

Extracted from: <http://picosec.org:8080/security/>

# Security Analysis

The aim of conducting a security analysis for Picosec is to identify the key risks in the IoT space, listing out the vulnerabilities in the internet of things as well as the threat vectors that can exploit these vulnerabilities. This risk identification will help to build a detailed list of security and privacy requirements that need to be fulfilled to secure IoT devices from attack.

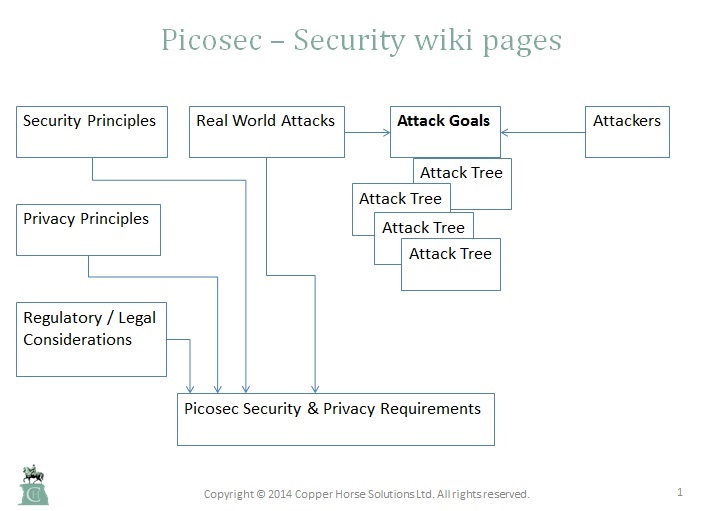
The [threat-based Security Analysis for the Internet of Things](http://picosec.org:8080/security/Threat-Model/Ahmad-Threat-Analyses.md) identifies key use cases namely home automation, health care and automotive that are very relevant to an IoT environment and gives a high level overview of the key threats in such an environment, along with a classification of the attack impact. The security and privacy requirements in the Internet of Things is also discussed in this paper which gives way for a more detailed analysis of the[privacy](http://picosec.org:8080/security/Threat-Model/Privacy%20Requirements.md) and [security requirements](http://picosec.org:8080/security/Threat-Model/Security%20Principles.md) an authenticated, authorised user of an IoT device should expect to have.

The [threat model](http://picosec.org:8080/security/Threat-Model/) lists out the types of [attackers](http://picosec.org:8080/security/Threat-Model/Threat%20Actors.md) in the internet of things and their possible motivation for attack along with the related impact of attack. The identified attack goals are then analysed to build a number of [attack trees](http://picosec.org:8080/security/Threat-Model/Attack%20Trees/).

The [landscape analysis](http://picosec.org:8080/security/Landscape-analysis/) section has an analysis of the [attacks](http://picosec.org:8080/security/Landscape-analysis/Real%20World%20Attacks.md) that have been in the news of late or will be conducted at the Blackhat/ DEFCON conventions. The analysis lists out the identified weaknesses, the implications of these IoT attacks to Picosec, as well as possible mitigations to the problem.

The [market analysis of device enrolment](http://picosec.org:8080/security/Landscape-analysis/Market%20Analysis%20to%20investigate%20enrolment%20of%20IoT%20devices.md) identifies a number of devices in the IoT space, mainly those devices that either lack a user interface or have a very small UI. The enrolment procedure for these devices is discussed for a more detailed understanding of the constraints of devices in the IoT space.

And finally, a security evaluation of the design of [DTLS](http://picosec.org:8080/security/DTLS%20analysis/) and its suitability for use in constrained environments, along with solutions to the possible problems that may be encountered in its use is also included.





# Threat-based Security Analyses for the Internet of Things

bliography:

* ‘IoT.bib’ …

The Internet of Things (IoT) is an emerging paradigm focusing on the inter-connection of things or devices to each other and to the users. This technology is anticipated to become an integral milestone in the development of smart homes and smart cities. For any technology to be successful and achieve widespread use, it needs to gain the trust of users by providing adequate security and privacy assurance. Despite the growing interest of the research community in IoT, and the emergence of several surveys and papers addressing its architecture and its elements, we are still lacking a thorough analysis of the security and privacy properties that are required for a system where the constituent devices vary in their capabilities. In this paper we provide a threat model based on use-cases of IoT, which can be used to determine where efforts should be invested in order to secure these systems. We conclude by recommending measures that will help in providing security and assuring privacy when using IoT.

# Introduction

In the last few years the world has experienced rapid advancement in technology, the likes of which has had a significant impact on our daily lives. The rise of technologies - smartphones, tablets, laptops and PCs has engendered an increase in interconnectedness through time and across the spatial dimension. Contemporary technology has moved beyond fostering only connections between humans, and now facilitates both the linkage of people to things and indeed, things to one another, to achieve a common goal; this being termed The Internet of Things (IoT). IoT is believed to be the next milestone in the technological evolution of the world, it having an expansion rate 270 percent higher than mobile devices in less than six years @Yves2014. Given this, many governments and large corporations have earmarked substantial funding for research on IoT.

IoT is going to have a substantial role in shaping the future of smart cities. From the private user’s perspective it manifests itself in the application of domestic tools at work; for example, systems such as the smart thermostat, smart car, and smart community. Moreover, with regard to the corporate enviornment, IoT will enable automation of work, the provision of smarter environments for employees, and the management of power consumption with the aim of reducing expenses @Buckl2009. IoT is able to achieve the aforementioned through utilisation of other technologies @Kortuem2010 [@Serbanati2011] - for instance, sensors, Radio Frequency IDentifiers (RFIDs), actuators, and smart meters - that are linked together to create a new emergent behaviour where each thing contributes to achieving the desired functionality. A particularly salient example of such an application is a thermostat system that senses the temperature and adjusts itself by learning the behaviour patterns of its users @Nest2014.

The value of IoT could not possibly be overestimated, however it is imperative that thorough consideration be given to all aspects of security and privacy. Indeed, tackling such facets, whilst a challenge, is all the more imperative, as IoT, being the amalgam of a great many individual technologies, many of which may well have flaws with respect to security and privacy, could conceivably be instrumentalised in a sinister and far more threatening manner if there is a failure to afford sufficient attention to the subject matter of this paper.

The complex nature of security in IoT revolves around the fact that, while in itself connecting several technologies together is a great challenge, the system attempts to securely connect devices that are limited in computation, power, and storage. Some of the devices used by IoT can accommodate only very basic security mechanisms, the likes of which are incapable of maintaining the integrity and confidentiality of the users’ data. Moreover, these devices - for instance, sensors, and RFIDs - lack a simple user interface, like an ON/OFF button or status indication, thus presenting a visual psychological limitation for people when it comes to trusting these devices.

Nowadays, privacy has became a hurdle; slowing the advancement of many technologies@Xu2011. Furthermore, it has been shown that trust in a technology diminishes when the latter slanders or exposes the individual @oxford2013 [@Scandal2014; @Best2014], and, recently, many technologies have failed to provide adequate security and privacy mechanisms, thereby causing pain and suffering to those afflicted @Hinduja2010. In order to gain the trust of the public in the Internet of Things, we need to ensure the same failures with respect to privacy and security do not come to pass with this system, by ensuring the appropriate mechanisms to guarantee such things exist from the onset.

