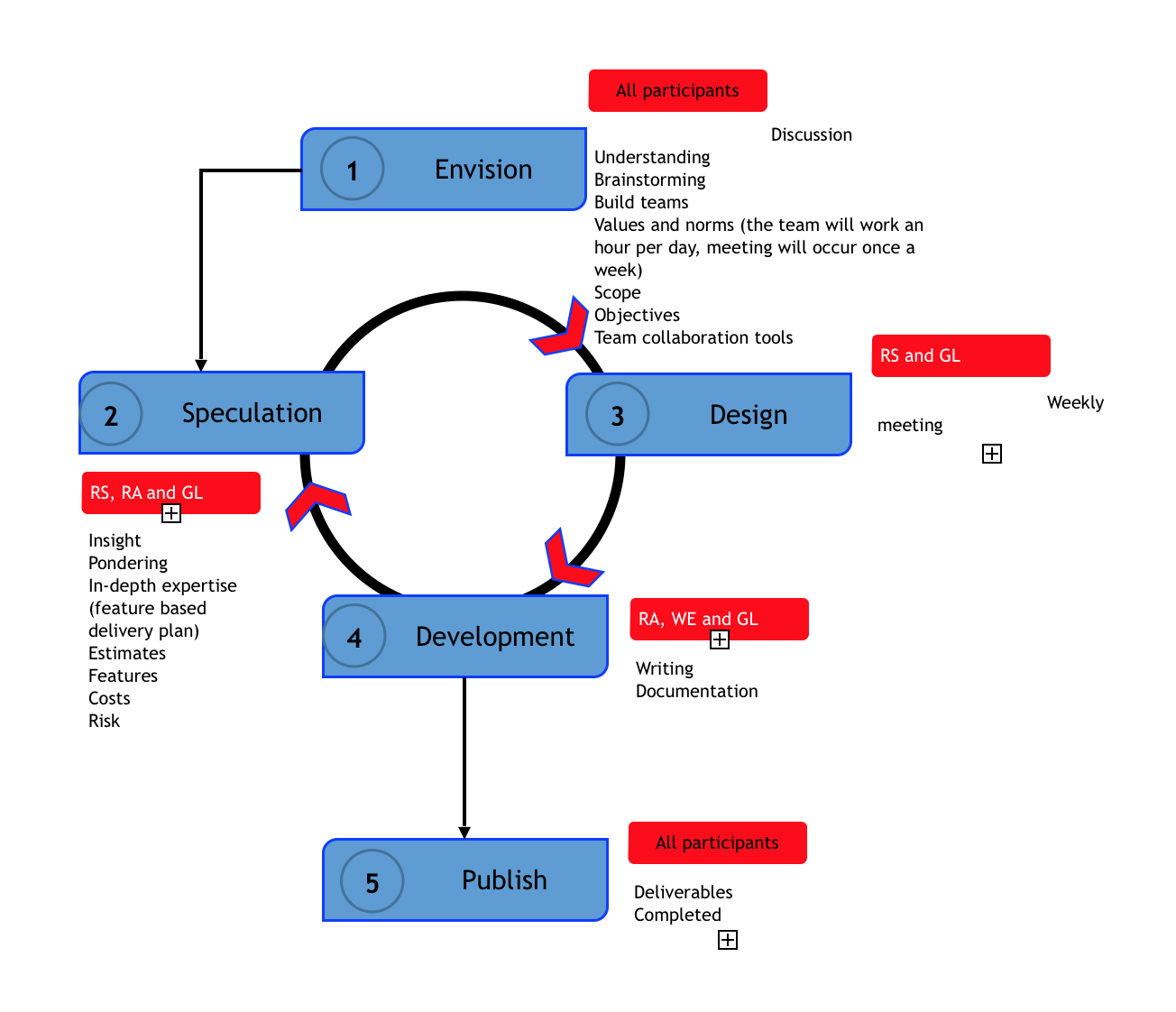
**Contributor Team Five: Advisors Group (meeting to be determined)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Name** | **Email** | **Affiliation** | Preferred time | Preferred day | **Tasks** |
| Mohammed Aledhari | [mohammed.a.aledhari@gmail.com](mailto:mohammed.a.aledhari@gmail.com) | Doctoral Associate at Center for High Performance Computing and Big Data, Western Michigan University | 6 - 9 P.M.  12 - 5 P.M.  EST/UTC-5 | Mon. - Fri.  Sat. - Sun. |  |
| George Corser |  |  |  |  |  |
| Kewei Sha |  |  |  |  |  |
| Anna Slomovic |  |  |  |  |  |
| Binit Sharma |  |  |  |  |  |
| Lucian Cristache |  |  |  |  |  |
| Rajesh Nighot | Rajesh.nighot@nebulian.com | Independent Consultant, Gujarat, India | 8pm to 11pm  (local)  UTC+05:30 | M-F |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**2.4 Contributor Interests & Expertise:**

|  |  |  |
| --- | --- | --- |
| **Contributor** | **Interests** | **Expertise:** |
| **Sandhya Aneja** |  | Wireless Networks Security, Data Security |
| **Mohammed Aledhari** |  | Networks, IoT big data, Microcontrollers and Machine/Deep Learning |
| **Ali Kashif Bashir** | Review/editorial services. | Computer networks (Wireless and wired). SDN/NFV, IoT, etc. |
| **Rajesh Nighot** | Power systems, cyber security, wireless and FO communication, Public Policy, IoT | Networks, power system software, Public Policy for Electricity Sector, Management of Large Infrastructure Projects, Railway Electrification, FO communication, Algorithms, Automation and Regulation |
| **Nagender Aneja** | Network Security, Networking Protocols, Ad-hoc Networks,Social Networking, Automation, Smart Homes and IOT, Patents | M.Engg Computer Tech. and App.  PhDComputerEngg(Pursuing)  Experience of handlingSoftwarebased Patents from Microsoft Corp. |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**C. Project Management**



**D. Background - ETAP and conversations with DHS**:

Three activities that protect government agencies:

1. The Einstein Program is an intrusion detection program for monitoring network gateways used by government agencies.
2. The Trusted Internet Connections Initiative limits the number of Internet connections used by the federal government and filters related traffic.
3. The Continuous Diagnostics and Mitigation Program provides cybersecurity tools for each agency’s environment to assess assets and vulnerabilities.

