Challenges to ensuring human safety throughout the life-cycle of Smart Environments

David Kotz
Dartmouth College

Travis Peters
Dartmouth College

ABSTRACT

The homes, offices, and vehicles of tomorrow will be embedded with numerous "Smart Things," networked with each other and with the Internet. Many of these Things are embedded in the physical infrastructure, and like the infrastructure they are designed to last for decades – far longer than is normal with today's electronic devices. What happens then, when an occupant moves out or transfers ownership of her Smart Environment? This paper outlines the critical challenges required for the safe long-term operation of Smart Environments. How does an occupant identify and decommission all the Things in an environment before she moves out? How does a new occupant discover, identify, validate, and configure all the Things in the environment he adopts? When a person moves from smart home to smart office to smart hotel, how is a new environment vetted for safety and security, how are personal settings migrated, and how are they securely deleted on departure? When the original vendor of a Thing (or the service behind it) disappears, how can that Thing (and its data, and its configuration) be transferred to a new service provider? What interface can enable lay people to manage these complex challenges, and be assured of their privacy, security, and safety? We present a list of key research questions to address these important challenges.

CCS CONCEPTS

• **General and reference** → **Surveys and overviews**; • **Computer systems organization** → **Embedded and cyber-physical systems**; • **Security and privacy** → *Distributed systems security*; *Usability in security and privacy*;

ACM Reference format:
David Kotz and Travis Peters. 2017. Challenges to ensuring human safety throughout the life-cycle of Smart Environments. In *Proceedings of SafeThings'17, Delft,Netherlands, November 5, 2017,* 6 pages.
DOI: 10.1145/3137003.3137012

1 INTRODUCTION

One of the common visions for the future Internet of Things involves the deployment of *Smart Things* in everyday living environments – homes, offices, cars, shops, schools, and more – resulting in *Smart Environments*. These networked Things offer many potential benefits to the owners of the Smart Environments (more efficient use of energy, for example) or to the occupants of the Smart Environments (personalized services, ready access to information, improved health and wellness). If not designed, deployed, configured, or managed correctly, however, these same Things can create unsafe conditions and increase risk of harm to persons and property. In this paper we explore the relationship between security, privacy, and safety, and identify challenges that must be addressed before the vision of Smart Environments can be safely realized.

Given the broad conversation (and hype) around IoT and Smart Environments, let's begin by defining the scope of this paper and some of the terms used herein. In this paper, the IoT refers to the *Internet of Things*, a vision in which a wide range of everyday objects become *Smart Things* through the inclusion of digital electronics and a network interface that allows them to communicate with other Things and, directly or indirectly, through the Internet with remote services.[1] Smart Things typically have the ability to sense their physical environment (through sensors) and, sometimes, to act on the environment (through actuators). They may or may not have a human user interface. They may be stationary or mobile. They may be small (like a remote control) or large (like a refrigerator). They may be battery powered or line powered. A *Smart Environment* is an environment involving a collection of Smart Things, interacting with the environment, with its human occupants, with each other, and with remote services, to accomplish one or more applications. Things – and human occupants – may come and go from the environment, over short and long time scales.

The environment has an *owner*, a human individual or organization. Each Thing also has an owner – again, a human individual or organization. Importantly, the environment owner may not own all the Things in the environment – indeed, this could be a common case. In a school or shop, for example, one organization may own the environment and the embedded infrastructure (Smart Things for heating, cooling, lighting, inventory, communication, physical security, and display) but occupants may enter the environment wearing or carrying personal Things (for purposes such as education, entertainment, or wellness). In some settings, we must further distinguish the *operator* of Things from the *owner* of Things. For example, a shopping mall may own the physical environment and the embedded infrastructure, but may outsource the operation of that infrastructure to one or more companies that specialize in management of complex building infrastructure. The individual shopkeepers, as renters of environments within the mall, may deploy their own smart-environment Things to manage inventory, deter shoplifting, or personalize customer experience. The shopkeeper may outsource operation of these Things to a central organization that has licensed a franchise for this shop.