In this paper we discuss the Internet of Things from a use cases perspective. The following section provides a general overview of the work done in the field; section 3 details several interesting scenarios which are relevant to today’s world; section 4 discusses a threat model; section 5 provides a security analysis to the IoT devices based on these use cases respectively; section 6 lists security and privacy properties desirable in IoT systems; whilst finally, in section 7 we give a glimpse of the future work we plan to do in this field. In particular, our main contributions are:

* Defining several use cases for the Internet of things,
* Establishing threat modelling as a method for analysing the use-cases defined,
* Formulating a set of desirable security and privacy properties for IoT.

# Related Work

Due to the rising interest in the Internet of things, there have been numerous publications on security and privacy in this context. There are currently a myriad of descriptions of IoT visions, applications, and enabling technologies @Atzori2010 [@Ciscoiot; @Miorandi2012; @Gubbi2013] that briefly address some security and privacy aspects. Atzori et al. @Atzori2010 has discussed the importance of security in IoT context and focused on the security aspects of the elements. In this survey its pointed out that due to the limitation of the devices composing the IoT, and the properties of the current communication protocols, it is very challenging to employ complex security mechanisms. Some devices might not be able to have access control for different users, support sufficient authentication schemes, or even use secure communication channels between devices. However, it is important to keep in mind that the required security measures are application dependent. For instance, in Near Field Communication (NFC), physical proximity is a must for establishing the communication, which makes this technology useful for various applications, due to this property, some applications using NFC might not require a complex security scheme such as encrypted channel. For example, in some instances the users might not care about other people seeing the exchanged data in their presence. In a domestic use for IoT, in order to prevent children from watching TV without adult supervision, the user might not need complex communication protocols and it would suffice to use access control mechanisms only to access the device, or symmetric encryption rather than asymmetric for communication.

The Internet of Things poses many security and privacy challenges@Weber2010 due to its heterogeneous nature. Different research groups have adopted diverse directions for addressing these issues. Roman et al. @Roman2011 presented several technologies in IoT context, discussed current technologies and their feasibility for some IoT devices, and provided a set of security requirements for IoT devices. In a subsequent study, the same group @Roman2013 compared the centralised and distributed architecture of IoT and their implication on security aspects. Moreover, Kozlov et al. @Kozlov2012 discussed security and privacy threats in IoT architecture, using systematic approach to analyse the threats at different levels of the architecture.

Threat models to IoT have been presented by Babar et al. @Meghanathan2010 who gave a general threat model that is not IoT specific, however, can be reflected on it. Nontheless, the field is still lacking a clear reference to the actual threats encountered in IoT, and in what applications security is more crucial. Abie et al.@Abie2012 focused on a risk-based adaptive security in a Healthcare application by taking risk management approach that adopts game theory theme to develop an adaptive security decision-making model. Similarly, Gan et al. @Gan2011 focus on security analysis of the network points and suggested solutions to some problems.

Even though IoT has been out for many years, it didn’t get the sufficient attention it deserves. According to Whitmore et al.@Whitmore2014 not much work has been done on security and privacy in IoT context, and most of the work was focused on the devices as individual entities rather than being part of an IoT system. Despite the various attempts to deal with security and privacy issues in IoT, a holistic analysis and risk assessment is still lacking. Due to the incompleteness of the security and privacy requirements, IoT still needs to overcome this obstacle that may prevent it from becoming widely adopted.

We argue that in order to be able to understand the security and privacy risks behind IoT we should relate them to a specific application, as each scenario bares its own concerns, thus providing us with a clear definition of the threats behind each use-case. In this paper we describe the vision of IoT by providing several use-cases, and use threat-based security analysis method to help us in formulating the security and privacy recommendations to overcome some major challenges in IoT.

# Internet of Things use cases {#sec:use\_cases}

In this section we present three representative IoT use-cases that have a high likelihood of being integrated into our daily routines now and in the near future. We describe how IoT elements, such as sensors, actuator, RFIDs, Internet, Network, and Near Field Communication, can support different applications, and help increase IoT adoption. Analysing the functionality of IoT elements in different scenarios is a method that allows us to perform case-based security analysis, and formulate the security and privacy properties that will support the use of IoT by many users.

## Power Management

One of the most prominent uses for an IoT based smart system is managing power consumption both in the private and industry sectors. In a world where the resources of energy are becoming scarce, it is essential to have such a smart system that will contribute to maintaining these resources.The strength of the power management system is in the ability to manage the execution of different devices while keeping power consumption within allowed boundaries. This can be done by using a smart meter@Venables2007 that supplies the system with real time data to enable scheduling the devices’ operation. For example, the user can sync between two devices, when one device pauses the other resumes execution.\ In a smart house a domestic thermostat system is an essential component to set and control the temperature. It uses a temperature sensor, that can monitor the room’s temperature with reliance to desired properties and send feedback to an actuator to initiate a change when it detects any divergence from these values. This would include setting the temperature to a certain range defined by the user. The thermostat would then adjust its activity to maintain the room temperature within the configured range.

The employment of a network further improves the control of the user and enables managing the thermostat remotely and thus preparing the room temperature for his arrival; by the time the user gets to the house the room is set to a convenient temperature. Many of these functions can be achieved while reducing power consumption. The system can benefit from a location device that is connected to the user’s smartphone and can send signals to turn on/off the system according to the distance from the location device. Another device with even finer control is a movement sensor that identifies the movement and responds accordingly by turning off to improve power consumption when the user is not present in a certain room for a prolonged period of time. In a matter of days the system learns the user’s habits and automates its usage, for example, when waking up in the morning it turns the system on and when going to bed it turns it off.\

## Smart Car

In an automated world, people will no longer need to sit behind a wheel and suffer from driving for hours, by the year 2020 it is believed that people will be able to enjoy a new technology of automatic-driver @Rosenblatt2014. In a modern world, smartphones will be used as an access control to unlock the car@Clark2010 [@Telekom2011], replacing conventional keys, thus solving the scalability problem of having a key for each user. The Near Field Communication is a perfect candidate for this feature due to its short communication range that gives assurance of the user’s physical presence.

Once an authorised user unlocks the car, it can surf the Internet in order to download road maps, connect to the city’s infrastructure to get live updates on traffic, signals from traffic lights, and even report status to contribute to a bigger system like Vehicular Network @Moustafa2009. The car will use this information in order to plan its route to arrive at the destination in the fastest and most economic way. By knowing the time of change in the traffic light, it can adjust its speed so that less fuel is being consumed, and report a more accurate time estimate for arrival.The car will also communicate with the surrounding cars in order to coordinate driving in the street. For example, when a car wants to pass another car it will communicate with its system and arrange the passing in a safe way.\ In addition, the reported increase in unfortunate incidents where children were forgotten in cars; according to Safe Kids Worldwide: every 10 days a child dies from heatstroke in vehicles@Heatstroke2014, encourages the adoption of alert mechanisms such as amovement sensors to identify if a child or an animal was left in a locked car and report to the relevant parties. Finally, in order to make the travelling experience more convenient for the users, they can connect to TV channels at home and watch their favourite shows while travelling.

A smarter car can contribute to a more secure world; it can prevent unauthorised users from driving/using the car, hence it can protect against theft. Only authorised users who belong to a “white list” are allowed to drive a car. Similarly, it would prevent reckless teenagers without a driving license or elderly people from using the car causing damage and loss of lives.

