**UNIT-4**

**A human-centric trust model for the Internet of Things**

For IoT security to be successful, there needs to be an effective way to reason about how humanity can trust the security, safety, and privacy of this massive transformation of the world. Most importantly, “ordinary people,” whether they are consumers or workers, must be able to safely, reliably, and intuitively interact with vast, complex, interconnected systems of IoT devices. It can be overwhelming to think about all the ways individuals and society can be damaged by the haphazard engineering of systems that merge the physical and digital worlds. Technologists have done a terrible job with security technology so far, yet now we are about to impose those failures onto the physical world on a scale that only ubiquitous, pervasive, even invasive computing and connectivity can accomplish. Continuing the status quo is unsustainable.

The IoT can be thought of as a hyper-connected, hyper-distributed collection of resources. The complex ecosystem surrounding IoT devices means trusting them will not be intuitive. These connected devices can potentially be controlled and observed by others anywhere on the planet. For example, before the IoT, it was always easy to physically check the locks on your doors and decide to trust those who had the keys. Now with Internet connected “smartlocks,” you can check or alter their state from anywhere. How can an “ordinary person” track who has the electronic key and discern that the software controlling the lock is secure and resistant to hacker attacks? A February 2017 survey of IoT consumers showed that [72% were not sure how to check if their devices had been compromised](http://www.mediapost.com/publications/article/295861/44-concerned-about-personal-info-theft-through-th.html).

Users should still be able to delegate trust and authority with the same level of certainty as when using purely physical devices. Whether home automation devices or industrial devices, technologists have a responsibility to provide people intuitive and simple methods to accurately discern what devices and services can be relied on, and what threats they should rationally worry about. This poses the question, “How can we get back to a place of relative simplicity of function and where the average user has a reasonable understanding of the integrity of their connected devices?”

**The need for a human-centric IoT trust model**

There currently isn’t an effective and widely adopted **trust model** to guide IoT device designers and service providers. A trust model can describe how IoT resources are protected and governed, how their ability to preserve security, safety, and privacy can be relied on and how they may have capabilities to defend themselves from attack. It is fair to say that currently, designers haphazardly add device connectivity, remote control, and other IoT features to devices, while leaving the user with risks that are hard to understand and manage. An effective trust model will clarify device providers and service providers’ responsibilities and point to ways in which we can ensure that people can use IoT devices with little worry.

Currently, there’s not a reliable and complete inventory of threats for the IoT, nor have the threats that have been identified been properly prioritized. As an example, a relatively new threat has burst on the scene over the past few years, called ransomware. In the context of IoT, this should be fairly high in priority. A new trust model that takes this into account is needed to underpin the means for mitigating associated risks.

What then is a trust model and how can it be “human-centric?” The word “trust” in this context means reliance. A trust model shows how each entity in an ecosystem relies (or could rely) on another. And human-centric in this context means a trust model aimed at giving effective administration of security, not to computing professionals, but to average users. A human-centric trust model can be created to show how ordinary people can sensibly delegate to others access to controls and data associated with IoT devices and systems.

With such a trust model one can ask such questions as how can IoT devices be relied on to defend against viruses? Can they update themselves to repel new attacks or do I need to take responsibility for that? If a device is compromised, do I need to isolate it or can a service take care of that? If I delegate access to my home sensor information to my power utility, what can they do with the information and how is it protected? A human-centric trust model can help developers determine things such as: Who and what I can rely on for protection? When I give others access to my devices or information from their sensors, how I can rely on them? How can I limit the ability of others to use those devices?

**Scaling a human-centric IoT trust model**

What are the components of this new IoT trust model? What will likely be different from existing security models? The most obvious answer here is scale. We need to address many (billions) of devices containing multiple sensors and controls (sometimes dozens or more per device). These are also truly hyper-connected devices (part of multiple networks and can somewhat randomly intersect with many networks over time).

Two things come to mind when dealing with such massive scale. The first being how can devices autonomously defend themselves? Secondly, can we rely on network security techniques to keep our things out of trouble? The answers are: 1) a scalable trust model needs to place a lot of responsibility on device and application self-defense and provide for distributed security administration, and 2) we cannot rely on network security techniques since they subject an ecosystem to weak-link vulnerabilities. Once any network is penetrated, the attack can work its way to multiple networks by exploiting devices that overlap with other networks. A network security approach attempts to isolate devices that by their nature want to communicate. Such an approach cannot scale.