Given this context, then, we turn our attention to *safety*. In this paper, we consider a Smart Environment to be *safe* if it does not create undue risk of harm to persons, organizations, or infrastructure.

SafeThings'17, Delft,Netherlands
© 2017 ACM. 978-1-4503-5545-2/17/11...$15.00
DOI: 10.1145/3137003.3137012

[1] There seems to be no universal definition for the term *IoT*; Wikipedia cites several [9].

Persons may suffer physical harm, financial harm, or reputational harm. Organizations may suffer financial harm or reputational harm. Infrastructure may suffer physical harm, which can cause financial harm to its owner and logistical harm to its occupants. (Suppose a school burns down but nobody is injured – the city must pay for a new school and the schoolchildren have no place for school.) We are primarily concerned about proximal harms, including direct and immediate threats to physical, financial, or reputational safety. Smart Things, and the resulting Smart Environments, may create risk because of errors in design, implementation, or configuration, or due to mechanical or electrical failure.

In this paper, though, we are most interested in exploring the harms that may be incurred by Smart Things (and collectively, Things in Smart Environments) due to cyber-security or digital privacy failures. A security vulnerability (whether a flaw in design, implementation, or configuration) in a Smart Thing could enable an attacker to cause that Thing to behave in ways that create physical harm to the Thing, the environment, or the occupants. A security or privacy vulnerability (whether by design or due to flaws in design, implementation, or configuration) in a Smart Thing could expose sensitive personal information about the owner or occupants and thus cause them reputational harm.

Indeed, our position is that security and privacy are necessary (though certainly not sufficient) to ensure safety. This aspect may be one of the unique characteristics of Smart Things and Smart Environments, that differentiate them from traditional "non-smart" Things. Furthermore, the Internet provides an entryway for a remote adversary to attack the Smart Things, and the Smart Environment, effecting harm at a distance – another key differentiator from our traditional understanding of safety in everyday environments. The adversary need not be physically near to cause harm.

Indeed, what kind of adversaries should we consider? A remote third party, intent on causing harm to the occupant, owner, operator, Thing, or Environment, is the type of adversary commonly envisioned. A Thing manufacturer, or vendor of an associated service, may be adversarial with respect to the privacy of the occupant or owner – for example, a Thing that captures information about occupants for use by the service and yet shares or abuses this information in ways that violate the occupants' expectations of privacy. Similarly, a Thing owner or operator may violate occupant privacy. In some scenarios, the occupants themselves may be adversarial, by attacking the Things in a Smart Environment they occupy – consider students in a school, or renters of an apartment, or customers in a shop, exploiting vulnerabilities in nearby Things to obtain benefits for themselves or to purposely cause harm to the infrastructure or owner of the Environment.

For that matter, we should consider the varied goals of an adversary. Some may be malicious, deliberately seeking to cause harm. Others may be greedy, seeking benefits for themselves while incidentally (and perhaps unintentionally) causing harm to other persons or to the infrastructure.

Thus far we have considered occupants, operators, and owners. There are more interested parties involved, however. Smart Things and Smart Environments exist in the context of society, and thus interact with an economic, legal, and social ecosystem. Consider, for example, insurance companies (who have a financial incentive to ensure the safety of Smart Environments and their occupants), public officials (who may be responsible for enforcing safety regulations in public environments and have an interest in public health), emergency responders (who need access to infrastructure when responding to fire and medical emergencies), and law enforcement (who also require access to infrastructure when reacting to emergent situations and who may legally require access for investigative or forensic purposes). Smart Things and Smart Environments must recognize the needs of these other parties – sometimes required by law or by contract – and yet not allow the resulting interfaces to be co-opted for mis-use by hackers or by corrupt officials.

Clearly, Smart Things and Smart Environments are a complex subject. In this paper, we summarize the challenges of establishing and maintaining Smart Environments and the Internet of Things across their life cycle. In the remainder of this paper we outline a series of critical challenges, with an emphasis on safety and particularly on those challenges related to security and privacy. We conclude by extracting a list of critical research directions and call on the community to focus its energy on these challenges.