Challenges in meeting cybersecurity needs:

1. A shortage of skilled workforce to perform cybersecurity, which is getting worse.
2. No cybersecurity data standards, which cause issues for interoperability, reduces analyst productivity, and causes delays.
3. The effectiveness of detection and mitigation efforts is not optimal.

The Internet of Things will present an infinitely more complex situation for security and privacy. Current management of networks is poor at best even with an entire organization set up to do security for managed networks. How much more difficult will a managed network of Internet of Things look?

According to DHS, there are three components of the cyber‐ecosystem that need to be addressed:

1. One is the enterprise architecture, whether that’s enterprise IT, the cloud, or process control systems. “For instance, [DHS worries] about process control systems, because we protect critical infrastructure,” he said. “That cyber‐ecosystem will also need tools and capabilities” to sense attacks, determine a course of action and take action, he suggested. Those tools and capabilities probably will need to be automated, for speed. This area remains in its infancy, however, and some warn of unintended consequences.
2. The second component is the concept of a “cyber weather map,” which gathers cyber incident and reputational information, performs analytics and outputs the results via visualization tools.
3. The third component is an information infrastructure that can share information in “cyber‐relevant time,” driven by automation.

A 'cyber weather map' would pro-actively identify security risks via the Einstein program. This is a valuable place to look regarding proactive cybersecurity, though it is not without its controversy. Version 3.0 of Einstein, which will monitor government computer traffic on private sector sites, sits uneasy in light of the history of the NSA's warrantless wiretapping scandal made famous by Snowden.

Department of Homeland Security officials have expressed uncertainty about whether private data can be shielded from unauthorized scrutiny in such a scenario and the belief prevails that Einstein 3 is set to interfere with citizen privacy, and could be abused by both official (government) and unofficial (terrorists/hackers) players (Jared Bielby). If we are looking to choose between security and privacy, we will get neither.

The key to using such a program would be twofold, first a priority put in place that secures the data about the data (metadata) from further abuse, and two, an assurance of the maintenance of individual privacy through the use of efficient Big Data best practices. Einstein 2 (and 3) is certainly a place to start.

Fonash's map also projected the Trusted Internet Connections Initiative, which has set up 6 milestones towards security success, by, namely, reducing external access points towards an optimization based on simplifying the guard. The type of direction security needs to take is to look to simplify and reduce data flows rather than adding extra complexity that in tern can be hacked.

One of Fonash's main points, expressed at both the San Jose ETAP as well as the recent ETAP meeting in DC, is that we are setting ourselves up for failure by complicating the technology security situation. For every security-measure implemented by the "good" guys, we are only inviting an equal and opposite counter-measure by the "bad guys".

We are incapable, as-is, in securing our data and privacy, even with a department dedicated solely to the purpose, never mind the advent of IoT (Peter Fonash).

The last piece of Fonash's map deals with the Continuous Diagnostics and Mitigation Program, which advocate an increase in sensors to detect threats. The advantage to this method is in an optimization of security that detects security flaws but doesn't necessarily increase the risk of hacking so long as the sensor array is minimalized to detection functions only.

Technology needs of the cybersecurity challenge for critical infrastructure:

1. *Interoperability*: a need for interoperability of tools that overcomes the limitations of individual tools, existing in a shareable format where everyone understands them.
2. *Automation*: once interoperability is optimized, the move can be made towards automation.
3. *Authentication*: knowledge of the source of shared information [and validitation of its integrity – Nicolaides]
4. *Information Sharing*: with interoperability, automation and trust, information sharing will follow, where knowledge can be garnered through shared learning via each other’s mistakes, experiences and practices (Fonash).

All of these practices and processes should fit within a risk management framework for the full cybersecurity lifecycle (identify, protect, detect, respond and recover), keeping in mind that adversary agents will also continue to improve (Fonash).

**Increasing incentive towards Internet Development:**

Profit, cost, and features such as convenience are currently higher priorities in Internet development than security and privacy protection. What can be done to provide incentives towards security and privacy as priorities? (Alan Chachich)

*Proposal from the Washington DC ETAP:* create a multi-dimensional framework picture to visualize the problem being confronted. How can IEEE influence progress--where are the "hot spots" where IEEE can make a difference to increase security and privacy? There are two areas where IEEE might exercise influence: design and policy.

Rather than imposing laws, economic incentives are a far more efficient way to reach all stakeholders and are ultimately more useful in achieving desired results.

**The IEEE Center for Secure Design** advocates a 10-point process for avoiding the Top 10 Software Security Design Flaws, which includes the following:

1. Earn or Give, but Never Assume,
2. Trust Use an Authentication Mechanism that Cannot be Bypassed or Tampered With
3. Authorize after You Authenticate
4. Strictly Separate Data and Control Instructions, and Never Process Control Instructions Received from Untrusted Sources
5. Define an Approach that Ensures all Data are Explicitly Validated
6. Use Cryptography Correctly
7. Identify Sensitive Data and How They Should Be Handled
8. Always Consider the Users
9. Understand How Integrating External Components Changes Your Attack Surface
10. Be Flexible When Considering Future Changes to Objects and Actors

The IEEE Computer Society’s Center for Secure Design (CSD) mission statement aligns with the goals of the ETAP events, where the issues involved in technology and policy go hand-in-hand with recognizing software system designs that are likely vulnerable to compromise and preemptively designing and building software systems with strong, identifiable security properties to avoid flaws from the outset.