Another property of an IoT model that helps deal with massive scale is the use of **services and distributed applications** that help individuals visualize and easily administer security for devices. For example, a homeowner or factory manager could subscribe to specialized, cloud-based services that scan sensors in their networks for anomalies or behavior signatures that indicate illicit behavior. Such services can use sophisticated information sharing capabilities to formulate knowledge bases of device behavior patterns. These can be drawn upon by local applications that administer privately managed sets of devices and sensors. In essence, there can be automated, distributed “neighborhood watch” systems that share observations and disseminate warnings of wide-scale attacks. How these systems behave, especially with respect to their own autonomy and their functioning as human decision support systems are also potentially parts of a trust model. It would also be necessary to consider how to make this information accessible and comprehensible to the average user or worker.

Will simple things like a light switch, home speaker, or toaster also need sophisticated security sub-systems? Maybe, but the use of a trust model in conjunction with system analysis can help keep things simple and scalable. If a device is “IoT enabled” by merely adding a generic computation and communications stack with a generic operating system that enables arbitrary applications and device interactions, then you are at risk for security problems, even with so-called simple devices. However, if the system design is guided by a trust model for governing interactions and functionality, then designers can more easily keep things simple and limit risks.

The trust model can also call for a secure update capability, allowing new features to be safely added when a need is identified rather than loading a device with potentially exploitable features. In addition, devices can be asked to implement a relatively simple reference monitor that accepts commands from other devices on a very limited network or from a limited number of other devices. More generally, IoT device designers should keep functionality limited and explicitly enable new features only after fully vetting the inherent security risks.

**What would an IoT trust model look like?**

This article won’t prescribe a detailed plan for a trust model. But, it makes sense to enumerate some of the components of a trust model that address some of the unique challenges for the IoT. In this context, a trust model consists of entities and processes that one may rely on to help preserve security, safety, and privacy for Internet connected things. Below are a series of points that will help identify various components of such a model.

**Devices and hosted applications**: When I bring an IoT device into my environment, what aspects can I rely on for security, safety, and privacy? What are the intrinsic properties and capabilities of the device that make it trustworthy? What are my responsibilities? What can I expect from other entities such as the device supplier or the services that interact with the device? If it’s a simple thing, I certainly don’t want a long list of instructions about how to keep it, myself, and my household safe. Making this intuitive will be a challenge.

**Resources**: It helps to identify certain components a trust model will need to address. An IoT device can have various resources made available to a number of entities through the Internet. They might consist of device controls and state information, as well as streams of information from connected sensors and computation capabilities. How do I know what those resources are and who has access to them? How do I govern access to the device? There is also the question of how well these devices protect themselves from attacks and how robust are those defenses? Again, the challenge will be to make the answers intuitive for a broad range of people.

**Trusted attributes**: To make decisions regarding the trustworthiness of devices, processes associated with them, or entities accessing the device or my network of devices, I may rely on assertions made by others that I trust (such as a device is “child-safe”). Setting aside, for the moment, the question of what makes an attribute trustworthy, how can I reliably use these trusted assertions? Consider this context: if I give a youngster access to some home automation capabilities, I might want to be reminded that this action includes a hot water temperature control and is not considered child safe by the developer. Sensor data might have attributes. Some data may be sensitive (such as motion data with time stamped GPS coordinates) and derivatives of that data might be claimed to be anonymized. How can such data be reliably labeled? How can proper usage of labels be ensured? Classification and labeling can be complex and has liability implications, but must be addressed as part of an IoT trust model.

**Delegating trust**: Another important aspect of any effective trust model will address the concept of delegation. How do I practically delegate trust to someone else? There are a number of contexts for this. For example, when I bring a device home, I claim it as mine, perhaps with some straightforward gesture. Only I can control it and be privy to the data it collects. But, if I want to give others access to it, how can that be done reliably and with full understanding of the implications? How can I ensure that this delegation of trust will be enforced? The answers may not be straightforward and I may require some aids to guide me.

**Virtual composite devices**: Part of the reason for why these human-centered difficulties need to be considered in IoT trust models is that physical devices can be virtualized as well as be parts of **virtual composite devices**, the components of which may interact. In home automation, such composite devices may be called “scenes” where multiple devices cooperate to perform a certain household task. In an industrial or metropolitan context, composite virtual devices will be arbitrarily complex.