2 CHALLENGES

As noted in the previous section, a future involving IoT, Smart Things, and Smart Environments is a complex ecosystem that raises unsolved safety-related challenges. Indeed, although the prior literature related to IoT safety, security, and privacy has raised some of these issues [1, 2, 4, 7, 8, 11, for example], we believe that the challenges are even more complex than most developers or writers envision. In this section we summarize some of the key safety challenges with an emphasis on those related to security and privacy.

In particular, we argue it is important to think of the life-cycle of Smart Things, and of Smart Environments. Maia Neto et al. recently took this approach in presenting the "AoT" architecture for the management of Things throughout their lifetime – from manufacture to retirement – with a focus on authentication and access control at each stage [4]. While the AoT structure is commendable, it makes simplifying assumptions suitable for a smart-home environment that may not apply for a broader range of Smart Environments. AoT presupposes a single homeowner, or small group of home occupants, that control all Things throughout their life-cycle. We anticipate more complex settings involving multiple owners, operators, and occupants, and that there may be hundreds of Things that observe occupants of a Smart Environment without their knowledge.

We thus describe a series of challenges, loosely organized along the Thing life-cycle from the provisioning of a Thing, through its operation and relocation, to its retirement.

(C1) Things must be configured – securely

The Smart Environment of the future will include a variety of Smart Things – perhaps dozens or hundreds of Things. It will be a rare environment that is created from scratch, all at once, by a single developer or owner. Indeed, we anticipate that new Things will be introduced to the environment from time to time, installed by an owner, operator, or occupant on either a permanent or temporary basis. New Things will need to be configured to operate in this particular Smart Environment, to be suited for the Things' owner, to be connected to the relevant cloud services, and to be connected to the other Things in the Environment and beyond. This configuration process may be complicated, particularly given the scale and variety of Things in the Smart Environment – and requires strong and usable security controls. Specifically, someone configuring a new Thing must be able to impart correct and authentic configuration information, without requiring technological skill or experience. (With the *Wanda* system, for example, the person can simply point a digital "wand" at a new compatible IoT device to securely impart configuration information and enable that device to join the Wi-Fi network or to connect to other Things in the environment [6].) With incomplete or improper configuration, Things may not act when they should, or may act badly; with an insecure configuration process, adversaries may take control of Things during the configuration step or may obtain key material that enables them to access or control Things in the future. Either case has the potential for harm to the occupants or infrastructure.

Robust, usable interfaces and mechanisms like Wanda are needed to enable owners and operators to configure and reconfigure Things and their inter-connections – and to validate those configurations to ensure keys and other sensitive information are securely installed. Things (or a Hub or Controller device overseeing a collection of Things) must be able to authenticate a person attempting to (re)configure those Things, and to verify their authorization to do so. Any such authentication system must anticipate the use of proxy personnel, authorized by the owner of a Thing or Environment, because many ordinary people will not have the interest or expertise to configure their Smart Things.

(C2) Things may have multiple owners

Although IoT literature commonly envisions a single Smart Environment in which a single person (or organization) owns and operates all of the Things in that Environment – such as a homeowner who purchases and personally operates all the Things in her home – we anticipate that IoT reality will be far more complex. Consider an apartment dweller, who rents the Environment from a landlord who owns and operates some of the fixed IoT infrastructure, but who deploys some of her own Things in the Environment. (For a more challenging case, consider a hotel or vacation rental in which the occupants change every day, or every week.) To ensure safe operation, these landlord-owned and occupant-owned Things need to co-exist and even cooperate; conflicts in their operation could lead to physical safety risks or personal privacy risks. The trust relationships are complex; the landlord must trust the occupant not to abuse the apartment infrastructure and the occupant must trust the landlord not to collect or expose personal information. Furthermore, cyber-security vulnerabilities in personal Things could become a vector for an external adversary to attack the landlords' infrastructure, and vice versa.