The adoption of smart cars will pass several phases before making an appearance on the streets. A prototype of this system adopted in an airport context where vehicles move between unpopulated buildings will be greatly beneficial to automate the airport’s functionality.

## Smart Healthcare System

As the life span increases and new chronic diseases develop there is a need to provide medical attention to a growing population where certain patients require constant monitoring. However, the current facilities at hospitals and clinics are very limited and cannot accommodate many individuals. Therefore it is essential to develop the capability to follow the health condition of patients either at home or in the hospital when applicable. This can be achieved by using sensors to monitor the patient’s condition and send the report back through the Internet to a system that analyses the obtained data and alerts the suitable staff member, thus allowing the health care system to identify health issues earlier, and respond faster to emergencies. In recent years, similar remote treatments have been introduced in the form of devices like insulin pumps and heart-pace units that are attached to a patient, providing an automated and rapid response when needed.\ In a smart hospital, RFIDs can be used to identify patients, items, and doctors easily and rapidly, e.g in a case when an anonymous person gets in an accident and it is critical to obtain the relevant medical records without any delay. It will also allow the staff to keep track of the doctors’ location to allow for better response time during emergencies. Connecting RFID tags is not limited to people, one of the main issues in many hospitals these days is loss of medications and unauthorised use of expensive medical instruments@Moto2011. Hence, tracking things with RFIDs can reduce these losses and help to track them.

# Threat Model

## Sources of Threats

After discussing the features of IoT and how can they be employed in several scenarios in a smart world, it is now feasible to identify the potential threats they are subject to in the context of the use cases presented in the previous section. There are three main entities that pose risks to the security and privacy in IoT:

1. **Malicious User:** Is the owner of the IoT device with potential to perform attacks to learn the secrets of the manufacturer, and gain access to restrictive functionality. By uncovering the flaws in the system the malicious user is able to obtain information, sell secrets to third parties, or even attack similar systems.
2. **Bad Manufacturer:** Is the producer of the device with the ability to exploit the technology to gain information about the users, or other IoT devices. The manufacturer can expose the user data by selling information to interested parties, or by giving bad security design with many flaws. In addition, in IoT context where different objects connect to each other, a manufacturer can attack another competitors’ devices to harm their reputation.
3. **External Adversary:** Is an outside entity that is not part of the system and has no authorised access to it. An adversary would try to gain information about the user of the system for malicious purposes such as causing financial damage and undermining the user’s credibility. Also, cause malfunction to the system by manipulating the sensing data such as transmitting electromagnetic signals to inject fake data.

## Classes of Attacks Vectors

Classifying the attacks on a system is essential for understanding the risks. We choose to address several categories to identify threats@Myagmar2005. These threats will be considered in more detail in the security analysis of the use-cases presented in section [sec:use~c~ases].

1. **Device Tampering:** IoT devices are tiny devices integrated in other systems such as cars, light switches, TVs, ovens, and others. Some of the IoT devices spend most of the time unattended, thus, they can be easily stolen without being noticed. Once a device falls into the wrong hands, various sets of attacks can be performed such as secret stealing, software manipulation, and hardware tampering. It is important to mention that an adversary can tamper with the device and use it to insert impostor to the system, use the device maliciously or out of its intended functionality.
2. **Information Disclosure:** is the act of revealing information to an entity which does not have permission to see it. This includes accidental exposure, targeted attack, and inference or correlation. An attacker can obtain information by eavesdropping on the network channel, physical access to the device, or through accessing the device over the network.
3. **Privacy Breach:** unlike Information Disclosure, an adversary does not necessarily need to have access to confidential information to learn about the user, the adversary can infer private information from other sources such as meta data.
4. **Denial-of-Service:** refers to the property of being inaccessible when requested by an authorised user. The system must have the ability to continue operating even when some undesired action is being performed by malicious users. This class of attacks can be performed by stealing the device, manipulating its software, or disrupting the communication channel.
5. **Spoofing:** refers to using others’ credential in order to gain access to otherwise inaccessible service. The credentials can be obtained directly from a device, eavesdropping on the communication channel, or phishing.
6. **Elevation of Privilege:** is when an unprivileged user gains privileged access to a device/service. This can be achieved by installing an impostor in the system that pretends to be another device, that has privileged access in the system.
7. **Signal Injection:** is when an attacker inject fake data to the system to change the sensed data, such as transmitting electromagnetic signals to a sensor.

# Attacks Impact

In order to make recommendations on how to secure IoT and to appreciate the severity of the threats it is subject to, it is not satisfactory to list the potential hazards without thorough consideration of their actual impact and likelihood, which will be context dependent. Many previous works focus only on the technical aspects of IoT devices and do not give attention to security in their application, we identified a gap in the literature and we try to help in understanding this gap by taking different approach to analyse security and privacy requirements in IoT. In this section we provide some attacks analysis and address the security and privacy concerns for each device using the use cases from section 3, giving a better overview of where strict security measures should be implemented.

## Actuators

The actuator function in IoT context is equivalent to the write operation in PCs. In a world of things, an actuator can be operated by the user over the network, by receiving signals from other devices, or by being physically triggered by the user.

1. **Security:** An attack on this device can cause damage to the user in different domains. In the power management scenario, unauthorised triggering of the actuator can result in financial loss due to excessive power consumption. The damage can be even more severe in the smart car scenario where a malfunction in the breaks’ actuator can result in loss of lives@Koscher2010. In the smart healthcare system, an actuator can be the trigger for injecting medication to a patient monitored at home, and any mistake or malfunction in this context can result in a wrong dosage of medication which can have fatal impact.

## Sensors

The sensors collect data that is transferred to other components in the system to be analysed and result in a certain response or activity.

1. **Security:** The collected data can be a source of an attack@Eschenauer2002, such as when data is fabricated due to a physical attack, resulting in an unexpected behaviour of other entities in the system. In the power management use case, fake data from the sensors results in a different behaviour by the actuator, thus activating the thermostat at wrong time which will be manifested in financial loss to the user. However, in this system it is unlikely to learn substantial secrets about the user from the sensed data. In the healthcare system, fake data can result in wrong prognosis of the patient, administration of wrong medication that can result in allergic response or even life-risk@Parmar2012 [@Alexander2013]. It could also send fake alerts and cause financial loss, for instance due to sending a medical team to the wrong patient.
2. **Privacy:** The data collected from these devices can reveal information about the user’s habits, even though it might not reveal secrets about the user. For instance, in the power management use case the attacker can learn from basic analysis of the movement sensor data when the user leaves the house, goes to sleep, or wakes up in the morning. In the healthcare system, the signals from the sensors used to report the patients conditions can reveal the medical function of the device, thus reveal private information about the holder.

## RFID tag

The RFIDs involve the use of a reader device to identify a tag. These devices became popular due to their low cost, but still have the ability to track and identify objects. However, this technology raises many security and privacy concerns@Molnar2004 [@Lehtonen2007].

1. **Security:** The limitation in hardware and power of these elements prevent the adoption of sufficient security mechanisms@Weis2004 [@Rotter2008]. For instance, holders of RFIDs tags must not be identified by an attacker with a tag reader, thus, scanty access control mechanisms might lead to information disclosure@Lehtonen2007. In the smart car example, an attacker within a close range of the user might be able to intercept the signals when accessing the vehicle, in which some of these signals can be the credentials of the user. An attacker can use these credentials to steal the car.
2. **Privacy:** A main function of RFIDs is the ability to track. Therefore, this can pose a huge privacy concern, when it is exploited in a bad way@Gudymenko2012. In the Health care scenario, privacy is the main concern for employees when using this technology, since they can be tracked constantly. Also, an attacker can learn about the health condition of patients by standing close and intercepting the signals from the RFID tags@Abie2012 that are used to monitor their condition.