**E. Framework Guidelines:**

1. The framework for the below collaborative research and writing project will be determined by industry experts where participation for the project is exacted on a voluntary basis.
2. Initial leadership for the project is to be determined by members of the Internet Initiative’s organizing committee and a hierarchy of leadership will be established for the project by the project lead.
3. The project is to be headed by one individual chosen from among industry experts, known as the project lead. The lead will determine the direction and output of the project based on the advice of other participating industry experts or will delegate leadership accordingly.
4. The project lead will have final say on team development, project direction and will arbitrate disputes for the purposes of maintaining direction and focus.
5. The team lead will determine the direction of the project. An initial framework outlining the direction of the project must answer the following questions:
   1. **Will the project be towards a written whitepaper or the development of an IEEE standard, or both?**
   2. **Will the whitepaper/deliverable be neutrally descriptive in nature, or advocate a specific position?**
   3. **Has there been previous efforts and research in this space? What will this project offer that hasn’t already been done?**
   4. **What is the timeframe for the completion of the deliverable?**
   5. **How many hours will the participants volunteer weekly to the completion of the whitepaper?**
6. While the project is voluntary, the Internet Initiative asks that participants initially determine their commitment level to the project and respect their commitment towards the completion of the project.

The above framework for collaboration on the whitepaper is based on previous ETAP conversations, follow-up email conversations and individual expertise.

**F. White papers for Review**

1. Stankovic, J. A. (2014). Research directions for the internet of things. IEEE Internet of Things Journal, 1(1), 3-9. <https://www.intercom.virginia.edu/~stankovic/psfiles/IOT.pdf>. This paper discusses ever-more-overlapping research areas: " Internet of Things (IoT), Mobile Computing, (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and most recently, Cyber Physical Systems (CPS)."
2. Chess, B., & Arkin, B. (2011). Software security in practice. IEEE Security & Privacy, 9(2), 89-92. <http://www.ecs.csun.edu/~rlingard/COMP680/SecurityInPractice.pdf>. See also <http://csis.svsu.edu/~gpcorser/cis355/gpcorser/zip/BSIMM6.pdf>
3. Fonash, P., & Schneck, P. (2015). Cybersecurity: From months to milliseconds. *Computer*, *48*(1), 42-50. <http://csis.svsu.edu/~gpcorser/cis355/gpcorser/zip/2015-fonash.pdf>
4. Cyber Physical Systems Public Working Group (2016): Framework for CPS. <https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf>
5. IEEE Internet of Things Group (2015): Toward a definition for the IOT. <http://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>
6. NIST (2014): Framework for improving Critical Infrastructure Cybersecurity <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>
7. A. Al-Fuqaha, M. Guizani, M. Mohammadi, **Mohammed Aledhari** and M. Ayyash, "**Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications**," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, Fourth quarter 2015.
8. J. Granjal, E. Monteiro and J. Sá Silva, "**Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues**," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 3, pp. 1294-1312, Third quarter 2015.
9. M. A. Crossman and Hong Liu, "**Study of authentication with IoT testbed**," *Technologies for Homeland Security (HST), 2015 IEEE International Symposium on*, Waltham, MA, 2015, pp. 1-7
10. Auto-isac, cybersecurity best practices document: Automotive Cybersecurity Best Practices, Executive Summary, July 21: 2016 <http://www.automotiveisac.com/best-practices/>
11. Jones, Meg Leta. ["Privacy Without Screens & the Internet of Other People's Things."](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2614066) <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2614066> *Idaho L. Rev.* 51 (2014): 639.
12. Strengthening the Cyber Ecosystem, Dr. Peter Fonash, Chief Technology Officer (CTO), Office of Cybersecurity and Communications (CS&C), 2014.
13. Stankovic, John A. "Research directions for the internet of things." *IEEE Internet of Things Journal* 1.1 (2014): 3-9.

**G. Narrowing the Scope:**

The below chart is a way of voting out the issues we feel are too broad while narrowing down what we think the focus of the paper should be. Feel free to add aspects to be addressed and to vote on those that others present. Place an X to vote against, place an Y (yes) to vote for.

Be sure to reference your below aspects/concerns using the whitepapers and research materials provided above and to add any new whitepaper bibliographic references to the "Whitepapers for Review" section above.