Multi-owner environments should be considered the common case, with due consideration to interoperability, usability, meaningful trust models, robust threat models, and mechanisms for attestation, authentication, and auditability.

(C3) Occupants will move across Environments

In this paper we envision Smart Environments such as homes, schools, offices, vehicles, shops, and other spaces occupied by humans. Humans move, of course, and thus the occupants of any given Smart Environment will change as people come and go; similarly, a person may encounter several Smart Environments during the course of a given day. Guest occupants may not understand what Things exist in the new environment and what risks may be posed by those Things, particularly privacy-related risks. When designing security and privacy mechanisms (and policies) it is thus necessary to recognize that Smart Environments will include occupants that are not the owner/operator of the Things in that Environment; indeed, those occupants may not be aware of (or consent to) the Things' collection of data about occupants. Are there ways to automate notice and consent? (Remember P3P [10]?) Are there mechanisms to automatically disable data collection during a visit by an occupant who has not consented to data collection? Indeed, the notice-and-consent model itself may be completely unworkable. If so, what *practical* solution would allow people to manage their privacy across Smart Environments? Early work has made limited attempts at this challenge [3].

(C4) Things will move across Environments

Indeed, when humans move to a new Smart Environment they may carry or wear Things of their own, suddenly and unexpectedly introducing new Smart Things into the Environment – perhaps an Environment controlled by a different, untrusted owner. The person may expect their personal Things to continue working – which may require those Things to discover and interact with Things already in the environment. Conversely, the Smart Environment may need to discover and vet the newly arrived Things. The migration of Things raises many questions: how do Things discover their new Environment and its Things? How do Things obtain information or other services from that Environment – and know whether to trust them? How do the existing Things discover and determine whether to trust the new arrivals?

These challenges are not limited to personal Things carried by occupants. Staff may move Things from room to room in an enterprise, such as in a hotel, office complex, hospital, or school. The secure configuration and re-configuration of Things, even within a single-owner setting, nonetheless requires one to solve many systems and security challenges.

The arrival of new Things could, if incompatible with the Environment, or insecurely reconfigured, result in failures or inappropriate behavior that cause privacy risks to occupants or damage to Things and the infrastructure.

(C5) Things may transfer to a new owner

People sometimes sell or gift used Things to others. When a Thing is transferred to a new owner, it must be cleaned, deprovisioned, and reconfigured. One might think a 'factory reset' may suffice – but how can owners *verify* that all sensitive information has been securely erased? To ensure safety, the prior owner must be able to verifiably erase cryptographic keys, identity and authentication information, and any personal information about the owner or occupants. The new owner must be able to verifiably ensure the prior owner has no residual access to the Thing, including backdoor or Trojan Horse mechanisms. The new Thing must be securely provisioned for its new owner and new Environment. Improper or incomplete cleaning, deprovisioning, or reprovisioning could result in risks to the old owner or new owner, or incorrect behavior of the Thing – and thus cause harm to either or both.

(C6) Environments may transfer to a new owner

Indeed, sometimes people sell or transfer entire Environments, such as when a homeowner sells her home or a landlord rents an apartment to new tenants. Such changes may require the removal, transfer, or reconfiguration of all Things in that environment. The prior owner will want to ensure that she has removed her Things from the Environment, and securely cleaned and deprovisioned those that remain. The new owner will, as above, want to ensure the transferred Things are safe to use. Indeed, both old and new owners may want a comprehensive inventory of Things in the Environment: not a simple task.