## Network,NFC and the Internet

IoT devices communicate with each other via a network connection. The communication protocols vary according to their function, thus vary in their security and privacy levels. Here we briefly mention the security and privacy behind the communication, and leave more detailed analysis of communication protocols for a future work.

1. **Security:** Due to the heterogeneous environment of IoT, different communication protocols are adopted with different security levels@Hu2010. It is most likely that IoT devices will communicate with each other via wireless channels, that will increase the system’s vulnerability to eavesdropping and mask attacks@Cha2009. An attacker can exploit the communication channel to gather information about the user such as location, credentials, and operation. A typical attack in the Smart car use case can be performed when one car tries to negotiate passing another car with the surroundings, however, receives erroneous information that can lead to chaos, accidents and loss of life. Also, an adversary can modify signals transmitted from devices to cause an unexpected or opposite response at other devices in the system, such as turning on a device instead of turning it off.
2. **Privacy:** The network is the main means of communication between IoT devices, thus posing critical point for information disclosure. For instance, when a smart car accesses a local node to download maps or updated traffic information, an attacker can learn about the destination of the driver. Furthermore, since automobiles can easily access the wide network, and have many elements such as stereo, microphone, and connection to the Internet. Bad manufacturers can use their technology to learn things about the users.

# Desirable Security and Privacy Properties

In this section we integrate the hazards and security analysis from previous sections in order to formulate the security and privacy properties for an IoT system. Including the following properties when developing a framework for IoT is essential to furnish a reliable, appealing, and secure system to many users.

## Security Properties

The ultimate goal is to keep the confidentiality and integrity of the system. For each breach point a different measure should be applied, we link between the security properties to the attacks vectors in section 4 [4.1.\*].

## Actuators, Sensors, and RFIDs {#actuators-sensors-and-rfids .unnumbered}

**SP1:** The device should be tamper resistant against unauthorised re-programing, and passive secret stealing. The device must maintain its security properties, this includes keeping the integrity and confidentiality of the user’s data and the device[4.2.2][4.2.4] when a physical attack[4.2.1] is launched, and prevent denial of service[4.2.4]. However, it should be possible for the user to update the firmware on the device.\ **SP2:** The IoT device must have aprotected storage by keeping the data encrypted to keep the confidentiality of the user information on the device[4.2.2], e.g. using security features of the hardware such as ARM TrustZone @Namiluko2013.\ **SP3:** : An access control mechanisms is needed in each device in order to prevent unauthorised access from compromising the entire system. The adoption of complex access control mechanisms is harder in some of the IoT devices such as sensors and actuator due to the limited storage. However, in some applications access control is a must since compromising one device can compromise the entire system, leading to information disclosure[4.2.5], stealing credentials[4.2.2], and denial of service[4.2.4].\

## Internet,Network, and NFC {#internetnetwork-and-nfc .unnumbered}

**SP4:** The data exchanged between the user and the IoT should be secured to keep the integrity and confidentiality of the user [4.2.2]. When the integrity of the data is compromised, the system acts badly and cause lose to the user.\ **SP5:** Identification and authorisation mechanisms should be employed. Only authorised entities can access the IoT device with different permission to read and write [4.2.4]. The IoT device needs to identify the devices in the system and be able to identify any impostors[4.2.6].\

## Actuators, Sensors, RFIDs, Network {#actuators-sensors-rfids-network .unnumbered}

**SP6:** The system must be available within normal parameters and adapt when some undesired action is performed by malicious user such as physical damage to a device[4.2.4], also the damage reflected from the adversary must have minimal impact on the system.\

## Privacy Properties

The privacy properties counter the privacy breach from section 4, where a malicious entity can learn personal information about the user.\ **PP1:** The data exchanged between a user and the IoT devices should be protected so that an attacker eavesdropping on the communication can’t infer information about the user. An attacker shouldn’t be able to infer the time when the user is present or absent, the user’s identity or any other sensitive information.\ **PP2:** The messages exchanged between IoT devices must not reveal Personal Information Identity (PII) of the user.\ **PP3:** Signals from a device must be sent in a privacy preserving manner so as not to reveal the device’s function since this can reveal information about the user.\ **PP4:** The IoT devices should keep record of the users personal information only when absoultly necessary, and in such a case it should be for a limited time only.\**PP5:** Only data that doesn’t reveal the personal information of the user can be collected such as aggregated data, e.g keeping a record of the number of people in a building, but not data relating to their identity like name, ID, and visual image.\ **PP6:** The user should be made aware what and when data is being captured.\ **PP7:** The user must be able to securely erase all private data from a device, e.g. if the device is to be resold.\

# Future work

Security should not be redesigned for every system, we would like to identify groups of use-cases and requirement frameworks that will lead to architecture, middleware, and libraries. In our future work we aim to build on the security analysis we have performed here and on the features of the different devices in an IoT system in order to develop a security package that can be used by designers for any use case. The objective of developing this package is to offer the users a generalised and complete package that includes a variety of security mechanisms suitable for different devices and different security levels. The designers will then be able to make their personalised combinations of these measures according to the desired application and can even assess the risk level in their design.

As we have discussed earlier, the IoT system encompasses devices with distinct features and limitations. Small devices such as RFIDs, sensors, and embedded devices, suffer from limitation in storage, power, and computation logic. On the other hand, powerful devices like laptops, PCs, and servers are less limited in the applicability of complex security measures. Our package will include the minimal set of functionalities to ensure the basic security mechanism compatible with the limited devices as well as much more sophisticated ones to be employed with the most powerful ones. In addition, intermediate mechanisms can be included to be used at the expense of increasing the costs or power requirement when high level security is required from the more limited devices. It is not a trivial question as to whether such a package is feasible and we aim to explore this further in the near future, where it will be interesting to investigate whether we will need to include a huge leap in the mechanisms employed in order to cover the full range of devices at a variety of security levels.

## Preliminary Risk Assessment

The risk assessment is what will most likely determine the security level for many systems. We provide a preliminary risk assessment for each one of the use cases from section 3, based on the attacks analysis presented in the previous sections. The risk assessment takes into account the severity of the attack as well as the likeliness of its occurrence. Table 1 summarises the different risk levels for each threat in the context of the use cases. These are directly deduced from analysing the security properties of the devices. Based on the risk assessment, different security mechanisms should be adopted using a scenario based approach. The risk assessment will play critical rule in designing IoT systems, however, more extensive study is needed.

**Attacks Vector** Power Management Smart Car Healthcare

Physical Threat 1 2 3 Information Disclosure 2 3 2 Denial-of-Service 1 3 2 Spoofing 1 2 2 Elevation of Privilege 1 2 3

: Risk Assessment

3 - High Risk, 2 - Medium Risk, 1 - Low Risk [tab:my~l~abel1]

# Conclusion

The Internet of things has finally stepped out of its infancy, and is gaining more attention from researchers and industrial communities. In this paper we discuss a vision for the Internet of things and relate it to previous work on security and privacy in IoT context. In particular we present the different approaches that have been taken by many researchers when addressing security and privacy. While many researchers focused on the security and privacy of the devices constituting IoT, few papers addressed threat models, security, and privacy analysis of the system as a whole. In our paper we adopted a threat analysis based approach to present a threat model as a method to analyse the impact of threats in different applications. From the threat model we deduced the security and privacy properties. This assessment will guide future work as to where more substantial efforts should be invested in developing security mechanisms for IoT.