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Aspect/Concern | Vote Out | Include |
| *Example: Bob* | *We should do it all!* | X,X,X,X,X,X, | Y,Y |
| Jared Bielby | Question: Should this paper be a standard? | X,X,X |  |
| Jared Bielby | Question: Should this paper be a descriptive whitepaper that makes suggestions for a standard? |  | Y,Y,Y |
| Glenn Fink | Task: Describe the security and privacy risks associated with IoT and set recommendations for mitigating them. |  | Y,Y,Y |
| George Corser | Task: Perform a literature review of existing "E2E security and privacy by design for IoT" (if any) list open research areas. |  | Y,Y, Y,Y |
| Tariq Saraj | Task: Start by determining what the purpose and targeted audience is for this paper. |  | Y,Y, Y,Y |
| Lucian Cristache | Task: Identify cybersecurity initiatives and frameworks and how those tie in IOT |  | Y,Y,Y |
| Lucian Cristache | Task: Identify actors, frameworks and policies that have an impact on security and privacy in IOT. Include interoperability frameworks and technologies. |  | Y,Y,Y |
| Mohammed Aledhari | Task: lacking of protocol standardizations for the IoT considered a big challenge because most of these protocols were developed by specific vendors, and these vendors typically promote their own protocol choices, don’t clearly define their assumptions, and ignore the other alternatives. so focusing on standardization will help in creating a solid secure model for IoT. |  | Y,Y,Y |
| Mohammed Aledhari | Task: Identify some IoT E2E security solutions by testifying when and where can be used two or multi-factor authentications models. |  | Y,Y,Y |
| Jared Bielby | Explore and outline concerns of fragmentation and how that may or may not affect end-to-end security. |  | Y,Y,Y |
| Kewei Sha | Tight coupling between physical systems and cyber systems. |  | Y |
| Kewei Sha | Low capable things that cannot support heavy computation needed in the traditional security solutions. | ? | Y |
| Kewei Sha | Security in the newly developed protocols used in IoT. |  | Y |
| Sukanya Mandal | IoT security in general or security specific to different IoT arenas |  |  |
| Sukanya Mandal | IoT Protocols Standardization |  |  |
| Sukanya Mandal | IoT Security Standards |  |  |
| Sukanya Mandal | Data Security in IoT |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**H. Narrowing the Scope 2:**

The below chart is a way of voting out the issues we feel are too broad while narrowing down what we think the focus of the paper should be. Feel free to add aspects to be addressed and to vote on those that others present under your initials.

Names and Initials:

1. George Corser=======G.C.
2. Jared Bielby========J.B.
3. Mohammed Aledhari==M.A.
4. Chris Hrivnak=======C.H.
5. Lucian Cristache=====L.C.
6. Dena Hoffman ======D.H.

Please add **1** to vote for, leave a blank for none:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| No. | Challenge/Issue | G.C. | J.B. | M.A. | C.H. | L.C. | D.H. |
| 1 | Topic of this working group paper "Create a set of guidelines and best practices so well investigated and thought out that others use it for their clarifications, laws, and product ratings" |  | 1 | 1 |  |  |  |
| 2 | Definition 1 "A wired or wireless network of connected devices which are able to process data and communicate with each other with or without human involvement" |  |  |  |  |  |  |
| 3 | Definition 2 "Interconnection of uniquely identifiable with embedded computing within the internet infrastructure. Primarily physical things with actuators. [Chachich] Differentiate from web of things" |  |  |  |  |  |  |
| 4 | Definition 3 "We define Internet of Things (IoT) broadly, to include Mobile Computing (MC), Pervasive Computing (PC), Wireless Sensor Networks (WSN), and Cyber Physical Systems (CPS). IoT devices may or may not be accessible by Internet Protocol (IP). They may or may not have a human in the loop" |  |  |  |  |  |  |
| 5 | Definition 4 "A universal digital language or protocol to connect and exchange data and commands between anything (living and non-living things that have unique identifiers), anytime anywhere to improve the quality of life (QoL) and provide best services without requiring human interaction" |  | 1 | 1 |  |  |  |
| 6 | IoT System Model with Policy Maker Role  7 Layers |  |  |  |  |  |  |
| 7 | IoT System Model with Policy Maker Role  5 Layers |  |  |  |  |  |  |
| 8 | IoT System Model with Policy Maker Role  3 Layers |  |  | 1 |  |  |  |