(C7) Things must be discovered and identified

When arriving in a new Environment, a new owner or occupant will want to know about every Thing in that environment: what is it? where is it? who owns it? who operates it? how is it configured? what terms of service apply? what privacy policies apply? At first, this cries out for a standardized discovery protocol that operates on common network media (Wi-Fi, Bluetooth, Zigbee, Ethernet, or powerline networks like X10). And yet, any Thing-discovery protocol or tool will pose privacy risks because guest adversaries may use that tool to invade the privacy of the Environment's owner, or an Environment owner could use such a tool to scan the Things carried by arriving guest occupants. Nonetheless, such a capability has important safety implications beyond the privacy risk. Unknown Things could be incompatible with current activities or future installation of new Things, leading to physical harms or security vulnerabilities. Malicious Things could attack innocent Things or simply be faulty and cause harm; early discovery could allow for problematic Things to be identified and isolated before harm occurs. Clearly, occupants and owners will require this 'inventory' capability even if they do not have the tools or authority to reconfigure every Thing discovered – because this knowledge is the foundation for any attempt to assess and manage their risk.

(C8) Things may fail – and must fail-safe

Smart Things are, in the end, physical devices – and they can fail due to manufacturing defects, mechanical failure, electrical failure, environmental effects, or physical abuse. Their behavior may also be impacted by digital failure, such as network congestion or outages. When Things fail, they may increase risks of harm to owners or occupants – and thus must be designed with graceful failure modes to ensure safety in the face of failure. Systems of Things may need to incorporate redundancy to continue safe, if degraded, operation in the event of component failures.

(C9) Thing vendors may change terms of service

Most Things will be manufactured by companies – and companies change over time. The company may change its Terms of Service, or may be sold to another company. A change in ownership or terms of service may raise new threats to occupant or owner privacy, or new threats to security or safety if the old promises have loosened or disappeared. These risks may be especially severe if the Thing operation requires back-end services provided by the vendor.

(C10) Thing vendors may disappear

Indeed, some companies may simply shut down, or stop supporting a product. Things may become inoperable, or behave incorrectly, without operational back-end services. Things may become vulnerable to newly-discovered exploits if regular firmware updates are no longer available. In the event a Thing becomes unsupported, how are Thing owners and Environment occupants notified? How do they understand the ramifications of the change?

(C11) Things will be thrown away

Digital devices often have a useful life-span of only a few years before they are discarded. As in the case of ownership transfer, above, Thing disposal requires verifiable erasure of personal information, key material, and configuration information. Discarded Things can expose personal information (recorded on the Thing, or accessible via the Thing) or authentication information (stored on the Thing) that could be used by an adversary to extract personal information or to infiltrate a Smart Environment where the Thing was once used. This challenge may be especially difficult when discarding an inoperable Thing – the 'erase' feature may not work – or when discarding an entire Environment, full of Things – where it would be impractical to locate and erase every Thing. Consider, for example, a home that is razed after damage by fire or flood, or a smart car that is a 'total loss' after a terrible accident. One aggressive solution is to generate an electromagnetic pulse that destroys all information stored on all Things within, say, a 10m radius.

(C12) Things will last longer than expected

On the other hand, some devices – especially those embedded in built infrastructure – are used for years or even decades. These Things raise long-term safety considerations such as backward secrecy in the face of newly discovered flaws in crypto or stronger computation, or vulnerability to newly discovered safety or security flaws in the Thing. Indeed, over time it may become increasingly difficult to discover and communicate with old Things, as older network interfaces and protocols are retired from newer computing devices. Although vendors may retire support for their older products, Thing owners may (out of ignorance, complacency, or necessity) continue to operate and depend on them. These challenges raise the potential for physical harm to Things, Environments, or occupants, or privacy-related harms to occupants past or present. What tools can assist Thing owners in managing outdated Things, and managing the risks they pose?

(C13) Everyday people manage everyday Things

Finally, it is critical to realize that many of these Smart Environments will be installed, configured, managed, and decommissioned by everyday people – not by systems administrators or technical support teams. Every one of the above challenges must be achievable without any more than a passing expertise with computing, security, or networking. Thus, it is essential to seek intuitive, usable interfaces that give occupants and owners a clear mental model about what is happening in their Smart Environment, what privacy risks may exist, and how they can configure Things to achieve their goals and meet their personal preferences.