## Privacy Requirements in the IoT

Privacy is one of the most sensitive subjects in any discussion of IoT protection. The data availability explosion has enabled user tracking and profiling, often carried out without consent. Users have access to an unprecedented number of personalized services, and the IoT environment itself would be able to acquire information about users automatically.

The data collected from IoT devices can reveal information about the user’s habits. For instance, in the power management use case the attacker can learn from basic analysis of the movement sensor data when the user leaves the house, goes to sleep, or wakes up in the morning. In the healthcare system, the signals from the sensors used to report the patients conditios can reveal the medical function of the device, thus revealing private information about the holder.

In the health care scenario, privacy is the main concern for employees when using this technology, since they can be tracked constantly. Also, an attacker can learn about the health condition of patients by standing close and intercepting the signals from the RFID tags that are used to monitor their condition.

As European regulators grapple with the challenges and complexities of formulating a technology-neutral Data Protection Regulation, the difficulties of applying “traditional” concepts such as consent, purpose limitation, transparency, data deletion, accountability and security to the data processing activities carried out by an “Internet-ready” kitchen appliance become readily apparent.

The creation of vast amounts of data that are a consequence of the IoT puts pressure on existing data privacy concepts. For example, data protection laws in the EU are based on the fundamental concept that users should be in control of their personal data. However, as we continue to generate more and more data in our daily lives, there is increasing recognition that not only will we never be in complete control over how our data is used but that our control is actually receding.

Privacy generally seeks to protect information that can be attributed to an individual, and to ensure that the collection, use, retention, disclosure and disposal of personal information is carried out appropriately.

**Personally identifiable data** is any data linked to a person or persistently linked to an IoT device: data that can identify a person via personal information or a device via a unique identifier. Included are user-entered data, as well as automatically collected data.

**Sensitive information** is personally identifiable data about which users are likely to be concerned, such as precise geo-location; financial and medical information; passwords; stored information such as contacts, photos, and videos; and children’s information.

### 1. Privacy by design

**Guidelines:**

1. Privacy by design gives users the tools they need to manage their own data. Users can use consent tools that permit IoT devices to access as little or as much of that data as desired.

Privacy by Design means putting the user first and helping them become aware of and manage the privacy implications of using devices in ways that enhance the user’s privacy experience.

**Implementation:**

The key challenge in this area is the lack of a UI on most IoT devices that makes management and communication of privacy implications to users difficult. As most IoT devices have capabilities to be managed and controlled via a management application on a smartphone, manufacturers could use this as a platform for communicating privacy notices to users and allowing them to manage their PI data.

### 2. Transparency and Openness

Transparency is essential since users should know which entities are managing their data and how and when those entities are using it.

**Guidelines:**

1. Users should be provided with clear, prominent and timely information regarding the identity and data privacy practices of various entities with access to their data.
2. They should also be aware of the access, collection, sharing and further use of their personal information, including to whom their personal information may be disclosed, enabling them to make informed decisions about whether to use a particular IoT device.
3. A privacy practice shoud be made available to users before the IoT device is enrolled and any data is collected.
4. An IoT device must not secretly access and collect personal information about users.
5. Users must know who is collecting or using their personal information and how they can contact that entity for more information or to exercise their rights.   
   This must be communicated in a notice.
6. Sharing personal information with third parties.   
   If third parties will collect or have access to user information for their own purposes, the user must be made aware at the earliest opportunity that their data will be shared. Users must be allowed to choose whether to allow this collection, access and use by third parties.
7. If user data will be retained after its use, users must be given information about:   
   a. The periods for which information may be retained and why.   
   b. How the user can exercise specific rights over their information.
8. Where possible, users should have choices about how – and how often – they are reminded about features and functionality that use their personal information.

**Implementation:**

1. Before a user installs and enrolls a device, he or she must be presented with information about:   
   a. What personal information an IoT device will access, collect and use .   
   b. What personal information will be stored. (on the device and remotely)   
   c. what personal information will be shared and with whom.
2. Users should have enough information to make an informed choice about whether to use a device and the consequences of doing so.
3. Help users manage their privacy: Make them aware of a device’s privacy default settings.
4. Give users easy to understand choices and mechanisms for managing their privacy.
5. If a device manufacturer wants to use personal information for a purpose that’s different from what was originally communicated in the notice, then there is a need for this to be explicitly communicated to the user.   
   This can be communicated to the user via the IoT management application.
6. Where technically possible, provide users with opportunities to determine how they will be prompted and how often they will be prompted to make decisions over access to, and use of, their personal information.
7. Users may be given the choice to ‘remember’ their log-on credentials, billing address, email addresses, or location. It is possible to provide blanket one-time prompting for each data type or granular more context-specific prompts.

In an Internet of Things world, where providing users with notice and choice often proves extremely difficult, surprise minimization is becoming a powerful tool businesses can use to help engender trust with consumers. This is about knowing what customers expect from your services and being accountable to them.

Recognizing that the legally required general privacy policy is not always the most effective way to get consumers’ attention, the ‘surprise minimization’ approach means supplementing the general privacy policy with enhanced measures to alert users and give them control over data practices that are not related to a devices’s basic functionality or that involve sensitive information.

As connected cars, appliances and wearables become more ingrained in our daily lives and consumer-facing interfaces less so, surprise minimization will play an even more powerful role. As an owner of a connected refrigerator, one might expect it to print out a grocery list, but you certainly wouldn’t expect that data to be shared with a health or life insurance firm. A solid business should notify and give people a choice when the data being shared or the person it’s being shared with is outside reasonable expectations.

A device must not access user data that isn’t required for it to provide it’s primary service. If, for example, a smart TV is collecting a user’s channel viewing data that is secondary to the device’s functionaly, you need to get a user’s active consent.

**Possible Solutons:**

1. The landing page on an IoT management application is an excellent place to publish key privacy facts, contact information and provide a hyperlink to a more detailed privacy statement. The key is presenting and communicating these details to the user in the absence of a user interface on the device.

### 3. Notice / Disclosure

**Guidelines:**

1. There must be a way for an individual to find out what information about him is in a record and how it is used. This should be specified by the device manufacturer/service provider via a notice.
2. This notice should be delivered just before collecting the data and gives users an opportunity to allow or prevent the practice. Another way to achieve the same end is to make readily available both a short privacy statement highlighting potentially unexpected practices, and privacy controls that allow users to make, review, and change their privacy choices via the device management application.

**Implementation:**

1. Prompt the user and make this information easy to discover and understand.
2. Keep it simple and make it easy to exercise choice.
3. Enable the user to reject the installation or activation if they do not wish their personal information to be used as explained to them.
4. Ensure usability and avoid excessive user prompts that will burden the user. Consider the user experience.

Probably known as the number-one responsibility for any user of personal information, telling individuals about how their data will be employed in an IoT context throws in a few twists. What kind of privacy notice can a toaster provide? How often will our car remind us that it knows where we are? How politely can a running jacket tell me that I’m just trying too hard??? Providing any kind of meaningful notice in this new environment is definitely a big challenge.