**I. Concerns to be Tabled**

|  |  |  |
| --- | --- | --- |
| Participant | Concerns: | Recommendations: |
| Jared Bielby | I'm concerned that fragmentation of the Internet will hinder efforts for an effective and secure end-to-end IoT. | I recommend that... |
| Kishan Nagiredla |  |  |
| Alan Chachich |  |  |
| Chris Hrivnak |  |  |
| Anna Slomovic |  |  |
| Karin Hollerbach |  |  |
| Glenn Fink | My concern is that the purpose of this document is unclear and the audience is undefined. I recommend first adopting an organizing principle and refining the document toward the greatest need that we can likely effect. | I recommend using SRI's Need, Approach, Benefits, Competition (NABC) framework as follows:  NEED: IoT products and protocols are emerging ad hoc with little regard for standards and even less for security and privacy. Because many of these devices will be very personal in nature, they represent a privacy risk. Because they are decentralized, often unmanaged, and have connectivity to the Internet they represent a security risk.  APPROACH: What is needed from this group is a description of the security and privacy risks associated with IoT and a set of recommendations for mitigating those risks. The document should provide general guidance and a way to measure whether each recommendation is being followed. The document should form the basis for future standards and guidelines but should not prescribe any particular solutions (e.g., EINSTEIN). It should also take into account the decentralized nature of the IoT, the multiplicity of ownership, the sharing of risk, and the voluntary nature of compliance.  BENEFITS: The document will provide expert guidance for creation of standards, best practices, and laws for security and privacy in the IoT. Vendors with little experience in these areas will be able to learn from the lessons of others. Governments will be able to identify national risks and will gain an informed basis for making policies. Consumers will benefit from the possibility of informed consensus on security and privacy among IoT vendors and with governments.  COMPETITION: Alternative approaches we should not take include: (1) Creating a standard because too little is known about the specifics of these devices, networks, and uses. (2) Attempting to directly influence national policies because premature legislation can harm economic benefits of IoT. (3) Writing a simple description of the problems faced because this would only admire the problem and not provide actionable information.  Instead, we should create a document that proposes general security and privacy best practices as a basis for discussion with industry and a first step toward collaborative development of laws and policies. |
| Lucian Cristache | It is a known concept that the security of a system is as good as its weakest link. There are many connectivity technologies involved in IOT at various stack levels including physical security.  Activity monitoring by an eavesdropper. An entity can use various eavesdropping techniques(e.g. wireless activity monitoring) to infer system/user activity or behavior and even tamper with the data.  Legal framework | Provide a risk management framework/network.  Have live safety ratings.  Systems/sensors can use semantic meanings to detect and report intrusions/tampering.  System/sensor design should use a layered approach with at least two distinct lines of defense – firewall, gateway/sensor - on separate physical or virtual cores. User interfaces prone to common attacks should use a separate core.  Use all other best practices for each component.  Use data storage providers operating under safe environments and jurisdictions.  IOT systems should preserve separation between sensing data(which is potentially more vulnerable) and personally identifiable information.  IOT systems can use constant streams or random stream of data techniques to foil activity pattern detection.  Use semantic techniques to identify the eavesdropping or tampering attempt.  Use low cost sensors which are discarded, recycled or deactivated.  Some IOT systems can be categorized as critical infrastructure e.g. hospital, airport, nuclear plant, transportation network. Attempts to interfere with such systems should be treated as a very serious crime or even an act of terrorism.  Incorporate cyber threat exchange protocols into trade deals.  Promote and adapt the Budapest Convention on Cybercrime.  Each service provider should disclose the jurisdiction(s) under which operates; including the jurisdictions of any third party infrastructure providers it uses(e.g. cloud infrastructure providers). |
| Thomas Coughlin |  |  |
| George Corser | Concerns:  1. In IoT context, Security and Privacy are not defined clearly enough to be measured by a computer so neither technologists nor policy makers can quantify cost/benefit tradeoffs  2. Our goal is: "Create a layered End-to-end Security and Privacy by Design model towards guiding policy. " In other words we are looking for a method to help legislators identify holes in IoT security and/or privacy so they can make better laws or policies. Our mission is to suggest a model. Is there a template we can use to do our work?  3. We have not yet identified a survey paper that specifies the spectrum of issues for the IoT S&P problem. I hope it will not be necessary but it is possible that we might have to write one ourselves. | Recommendations:  1. Identify example metrics (ex:[Corser](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=7422060&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D7422060)), system model (ex:[Cisco](http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf)), threat model (ex:[Shokri](https://infoscience.epfl.ch/record/148708/files/LocationPrivacyFramework.pdf))  2. Organize our framework using [Zachman](https://en.wikipedia.org/wiki/Zachman_Framework) style, at least at the start. Explicitly identify legal issues (ex:[Katz](https://en.wikipedia.org/wiki/Katz_v._United_States) and US DOT), technological realities (security/privacy to a computer may not be the same as human intuition), operational cost/benefit (eg: would privacy impair safety)  3. Perform a literature review of existing "E2E security and privacy by design for IoT" (if any) list open research areas. I found [Weber](https://www.researchgate.net/profile/Rolf_Weber3/publication/222708179_Internet_of_Things_-_New_security_and_privacy_challenges/links/0c96053cab03fee371000000.pdf), a 2010 legal research paper, and another law paper on [FTC.gov](https://www.ftc.gov/sites/default/files/documents/public_comments/2013/07/00031-86244.pdf), but we really need a technology paper. There is a [conference](http://siot-workshop.org/) focusing on secure IoT, and 17 survey papers on IEEE Xplore. A very highly rated conference: [IEEE SP](http://www.ieee-security.org/TC/SP2016/), but no survey papers on IoT from what I could find. |