**Automated performance aids**: These are systems that can help us understand the implications of actions such as including something as a component in a virtual device or system, or the implications of delegating trust to some entity. These will be an important part of a human-centric trust model that addresses both the scale and complexity of the evolving IoT. One potential example of such an aid are **intuitive gestures** used when in interaction with the IoT. Typically, such gestures are used in a specific context to point to specific things or virtual things, and refer to specific entities.

**Identity management systems**: For these automated performance aids, as well as other IoT related systems, to properly function, the right device or group of devices and the right entities who are to be trusted need to be identified. This will require identity management systems that are vastly larger in scale and much more intuitive. Here again, it is fair to say that the current inventory of **identity management systems** (such as username/password pairs, and X.509 and SAML certs) are woefully inadequate and rarely address many of the already known use cases for identity. And, of course, it is difficult to claim that these systems are intuitive and easy to use. While advances are being made in some aspects of identity management (notably biosensors), the territory that must be covered here is vast, and includes reliable references for virtual things and their configuration into composites and virtual systems that ordinary people will need to interact with.

**The role of security associations and reference monitors**

Trust models will have various layers. One layer will address the secure actuation of a trusted process. This layer will use the concept of **security association** and will need to be made both reliable and intuitive. For example, when I want to give someone access to my front door, I typically give them a physical key. I trust that they won’t copy that key and give the copy to someone else. With electronic locks, I can use an intuitive gesture on my phone to indicate I want one of my friends to be able to open the front door. One way (of many) that might be actuated is by causing an electronic key to be securely transmitted to both the lock and to my friend’s mobile phone. The lock will keep a security association between those keys and a permission to open the door.

Now my security association with the lock gives me the right to modify the security association table, but my friend’s security association with the lock does not. That is, I have delegation rights and she does not. This delegation process involves security protocols, key bindings, permissions, and other security processes. The idea of a **reference monitor** was mentioned before, and it will be an extremely important concept in IoT trust models, since all IoT devices can harbor one. A reference monitor can be appropriately simple or elaborate. It is typically implemented as a core (or kernel) process that checks each command against a list of security associations for permissions to take an action or access to some resource. Now, when my friend wants to open the door, the lock’s reference monitor will evaluate her command, and use of the electronic key I gave her, and perhaps the identity of the device she used if it is part of the security association. Much of this will usually be hidden from the user in a trust model layer. People should use simple gestures for this delegation of trust, but the model needs to understand how those gestures precisely carry out the intention of the command giver (and do no more).

Yet another part of an IoT trust model will be the concept of a **secure update process**. This is an area that has seen some success, at least in some contexts. That’s good, because the need to fix things that can potentially go wrong will surely be great as we integrate the physical world with the cyberworld. Again, the scale of IoT and its multitude of contexts will be challenging. Given the massive scale of IoT, it will likely be a good strategy to give devices the responsibility to update themselves and to do so in response to trusted notifications from automated systems such as attack monitoring systems. However, people have gotten used to updating their mobile phone OS and apps, but that process still causes disruption. In an IoT context, this may not be tolerable, especially when updates may subtly change the user experience of a faithful, reliable thing.

In this article, communications security hasn’t been covered, and as alluded, comsec processes may not want to be included as an intrinsic aspect of a trust model. Sometimes they will be part of the security actuation layer, but given the overall context of IoT and the myriad communications processes that may be both intrinsic and extrinsic to devices and systems of devices, in general an effective trust model will have to be actuated at the device and application layer, and not require isolation from communication processes.

**The inherent limitations of models**

The final point to be made regarding IoT trust models is that a model is not reality, nor is it even virtual reality. But humans can use the models for both the design and use of IoT devices and systems, and for understanding how they can be projected usefully into everyday contexts. There is a lot to do to scale the modeling process and properly connect it to the human experience. This may include standard names and references that people can understand unambiguously, and universal design paradigms that allow people with different capabilities to interact with the IoT conveniently and safely. For now at least technology communities can begin working together to model how the attributes of safety, security, and privacy can be assured without providing an undue burden for people. We need to make it simple for humans of all capabilities to properly implement IoT security. If not, we run the risk of the infrastructure of simple things we increasingly rely on to continue to fail on an ever-expanding scale.