But even setting aside the question of how to provide actionable notices, consumers absolutely must be able to find this information somewhere. How can these objects provide just-in-time notice and choice if there is no user interface at all?

When you build compliance around explicit consent notices, it’s inevitable that those notices will become longer, all-inclusive, heavily caveated and designed to guard against risk. Consent notices become seen as a legal issue, not a design issue, inhibiting the adoption of Privacy by Design development so that—rather than enhancing user transparency, they have the opposite effect.   
source:<https://www.privacyassociation.org/privacy_perspectives/post/a_brave_new_world_demands_brave_new_thinking>

### 4. Data Minimisation and Retention

**Guidelines:**

1. The collection of personally identifiable data should be minimised for uses not related to the device’s basic functionality, and the retention of such data should be limited to the period necessary to support the intended function or to meet legal requirements. This data should then subsequently be deleted or rendered anonymous.
2. Only the minimum personal information necessary to meet legitimate business purposes and to deliver, provision, maintain the primary function of a device should be collected and otherwise accessed and used.
3. The collection of sensitive information must be limited.
4. Data that can be used to identify a user or device should not be retained beyond the time period necessary to complete the function for which the data was collected or beyond what was disclosed to the user.
5. Procedures for deleting personally identifiable user data that you no longer need must be adopted and continually updated.
6. Set retention and deletion periods.   
   Personal information that is to be retained must be subject to retention and deletion periods that are justified according to clearly identified business needs or legal obligations.

**Implementation:**

1. Think about what personal information you need and then justify it. Is it really necessary? Are you required to collect it, share it or keep it to meet a business need or legal obligation?
2. Use personal information in ways users would expect when they made a decision to install and use an IoT device.
3. Justify the collection and retention of personal information according to identified business needs or legal obligations. Set a policy and implement it at a technical and business process level.
4. Once personal information is no longer required to meet a specific legitimate business purpose or legal requirements/obligations, it should be destroyed or anonymised.
5. Truly anonymous data may be retained indefinitely. To anonymise data, remove any information that could be used to identify a specific individual, ensuring it is not possible to re-identify the individual, and ensure that the data cannot be related to a single, unidentified individual by unique identifiers.

Going back to the Smart TV example, having the TV log every time a user changes the channel, may be acceptable, if at all. But having the TV scan all shared files on the home network would definitely fall outside any legitimate need and is a violation of user privacy.

### 5. Informed Choice / Consent

**Active consent:** This means a user is given a clear opportunity to agree a specific and notified use of their personal information. Active consent would apply to secondary non-obvious use of a user’s personal information such as a device requesting a user’s location where such data is not necessary to the functioning of the device. Active consent must be captured in a way so that consent is not the default option.

**Guidelines:**

1. There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
2. Intermediaries and platforms should only monitor their customers on affirmative opt-in basis absent a compelling operational necessity. Originally called “Secondary Usage”, this principle seeks not only to give an individual a voice as to whether or not PI is shared with others by offering an “opt out,” but also is intended to prevent inappropriate use of the data.

**Implementation:**

1. Where necessary, gain the user’s active consent.   
   This is the collection or use of personal information not necessary to the device’s primary purpose.
2. Where it is necessary to get active consent, users should be made aware of:   
   a. how long a consent is valid   
   b. how they can manage any consent given by them   
   c. the consequences of withholding or withdrawing their consent.
3. Users must be able to withdraw consent by simple and efficient means, without any undue delay or undue cost.

**IoT example:**

Applications that track a user’s location such as a wearable fitness tracker may not collect location for other purposes — for example, targeted advertising or analytics —unless the user gives their active consent.

LG Smart TVs, for example, were found to be reporting back to LG every time the user changed the channel. The TVs were also scanning all shared files on the home network and sending a running tally of those back to LG as well. The company allegedly offered an opt-out of “Collection of watching info” in its options menu, but apparently toggling the opt-out didn’t actually do anything. (source: [www.doctorbeet.blogspot.co.uk/2013/11/lg-smart-tvs-logging-usb-filenames-and.html])

This, in turn, brings up the question of whether home appliances should be monitoring consumers and reporting everything back to manufacturers by default? This sort of monitoring is particularly invasive. It monitors how consumers use all the various services accessed through that intermediary (such as websites, apps or here, TV channels).

As technology becomes ever more complicated, so it becomes ever more likely that consumers won’t really understand what it is they’re consenting to anyway, no matter how well it’s explained. It’s also a safe bet that users will simply ignore any notice that stands between them and the service they want to receive.   
source: <https://www.privacyassociation.org/privacy_perspectives/post/a_brave_new_world_demands_brave_new_thinking>

### 6. Purpose and Use

**Guidelines:**

1. Inform the user that personal data will be collected and give them the choice of active consent.
2. The access, collection, sharing, disclosure and further use of users’ personal information shall be limited to meeting legitimate business purposes.

**Implementation:**

1. If an IoT management application will retain a history of a user’s personal data, such as health data gathered by a fitness tracker, the user must be told about this and also how long the data will be retained and why. Users must give their active consent to retain a history linked to them as unique individuals and must be able to review and delete the history.
2. If users will receive advertising or sponsored results based on their collected stats, they must be provided with clear notice that the device is ad-supported. If users will receive advertising or sponsored results based on the stored history of that user’s health statististics, users must provide their active consent.

This may be a little difficult given that most IoT devices have a very small to non-existent UI. Working on this problem will be an important objective for device manufacturers and service/application providers.

1. If an IoT management application continues to collect, use or share collected data during operation of the device or after a user has stopped using the device;   
   a. Users must provide active consent to the continued operation of the data collection and should be able to set the level of granularity of the data collected.   
   b. The management application must include a means that alerts the user that the data collection continues to operate.
2. The device must provide easily accessible settings that allow the user to immediately turn data collection on or off.
3. When data collection has been activated, there must be a clear and prominent indicator of this.
4. If the device shares this gathered personal data of a user with other devices or services:   
   a.There must be a disclosure identifying and providing a link or other means to access the third party device or application.   
   b. Users must provide active consent to this data sharing.   
   c. Users must be able to easily manage these third party devices for example, to withdraw consent where desired.

**Possible Solutions:**

1. A symbol could be used to indicate that an IoT device is actively accessing a user’s data to enhance the user’s awareness and provide the opportunity to actively manage their privacy.   
   This would be subject to the device having some sort of UI.
2. Alternatively, users could be sent periodic messages via the IoT management application or alerted via other means(mail sent to the user account for eg) that their personal data is being tracked and collected.

**IoT Example:**

If a Smart TV is collecting user data such as the channels that have been accessed, there is probably no need to provide the user with additional privacy information or to obtain their active consent. However, if the device retains applications used and other contextual information about a user’s requests in order to build a profile and target the user with advertising at a later stage, then the device would need to tell the user about this and get their active consent before the user’s information is collected and used for these purposes.

### 7. Respect for User Rights

**Guidelines:**

1. Users should be provided with information about, and an easy means to exercise, their rights over the use of their personal information.
2. Users should have control over data practices that are not related to an IoT device’s basic functionality or that involve sensitive information.