| Premanand Narasimhan |  |  |
| Bernard Cohen |  |  |
| Sukanya Mandal |  |  |
| Kenneth Erney |  |  |
| Edward Marsh | 1. Is there a way to create a standard that applications follow to provide manufacturers / designers a template or requirements to meet in order to have internet security? | If there the goal is to make requirements, or standards, then this may be a mechanism that will provide for better internet security. Suggested practice is not something that can be licensed or enforced. |
| Gopalakrishnan Renganathan  Assistant Professor,  Instrumentation & control Engg,  India. | As discussed in DHS, the IoT plays important role in documenting the end to end security tools. So the main concern here, is to enhance the IoT tools and make it user friendly & also secure. | I recommend the standards of IoT to be improved there by improving the internet tools and other links more secure and safe for the users. |
| Mohammed Aledhari | I think there are many issues need to be discussed (IoT security, privacy, Trust and Authentication). All of them affect End-to-End IoT security | I recommend that... |
| Tariq Saraj | I think we should start by determining what the purpose and targeted audience is for this paper.  Specially, I'm concerned of what the impact of end-end will be for the Asia Pacific Region.  Will this project also consider Recursive Internet Architecture (RINA)? EU is now heading towards RINA so we may lose huge audience in the near future regarding this contribution. |  |
| Steven Collier |  |  |
| Oscar Gunnerlind |  |  |
| Roman Zillek |  |  |
| Ali Kashif Bashir | I am concerned and interested in following: 1- Standard security features. 2- varying security requirements in different IoT applications, 2- Privacy concerns in accordance to 1 & 2 and the otherwise. | The topic can be divided into sub-topics, e.g., as per concerns and we can form teams to work on each sub-topics and then later their work can be merged to meet the goal of this activity. |
| Kimon Nicolaides | 1.Goal - I think we need to clarify our Goal as stated here. Says 'set the standard' but are we setting a standard here or producing a whitepaper/guideline document or a CoP? Approach will differ accordingly.  2.Would be good to expand on the specific challenges of IoT in the wider framework of network security, and therefore determine strategies for their mitigation. | 1. Define Goal and forward roadmap beyond current deliverable 2. Provide view of what IoT is, the potential use cases, related concept of operations and how these are likely to evolve, while outlining some of the challenges this brings and potential solutions. IoT represents a change in security dynamic due to a number of key factors such as total scale of deployment and transacted data, challenges with interoperability and effective availability/implementation of relevant security standards across the e2e system, aggressive cost and size constraints on IoT products leading to potential tradeoffs, a highly varied spectrum of potential threats/attack modes, complexity in managing a forward upgrade path for ongoing mitigation of emerging security vulnerabilities and standards updates and so on. |
| Jitender Grover |  |  |
| Binit Sharma | Visions to be achieved: No Harm Only Benefit. Security, Privacy, Safety etc are addressed by No Harm. New Design Implementation should also be able to emphasize Benefit part also. | 1. Ensuring No Harm (Compulsory/Mandatory) and Emphasizing Benefit if possible. 2. Short Term/Long Term Implementations. Short Term addresses the Solutions to Existing ICT and Long Term aims Exhaustive Design Implementations achieving 100% Failsafe and Safe system and services. 3. As IoT by Design is more rigorous compared to Protecting the Internet Traffic.. boost to supporting R&D and Necessary Information Theory Formulation is needed. 4. Exhaustive Strength, Weakness, Opportunity and Threats Analysis and Solution (by Design in Long Term) 5. Seamless Interoperability by Design. 6. Making Man responsible for Machine. (Digital ID for All Entities, both man and machine (liable to man), Digital Registry. 7. Test and Benchmarking Implementations too. 8. Get-Set-Create-Advocate-Operate-Regulate: Universal Collaborative Action Project. 9. Collaborative Pro-action towards unanimous Implementation. 10. Clearly defined Laws for Intentional Harmful Attempts. |
| Martin Murillo | 1. In the context of IoT, the implications of security go beyond loss of privacy or economic consequences. Lack of security implies impacts on physical things and thus to the physical wellbeing of humans. Depending on how critical the application is, the damage can be different. Currently 80% of privately owned critical infrastructure has public implications. The incumbent IoT could worsen this. Depending on the IoT application, availability, integrity and authenticity will have more priority than confidentiality.   2. (Contrary to 'romantic' views of IoT) IoT devices are highly depending on cloud services. This is for various reasons: convenience, current Internet architecture, resource constraints, decisions of key industry leaders, etc. In the absence of standards, regulations, or best practices, private institutions choice is dictated by technical feasibility. At times security is not a significant variable in the choice. | 1. Have in mind risk, incident reporting and response, resiliency. Include different stakeholders, besides technical.  2. "End to End" could mean IoT-Cloud-IoT communications. Might also mean Cloud-Cloud communications, etc.  3. Consider our role to be of "organizers" or recommenders. This is because IoT is a concept that organizes or gathers existing devices and existing protocols and standards in order to create an ecosystem. The putting together of this ecosystem can be made in manners that maximize security.   Thus key in our context is to have a good macro view of the "market". As suggested by others, a layered approach is a good start.   A very conservative output would be to recommend the usage of sets of standards and architectures that might already exist. A very aggressive output would be to take part in the design of the future Internet (I.e. Internet 2) for influencing security for IoT ecosystems (for example). |
| Margaret Loper |  |  |
| Samah Ghanem |  |  |
| Geoffrey Hartwell |  |  |
| Kewei Sha | 1) Tight coupling between physical systems and cyber systems.  2) Low capable things that cannot support heavy computation needed in the traditional security solutions.  3) Security in the newly developed protocols used in IoT.  4) Higher privacy requirements in the IoT systems.  5) More challenges in the trust management. Efficient reputation evaluation system is needed. |  |
| Edward Marsh |  |  |
| Dennis Inegbedion |  |  |
| Geoffrey Hartwell |  |  |
| Jernej Mavrič |  |  |
| Sandhya Aneja |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**J. Meeting Minutes**