Summary. We face all these challenges today, even with the limited scope and scale of Smart Things currently available. Although not every challenge is relevant to every type of Thing or Environment, we recommend that designers consider all of the challenges and how they may apply to the systems they develop or deploy.

3 RELATED WORK

Due to limited space, we cannot survey the entire literature on safety in IoT or Smart Environments. Instead, we highlight several recent reports on the security, privacy, and safety challenges in the Internet of Things, all of which provide useful perspectives on some of the above challenges. The U.S. National Security Telecommunications Advisory Committee published a 2014 report on the Internet of Things, with an emphasis on IoT in the National Security and Emergency Preparedness infrastructure [5]. The U.S. Department of Homeland Security released a 2016 report on *Strategic Principles for Securing the Internet of Things*, in which they lay out six principles [8]: incorporate security at the design phase, advance security updates and vulnerability management, build in proven security practices, prioritize security measures according to potential impact, promote transparency across IoT, and connect carefully and deliberately. Ahmed et al. presented a survey of IoT and Smart Environments, listing open research challenges [1]. The Computing Community Consortium (CCC) released a 2017 report with useful scenarios involving smart devices in homes and smart devices in hospitals, with nods to security and physical safety, privacy, and usability [2]. They end with a page of recommendations. Finally, Smith published a 2017 book with an overview of the *Internet of Risky Things* [7], including discussion of IoT architectures and application areas; security, identity and authentication; privacy, economic, and legal issues, and the "digital divide".

4 DISCUSSION

It should be clear from the many challenges described above that much more research is needed in order to develop a safe, secure, and privacy-preserving future for the Internet of Things and Smart Environments. Here we identify a few of the key research questions that should be explored to address the above challenges, and present potential directions for solutions where possible.

Risk management (C1-C13). Our definition of *safety*, above, is all about avoiding undue risk of harm. Ultimately, then, safety is about risk management. While one can strive to engineer Things to avoid harm, it is impossible to prevent all forms of failure or attack. Consider the automobile industry: although they strive to make cars better able to avoid accidents, they also make the vehicle safer for passengers in the event of an accident. When developing Smart Things and Environments, we must ask: *How can Smart Things and Smart Environments ensure safety properties even in the face of failure or attack? How are Smart Environment owners/operators made aware of failed or compromised Things?* Smith proposes designing modular systems, which makes it easier to "break off pieces" that cease to work or that are no longer needed [7].

Prioritizing risk (C1-C13). The challenges and requirements vary tremendously for different IoT applications, as do the risks of various forms of harm. *Can we develop a structured model for characterizing and grading the most important risks in a given application, allowing developers to focus design and implementation effort on the most substantial risks? Can such models help occupants or owners to assess and manage their own safety risks?* Perhaps we can look to the automotive or aeronautical industry for examples of risk classification.

Multi-owner, multi-occupant Environments (C2-C3). Many of the above challenges arise because different persons or organizations act as owner, operator, or occupant, creating challenges around trust and privacy management, and leading to potential safety concerns. *What security architecture allows an Environment owner to manage a space with Things that are owned by unknown other persons, or for a Thing owner to manage its relationships with Things owned by others? How is a Thing (or Environment) securely and verifiably transferred to a new owner?* To begin, Things and Environments must be designed with first-class concepts of *owner*, *operator*, and *occupant*, and must recognize they will change over time.

Intermittent connectivity (C8). The backbone of the IoT is the assumed connectivity among Things, and (via the Internet) to backend services. A lapse in connectivity, however, can render critical functionality of Smart Things and Smart Environments inoperable or even dangerous. Smart Environments need to plan for disconnected operation, building in redundancies, alternative controls, and fail-safe modes, similar to planes and automobiles. Thus, we must ask: *How can we architect Smart Things and Environments to be robust to lapses in network connectivity, with an aim to mitigate harm to humans and Things?*

Platform security (C1, C5-C7, C11). Things will need to be provisioned – at the manufacturer or during deployment – with cryptographic material that enables secure communications and remote attestation. The protection of these secrets is challenging, especially for resource-constrained devices; it will be even more challenging in Smart Environments where Things are always-on, networked, and physically accessible to adversaries. Thus, *How can we provide physical security for cryptographic material and computations, and a trustworthy platform for secure computation and remote attestation, in low-resource embedded devices?* Consider emerging microprocessors with embedded trustworthy hardware, and explore transferring these concepts to microcontrollers and embedded systems.