### 8. Accountability and Enforcement

**Guidelines:**

1. Assign responsibility for ensuring end-user privacy is considered and delivered throughout the product lifecycle and through applicable business processes.
2. Provide users with a solution to enable them to report problems/bugs found with a device that may breach the privacy of their personal information.

**Implementation:**

1. Each entity that collects personal information about users must ensure a company representative is assigned the responsibility for ensuring end-user privacy is built into IoT devices.
2. Any IoT device manufacturer or service provider is accountable for complying with applicable laws and with their general privacy policy and any privacy notices that they provide.
3. There is also a pressing need for someone in the organization to be responsible for reviewing the general privacy policy whenever the device is updated or when business practices change. This person should also maintain an archive of previous versions of the policy, maintain rules for limiting internal access to personally identifiable user data, act as the point of contact for privacy questions and comments, and stay informed of new privacy laws and regulations.
4. Users must be able to report problems with devices or the device platforms themselves. Users must be provided with information explaining how they can report any issue that they face or bug they suspect, or which are found to breach the privacy and security of their personal information. Procedures should be established and maintained to deal with such reports and address any specific threats and risks.

**Possible solutions:**

* Provide a short statement and link on the IoT management application landing page, and or your corporate website. Clearly signpost this. If you collect email contact addresses (with permission) you could also email that information to users.

### 9. Access

**Guidelines:**

1. There must be a way for an individual to correct or amend a record of identifiable information about himself.
2. Individuals must be able to find out what personal information a company has on file about them, and how they can gain access to it so that data in error can be corrected or removed.

**Implementation:** Users should have access to the personally identifiable data that the app collects and retains about them.   
This can be made available via the IoT management application.

There’s a general notion in privacy that individuals should have a right to access their information—indeed, this right is hard-coded into EU law. But when so much information is collected—and across so many devices—how can we provide individuals with meaningful access to information in a way that is not totally overwhelming?   
source: <https://www.privacyassociation.org/privacy_perspectives/post/information_pollution_and_the_internet_of_things>

### 10. Security

**Guidelines:**

1. Personal information must be protected, using reasonable safeguards appropriate to the sensitivity of the information. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.
2. Authenticate users where possible using risk-appropriate authentication methods.

**Implementation:**

1. Generally, PI is categorized, and thus secured, at the highest level, requiring strong authentication, encryption, and stringent controls over physical documents.
2. This is done by using security safeguards to protect personally identifiable data from unauthorized access, use, disclosure, modification, or destruction.   
   These safeguards should include, but not be limited to, the following:   
   a. Access control of personally identifiable user data on a need-to-know basis.   
   b. Use of encryption in the transit and storage of personally identifiable data.
3. Adopt technical measures and business processes to prevent the misuse or corruption of personal information.
4. Where a device creates or collects personal information considered sensitive, such as log-on details, SSIDs, financial details, such information must be stored and transmitted in a secure manner.

**References:**

1. <http://www.gsma.com/publicpolicy/privacy-design-guidelines-for-mobile-application-development>
2. <https://privacyassociation.org/news/privacy-perspectives/>



## Use cases

**1. Home energy**  
**2. Telematics**  
**3. Health care**

### 1. Availability

**Attack Goal:** Denial of service attack on IOT device

There are a wide number of DoS attacks that can be launched against the IoT. Beyond traditional Internet DoS attacks that exhaust network resources and bandwidth, the actual wireless communication infrastructure of most data acquisition networks can also be targeted (e.g. jamming the channels). Malicious internal attackers that take control of part of the infrastructure can create even more mayhem.

A DoS attack can be carried out in 3 ways:

1. By attacking the network and taking a device off the grid. An example of this would be cutting a connecting power cable.
2. By disrupting the communication channel and interrupting communication between devices. This could be achieved by a signal jamming attack or an IP flooding attack.
3. By physically removing a device from the network or destroying it. This would include theft of the device.   
   In this attacker model, active attackers usually lack technical knowledge, and can only hinder the provisioning of IoT services by destroying the actual ‘things’. This is a realistic attack in the IoT context, because things might be easily accessible to anyone (e.g. a street light).

**Impact:**

**a. Home:** In the case of a power management system, an attack on the availability of the system can cause significant errors in billing depending on the downtime.

If one considers the case of a home energy control system, an attack on a water control system could have potentially serious implications such as flooding of the targeted home.

**b. Telematics:** A DoS attack on an automotive control system can lead to traffic chaos and has serious threats to personal safety. A signal jamming attack can cause a disruption in the communication between connected cars and the controller, leading to potential loss of life.

**c. Health Care:** An attack on the availability of devices or automated drug administration in a medical centre has life threatening implications. For example, an attack on a pacemaker that is connected to the local network in a hospital to enable monitoring by a doctor, could lead to loss of life.

### 2. Integrity

**Attack Goal:** Modification of data

Device data can be modified either in transit between two devices or a device and a centralised update system, or it could be modified whilst in storage.

**Impact:**

**a. Home:** Modification of device data impacts, for example, the billing for the energy used by the device. An owner of such a system could stand to gain by modifying energy consumption data in the system. Data, such as updates that are being sent from a centralised control system to a home IoT device, could also be modified with consequences, such as improper functioning of the system.

**b. Telematics:** Modification of data, such as traffic patterns, transmitted between connected smart cars has fatal implications and could lead to traffic congestion, or worse - an accident.

**c. Health Care:** Modifying device data captured by health care monitoring devices, such as a pacemaker, can cause a physician to misdiagnose, prescribe the wrong drugs or administer unwarranted care.

### 3. Confidentiality

**Attack Goal:** Theft/Disclosure of data

Passive attackers can target various communication channels (e.g. wireless networks, local wired networks, Internet) in order to extract data from the information flow. An attacker that gains access to a particular infrastructure will be able to extract the information that circulates within that infrastructure.

Instead of things, active attackers can also target other infrastructures that store information, such as data processing or data storage entities. Most adversaries will aim to target systems that provide the biggest payoff, and central entities fall under this category – they store, manage, and process a huge amount of information.

**Impact:**

**a. Home:** If the device data is breached either in storage or in transit, it could constitute a breach of privacy and disclosure of sensitive data. This data could be analysed on the fly or it could be stored and used later for further attack. (Such as for a replay attack)

Data that has been intercepted can be studied for patterns or to gain further information about the functioning of the system. This information could be used for further attack, either a physical attack conducted locally or a remote attack.

Device data gathered from an organisation could also be disclosed for financial gain.

**b. Telematics:** Protecting the confidentiality of data in a telematics system may perhaps not be as important as protecting the integrity of the data.

**c. Health Care:** Confidentiality is of utmost importance in the health care space and sensitive medical data of an individual, if breached, would not only be a breach of privacy, but would also attract legislative and regulatory attention.

### 4. Authenticity

**Attack Goal:** Spoofing of authorised user privileges

If a malicious user gains access to an IoT device, he could possibly manipulate device data or spoof a false alert back to the user.

A malicious user, either an authorised user with limited access or an unauthorised user, could manipulate device data by spoofing user privileges to gain access to the system and then perform a host of attacks.

**Impact:**

**a. Home:** An attacker, who gains access to a device on the local home network, can use the access to spoof false alerts to a user or disable actual alerts in the case of a home alarm system.

**b. Telematics:** False authentication in a telematics control system enables an attacker to mess with the traffic signals, causing traffic congestion or accidents. An attacker who gains control of a controller area network(CAN) in a car can cause serious problems for the user of that vehicle, such as by messing with the brakes or steering wheel of the car.