**Notes/Minutes: Conference Call July 15th, 2016**

**Attendees:**

-Jared Bielby

-Dena Hoffman

-George Corser - Group Leader

-Tom Coughlin

-Lucian Cristache

-Alan Chachchin

-Martin Murillo

-Sukanya Mandal

**Housekeeping:**

1. Introduction: Introduction of George as leader of group and quick overview of objectives
2. Timing of Calls: Calls will be held biweekly at 3 pm ET. Dena Hoffman to set up WebEx calls
3. Affiliations: All participants please add their affiliations to the document here

**Notes:**

1. This document is the working document that will become the white paper
2. Defining Goals and Timeline: First part will be to define the goals and timeline and begin assigning tasks for the development of the white paper
3. Voting on Tasks: Table developed to help narrow the tasks and questions. This will also allow all participants to vote on the tasks. The tasks are based upon ETAP conference call. All are encouraged to add tasks.
4. Research: All please contribute to a literature review that needs to be considered. Please add the research under "White Papers/Standards Relevant for Review" section of the document. These can then be reviewed and discussed.
5. George's Vision
   1. What is the problem we are discussing
   2. What has been done so far on the topic
   3. Determine who the audience is and what is the literature size of the audience
   4. Define the components and structure for the white paper and then assign tasks.
6. Scope of Paper: Please call/email George with your thoughts – All – Open up call to discuss
   1. Alan C: "Good Housekeeping Seal of Approval (GHSA)": To help provide such a seal regarding the topic. This is one possibility. The larger point is that incentive needs to be changed for companies to do this up front and change the focus from the benefit from profit and then retrofit the security piece (Nancy W. of Cisco). Question is beyond the GHSA in going for a solution. Need to change the incentives to trigger having an impact and to have companies employ these measures. What needs to be thought of and what are the mechanisms that need to be considered as part of the axis – economic, XX, and XX. Goals is we don't want it to be cheaper for companies not to do the right thing (from DC ETAP).
   2. George C: - Certification may be along the lines. What is the plan and does the plan match what you want to do. You must consider societal costs when creating security.
   3. Alan C: Go beyond a single solution. Need to highlight the whole problem better. Different mechanism may exist in different industries. Rather than going right to the solution let's focus on the holistic problem. The certification process is one of several processes/solutions.
   4. George: Need to come up with a problem statement. Alan wrote the problem statement in XX paper (Jared has reference from DC ETAP and can add the reference here.) *UPDATE:* [Click here](https://onedrive.live.com/view.aspx?resid=2659E04707EC6B80!201&ithint=file%2cdocx&app=Word&authkey=!ALbnUbIA3reAe3I) for Access.
   5. Glenn Fink: In the process of publishing a book and one of the authors has done a survey on law. The FTC provides assurance of fairness to consumers that a product does what the vendor claims it will (not certification). Incentive is legal action could ensue if the product does not meet the "standards" outlined in their advertising. For example, a baby monitor was advertised as "secure" but the authentication did not work and the product was hacked. The company was sued by FTC and reparations put it out of business. IEEE should be in the business of making recommendations, not enforcing standards or product claims. However, we could provide a standard that FTC could enforce if vendors claimed. Better, I think we should provide recommendations that can be adopted by governments, vendors, and consumers. This could involve metrics of success that standards-enforcers/product-raters could use in testing.
   6. Alan C: Maybe we should be recom things that people should be doing, not pushing to be involved in certification. Has anybody looked at what the FTC does to provide incentive? Is this an incentive or dis-incentive?
   7. George shared Cisco IoT reference model. Suggested that the slides be added to the private group for all to have access. He also shared a broader view that covers the people who are involved with an example showing the IoT. Jared suggested adding these to the chart for the scope and voting them in or out for the white paper. Also need to determine how many items will be in the scope.
   8. Alan: What is the point of what we are doing/objectives to be defined in order to help then define the scope and problem statement to be addressed.
   9. Most important thing to take away and pursue for next meeting:
      1. George: Everyone who has a concept for the paper and write that vision/purpose statement and share it with the team to help develop a final objective statement.
      2. Alan: Alan to look at the paper he wrote on security for connected vehicle and see if there are any references that can be added to the research/reference section
      3. Glenn: Best practices and metrics is a direction that we need to be evaluating. Look at the IoT law chapters that tell us what the role of existing organizations so we can stay out of certain areas.
      4. Martin: Took part in various initiatives is that we should create a case study for an application to put it into practice and apply the objectives. Agree that we should be making recommendations
      5. Lucian: Focus on specific technologies around IoT since it covers everything from cloud to cyber security. We should identify those and come up with best practices for Iot technologies and infrastructure. Having a standard for a company is a good incentive – especially if it ties into IEEE Standards.

**Action Items/Agenda for Next Meeting:**

1. Affiliations: All participants please add their affiliations to the document here -- All
2. Research: All please contribute to a literature review that needs to be considered. Please add the research under "White Papers/Standards Relevant for Review" section of the document. These can then be reviewed and discussed. -- All
3. Scope of Paper: Please call/email George with your thoughts – All
4. Sharing Slides: George or Jared to upload the slides George shared so that everyone has access to these files. -- George/Jared
5. Objective Definition: Team needs to outline and agree on the objective and scope for this white paper. Need to determine the process to develop this and gain agreement.
6. Picture: Track down the original picture (top of page 2 of what Alan provided) in the ETAP – Glen may have this and can add it to the private group. -- Jared