Development of secure embedded systems (C7-C8). If history is any guide, many of the future exploits of Smart Things will take advantage of software vulnerabilities that result from careless programmers working with inadequate attention to security and with inadequate tools – languages, compilers, software verifiers, and testing frameworks. *What tools can assist programmers in developing secure software for embedded systems, and in particular, distributed systems of embedded Things?*

Development of common software infrastructure (C7). Much as the Internet is built on common components that, for example, ensure applications can accomplish secure communications without re-inventing cryptographic algorithms or network protocols, *the Internet of Things needs the development of common frameworks that could provide secure, robust, and usable mechanisms for Thing commissioning, deployment, management, and decommissioning.*

Mobility across Environments (C3-C5). People and Things will be mobile, moving from Environment to Environment, e.g., from home to school to office. These migrations may cause rapid changes in the constitution of Things in an Environment – and of the occupants in an Environment. *How, then, do we architect network protocols and management systems in support of frequent changes in the set of available Things – while maintaining safe and secure operation of the applications dependent on those Things?*

Authenticated data sources (C1-C2, C12). Today we often trust data-driven apps and services without knowing or verifying the data provenance. Given the expected dependence of many Smart Environments on sensors and sensor data, the injection of falsified data at sensors is a major concern. While falsified data is not a new issue – many are familiar with falsified data such as fake reports of healthy activity, and the risk of adversaries tampering with data at rest or in transit – we must consider how questionable data sources might impact the safety of Smart Environments and the humans that occupy them. We ask, *How are data sources authenticated? Once authenticated, how are data sources continually verified as being correct and uncompromised?*

Authenticated humans (C1-C7, C13). Many applications involving Smart Things or Smart Environments will be limited to authorized users, whether those be owners, operators, or occupants. At a minimum, the configuration (or re-configuration) of Things should be limited to authorized persons. *How, then, do Things identify and authenticate their user? How do Smart Environments identify and authenticate occupants, without raising privacy risks? How do Things verify authorization when sensitive actions are requested? How do owners and occupants delegate authority to others who assist in managing Smart Environments – without undue privacy risk?*

Discovery and management mechanisms (C3-C7, C11-C12). Given the anticipated scale of future Smart Environments, owners and occupants need efficient mechanisms to identify and manage their Things and their Environments. *What standardized protocols could enable the discovery and identification of all Things in an Environment?* Once identified, *How are large collections of Things easily established and managed by non-technical humans?* Consider, however, that malicious Things may not respect these protocols, or may exist passively (never transmitting on the network). *How is a proper inventory for all Things in a Smart Environment maintained when some of those Things, perhaps malicious devices, choose to hide or falsify their identity?* One approach could be to develop tools that detect electromagnetic emissions that are characteristic of computational and networked devices.

Unknown lifetimes (C11-C12). Since the lifetime of Things could outlast those responsible for maintaining them, or the software systems used to manage them, we must ask: *What mechanism can help manage Things that outlive their intended lifetimes?* Smith suggests that a device could automatically fail (into a safe state) at a given age, and alert the owners to its need for replacement [7]. If the device has outlasted its owner or manufacturer, however, whom should it contact?

Secure discovery and destruction of Things (C7-C8, C11-C13). When Things (or perhaps entire Environments) need to be discarded, *How does an owner discover all Things needing destruction, and verifiably erase all sensitive information from those Things before they are discarded?* Physical mechanisms may be most intuitive.

Attesting to safety properties (C1-C13). Ultimately, the key question is this: *How can users be assured that their Smart Things and Environments actually provide the safety and security properties they expect? What mechanism can Things use to attest their properties, and what interfaces enable normal humans to believe those attestations?*

5 SUMMARY

The Internet of Things poses great opportunities for Smart Environments in our homes, offices, schools, and beyond. There are many challenges, however, in developing Smart Things and Smart Environments for safe operation, that is, to ensure that they do not pose undue risk of harm to the owners, occupants, or infrastructure of these environments. We encourage readers to consider the challenges we pose, urge developers to design technologies with strong safety and security properties, and call on researchers to address the longer-term needs of this emerging technology.

ACKNOWLEDGEMENTS

This research results from a research program at the Institute for Security, Technology, and Society at Dartmouth College, supported by the National Science Foundation under award CNS-1329686. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the sponsor.

REFERENCES

[1] Ejaz Ahmed, Ibrar Yaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani. 2016. Internet-of-things-based smart environments: state of the art, taxonomy, and open research challenges. *IEEE Wireless Communications* 23, 5 (October 2016), 10–16. https://doi.org/10.1109/mwc.2016.7721736

[2] Kevin Fu, Tadayoshi Kohno, Daniel Lopresti, Elizabeth Mynatt, Klara Nahrstedt, Shwetak Patel, Debra Richardson, and Ben Zorn. 2017. *Safety, Security, and Privacy Threats Posed by Accelerating Trends in the Internet of Things.* Technical Report. Computing Community Consortium. http://cra.org/ccc/wp-content/uploads/sites/2/2017/02/Safety-Security-and-Privacy-Threats-in-IoT.pdf

[3] Apu Kapadia, Tristan Henderson, Jeffrey Fielding, and David Kotz. 2007. Virtual Walls: Protecting Digital Privacy in Pervasive Environments. In *Proceedings of the Fifth International Conference on Pervasive Computing (Pervasive)*, Vol. 4480. Springer-Verlag, 162–179. https://doi.org/10.1007/978-3-540-72037-9_10

[4] Antonio L. Maia Neto, Artur L. F. Souza, Italo Cunha, Michele Nogueira, Ivan O. Nunes, Leonardo Cotta, Nicolas Gentille, Antonio A. F. Loureiro, Diego F. Aranha, Harsh K. Patil, and Leonardo B. Oliveira. 2016. AoT: Authentication and Access Control for the Entire IoT Device Life-Cycle. In *Proceedings of the ACM Conference on Embedded Network Sensor Systems (SenSys)*. ACM, 1–15. https://doi.org/10.1145/2994551.2994555

[5] NSTAC. 2014. Report to the President on the Internet of Things. National Security Telecommunications Advisory Committee. (November 2014). https://www.hsdl.org/?abstract&did=789743

[6] Timothy J. Pierson, Xiaohui Liang, Ronald Peterson, and David Kotz. 2016. Wanda: securely introducing mobile devices. In *IEEE International Conference on Computer Communications (INFOCOM)*. IEEE, 1–9. https://doi.org/10.1109/INFOCOM.2016.7524366

[7] Sean W. Smith. 2017. *The Internet of Risky Things: Trusting the devices that surround us.* O'Reilly. http://www.worldcat.org/isbn/9781491963623

[8] US Department of Homeland Security. 2016. Strategic Principles for Securing the Internet of Things. (November 2016). https://www.dhs.gov/securingtheIoT

[9] Wikipedia. 2017. Internet of Things. (July 2017). https://en.wikipedia.org/wiki/Internet_of_things

[10] Wikipedia. 2017. P3P. (September 2017). https://en.wikipedia.org/wiki/P3P

[11] Judson Wilson, Riad S. Wahby, Henry C. Gibbs, Dan Boneh, Philip Levis, and Keith Winstein. 2017. Trust but Verify: Auditing the Secure Internet of Things. In *Proceedings of the International Conference on Mobile Systems, Applications, and Services (MobiSys)*. ACM, 464–474. https://doi.org/10.1145/3081333.3081342