**Notes/Minutes: Conference Call July 29th, 2016**

1. **Attendees:**
   1. Jared Bielby
   2. Dena Hoffman
   3. Alan Chachich
   4. George Corser
   5. Lucian Cristache
   6. Sukanya Mandal
   7. Glenn Fink
   8. Binit Sharma
2. **Housekeeping/Background:** Jared provided an overview from the previous meeting and outlined objectives and potential opportunities:
   1. **Cross Pollination Opportunities:** Jared outlined some opportunities and will turn over the ideas to George to determine if the group would like to pursue, and if so, sub teams to develop these opportunities
      1. **Interprose Summary Prospect:** The Internet Initiative would like this team to submit a summary of this paper. Assigned to George to determine who/how this will be done. Jared has some guidance thoughts on how to do this.
      2. **Potential Webinar:** Chris Januzzi (IEEE staff for 3I) would like to ask this group about creating a webinar around this white paper. Turning over to George to determine if group wants to do this and who would like to be involved.
   2. **Review from Previous Meeting** – what areas we want to focus on per the group's input
      1. **Vision and Purpose statement:** define and agree
      2. **Best Practices and Metrics**
      3. **Case Studies:** Look at various initiatives and see if we can find a good case study as a template for recommendations.
      4. **IoT Technologies:** Identify the appropriate IoT technologies
      5. **Slides** have been uploaded to private group to review from George
      6. **Review the objectives**
      7. **Review the slides from the ETAP** conference that Alan has uploaded.
   3. **Goal for this Group:** Our goal is to have a white paper available by mid-October in order to have it published by the end of the year. This should be using at the technology and policy aspects. Bring policy makers together with technologists.
   4. **Narrowing the Scope:** Would like to narrow the scope and then flow it through the template that has been added in the document with individuals selecting a part of the scope and then writing 3-4 paragraphs and/or abstract around each area to get the group started. All should note their sources when developing.
3. **Discussion – George**
4. **Newsletter**:
   1. **Scope Statement** has been drafted by Glenn. "Create a set of guidelines and best practices so well investigate and thought out that other use it to for their clarifications, laws, and product ratings" This white paper would be available others to write standards.
      1. **Lucian**: How tie into other industries. Our paper will be more general infrastructure.
      2. **Jared**: Would it help to include that the creation of the guidelines is from established practices and are inclusive of those differences?
      3. **Lucian**: There are so many out there from health care to automotive. I assume we should come up with best practices for worst case scenario and come up with recommendations based upon privacy for each vertical market.
      4. **George**: Our purpose is to come up with a set of best practices and guidelines and then dig deeper without looking at specific technologies. Let's go with what we have for scope statement:
         1. **"Create a set of guidelines and best practices so well investigate and thought out that other use it to for their clarifications, laws, and product ratings"**
         2. **Invite John Stankovic** as he's an IEEE Senior Member and has written on this topic and would be a good addition. George shared paper written by Stankovic that provides a good overview. Action: Write a proposal to Stankovic to join. - Jared?
      5. **George**: Shared a document (couldn't see what it was). Suggested this document be a key document used. Also like the sections. Suggestion:
         1. Use this document as our case study
      6. **Is this a survey paper or suggestive paper?** Need to define what is in/out of scope. The scope statement appears to be wider than a survey paper. Need to figure out if this is a suggestion of best practices or more. Suggestion is to begin writing and see if this brings to survey or something new with a conclusion.
      7. **Alan's ETAP Paper:**
         1. Without making it that the rewards/punishment not making companies do the right thing the concern is what can be done so those responsible for building the security into these things do the right thing.
         2. Gave example of Cisco ranking security as 5th on list in developing a chip and not in chip due to cost.
         3. It's about how security falls in the list of priorities for companies. Similar with safety and how does that fall.
         4. What can IEEE do to help make a difference? Where can IEEE play? Our expertise is in design and policy. In design there are considerations to make them failsafe. Policywise – what are the policies and penalties or incentives to keep safe? How does policy fit and can IEEE be influential in this debate? These are areas that IEEE can play a role and it's important because if you don't do it then it's all being done for nothing.
         5. Best practices would fit into this and would not be at odds with the scope of this group.
      8. Potential Section: Societal impacts not in automotive sector
   2. **Internet of Things:** Define and what technologies should be covering?
5. **Action Items/Agenda for Next Meeting:**
   1. **Stankovic Invite:** Write a proposal to John Stankovic to join this group. Jared and George
   2. **Relevant Policy Makers:** Everyone invite and research others who might be a relevant policy maker to invite to this conversation and could help guide us in this research. Jared to talk with Anna about suggestions for policy makers. All
   3. **Email George** regarding the following: All
      1. Scope as outlined above is good/edit? If the statement is not good enough then make suggestions to edit.
      2. Cisco reference is a good model?
      3. TOC: Do you like the automotive version and use this as a starting point? Please indicate if agree or make suggestions to edit.
   4. **Draft of IoT Definition:** First draft of defining IoT and then have the rest of the group be able to edit/react before the next meeting in two weeks. Cisco reference model is a starting point. George will create a snipet and bring forward to the group to edit/react. George to draft, share in the IEEE Collabratec group and others to react.

**Next Call:**

* **Begin Assigning Writings:** Review the aspects and begin assigning individuals to write the summary for each of the sections.

**Notes/Minutes: Conference Call August 12th, 2016**

Attendees:

George

Alan

Chris

Jared

Lucian

Sukanya

Samah

Martin

Notes:

Assigned tasks:

1. Draft non tech diagram based on Cisco model: *George, Martin*
2. Describe the security and privacy risks associated with IoT - prioritize:
3. Minimizing and controlling the attack surface: *Lucian*
4. Risk Assessment

Action Items:

**Notes/Minutes: Conference Call August 26th, 2016**

**Attendees:**

1. George Corser
2. Jared Bielby
3. Mohammed Aledhari
4. Chris Hrivnak
5. Lucian Cristache

**Notes:**

1. A short talk on publication recommended
2. Talked in details about the goals of ETAP and beyond the publications Recommended to follow up the IEEE internet initiative events
3. A quick talk on interest subgroups and roll of each one
4. Divided the process into stages and each stage can involve the whole working group or may have subgroups, and each subgroup can work independently or interact with other subgroups as shown in provided diagram
5. Narrowing the scope of the working group by asking participants to:
   1. Pick their interest subgroup(s) in the provided table - Supplementary Materials (**B. Contributor Teams**)
   2. Vote to the interest challenges/issues to be investigated in the provided table - Supplementary Materials (**F. Narrowing the Scope 2**)
6. Asking participants to provide their Gmail addresses (create one if you don’t have one!) to enable subgroup members to communicate with each other via Google Hangouts (daily, twice a week, etc. TBA)
7. Encouraging participants to start writing their thoughts in assigned sections
8. Agreeing on definition of IoT and IoT diagram
9. Deadline of filling up the provided tables is Next Friday Sep. 2, 2016 to finalize dividing subgroups with the assigned tasks

**Notes/Minutes: Conference Call September 23, 2016**

**Attendees:**

1. George Corser
2. Jared Bielby
3. Mohammed Aledhari
4. Glenn Fink
5. Sukanya Mandal
6. David Richardson
7. Lucian Cristache

**Notes:**

1. Need a thorough list of best practices to be captured in order to be considered and added to the research and potential use for the paper.
2. It is important for everyone to add their thoughts to the document in order to document the thought process and doing so might be in new sections.
3. Suggesting to add threat detection to the list of covered topics

© 2016 IEEE Internet Initiative, ETAP Internet Technology Policy Community. All Rights Reserved.

For more information, please contact jared.m.bielby@ieee.org