**c. Health Care:** An attacker who is falsely authenticated into the system can conduct an escalation of privilege attack to take control of medical equipment on the network or maybe even use this access to modify or delete medical record data.

### 5.Non-Repudiation

**TBD**



### Authorised user with limited access

**Motivation for Attack:**

An authorised user of the system may be bribed to perform an attack on the system or he may have an ulterior motive of his own, such as financial gain. A classic example of this would be a home user who manipulates an energy meter to avoid paying a utility bill.

Such a user may not have access to modify device data if controls have been put into place. This user can launch an attack on the system by using an entry point into the system for further escalation of privilege.

### Authorised user with admin privileges (Super user/root)

**Motivation for Attack:**

Such a user would have an easy way into the system and would not need to bypass any controls. This user may be bribed, socially engineered or blackmailed into launching an attack on the system or could do it for personal financial gain or out of revenge.

### Unauthorised user within the system

**Motivation for Attack:**

An unauthorised user within the system is someone who may have physical access to the network of IoT devices without a legitimate need for it. This attacker can leverage his access to the system to launch an attack or can be bribed/blackmailed/socially engineered into doing so.

### Unauthorised user outside the system

**Motivation for Attack:**

This is a typical attacker with no legitimate access to the network. The motivation for such an attacker would be financial gain, revenge, or to use the attacked system as a launch pad for further attacks of connected systems.



## Structured Analysis

Classsification and analysis of documented IoT attacks

## - Attacks in the news

### 1. Hack turns Belkin baby monitor into iPhone-controlled bugging device

**Domain:** Home

**Description:** A vulnerable wireless camera of a baby monitor was hacked enabling the attacker to monitor people in the room.

**Vulnerabilities:**

1. One-time access is the sole determinant for authenticating a device

* After initial connection of the WeMo baby monitor to a home Wi-Fi network, and access from an iPhone/iPad app over the same network, the iPhone has unfettered access to all audio picked up by the monitor. Access to the home Wi-Fi network isn’t necessary for the app to work after initial setup; all conversations within earshot of the monitor can be tapped as long as the iPhone or iPad has an Internet connection. This gives an attacker remote access to the monitor even halfway across the world. All an attacker has to do is get access to the home Wi-Fi network just once.

1. Lack of password authentication for accessing the monitor.
2. The devices operate on the premise that they’re not running in an environment where even one connected device is compromised. This essentially means that the security of a WeMo monitor depends on securing the home Wi-Fi network password.
3. The same mechanism that authorizes an iPhone that connects to a WeMo even once can be abused by malware to give virtually any Internet-connected device remote bugging capabilities.   
   - It was found that it is trivial for any computer that is already infected to obtain the credentials to tap the audio feed of a WeMo baby monitor connected to the same home network.
4. A weakness in another Belkin product, the Belkin Wi-Fi NetCam, was also found. While the NetCam requires a password to access video feeds, even by users on the same Wi-Fi network, the password is transmitted in plaintext to a server at the IP address 66.160.133.67. This once again makes it trivial for machines already infected with malware to retrieve the password and tap in to the video feed.

**Implications for MXD:**

1. Need for securing the mobile device the baby monitor connects to.
2. Securing the network perimeter.
3. Need for regular firmware updates.
4. Implications of using default passwords.
5. Intrusion of privacy and threats to personal safety.
6. Possible entry point into network for spread of malware, launch of further attack.

**Mitigations:**

1. The perimeter strategy to security is ineffective. The endpoint devices must strive to protect their own stack rather than rely on their network segment being completely trustworthy.
2. A smartphone or any other devce connecting to the home network should be authenticated upon each access.
3. All devices on the home network should be password protected.
4. Ensure adequate encryption of credential data in storage and transit.

**Source:** <http://arstechnica.com/security/2013/10/hack-turns-belkin-baby-monitor-into-iphone-controlled-bugging-device/>

### 2. Belkin WeMo smart home networks in danger of hacks

**Domain:** Home

**Description:** Researchers warn that more than 500,000 home automation devices have vulnerabilities that would allow attackers to remotely take control of thermostats, lighting, sprinkler systems, and more. The reserachers uncovered several vulnerabilities in Belkin WeMo devices, which would let hackers gain access to home networks and remotely control Internet-connected appliances.   
Many of Belkin’s WeMo home automation products let users build their own smart home solutions by adding Internet connectivity to any device. Once connected, users can control their appliances with a smartphone from anywhere in the world. However, hackers could also get into these networks.

**Vulnerabilities:**

1. Not enough encryption controls built in.
2. Weakness that allows hackers to impersonate Belkin’s encryption keys and cloud services to push malicious firmware updates and capture credentials at the same time.
3. No password set on telnet with root access.
4. Private undocumented web interface.
5. Public hard coded username and password.

**Fixed vulnerabilities:**

1. WeMo API server updated to prevent an XML injection attack from gaining access to other WeMo devices
2. WeMo firmware updated with added SSL encryption
3. Elimination of storage of the signing key on the device
4. Serial port interface password protected to prevent a malicious firmware attack.

**Implications for MXD:**

1. Ease of monitoring and conrolling home networks.
2. Malicious firmware updates can be used to gain access to other devices, like laptops and smartphones.
3. Motion sensors used by WeMo devices can be used by an attacker to remotely monitor occupancy within the home.
4. Belkin’s WeMo home automation products let users build their own smart home solutions by adding Internet connectivity to any device leading to an increased possibility of attack.

**Mitigations:**

1. Proper configuration
2. Proper crypto implementation (most hacks attack the implementation of the crypto algorithm)
3. Eliminate storage of keys on device
4. No password set on telnet with root access
5. Password protect the home Wi-Fi network
6. Avoid using default username and password

**Source:**

1. <http://www.cnet.com/uk/news/belkin-wemo-smart-home-networks-in-danger-of-hacks/>
2. <http://disconnected.io/2014/04/04/universal-plug-and-fuzz/>
3. <http://disconnected.io/2014/04/16/new-belkin-wemo-module/>

### 3. Hacker will expose potential security flaw in 4 million hotel room keycard locks

**Domain:** Home

**Description:** Vulnerabilities discovered in hotel room locks from the manufacturer Onity indicate that with a few hacker tricks and a handful of cheap hardware, the DC power port under the keycard lock might offer access to your room just as completely as your keycard.

Using an open-source hardware gadget built for less than $50, an attacker can insert a plug into the DC port, bypass the card reader, and open the Onity door lock in a matter of seconds.

The exploit works by spoofing a portable programming device that controls a facility’s locks and sets which master keys open which doors. The portable programmer, which plugs into the DC port under the locks, can also open any door, even providing power through that port to trigger the mechanism of a door lock in which the battery has run out.

**Vulnerabilities:**

1. The system’s vulnerability arises from the fact that every lock’s memory is entirely exposed to whatever device attempts to read it through that port.
2. The cryptographic key that’s required to trigger the door lock’s open mechanism is also stored in the lock’s memory, accessible by the spoofed portable device.
3. Use of a weak encryption scheme that allows an attacker to derive the “site code”–a unique numerical key for every facility–from two cards encoded one after another for the same room.   
   By reading the encrypted data off of two cards and testing thousands of potential site codes against both cards until the decoded data displays a predictable interval between the two, an attacker can find the site code and use it to create more card keys with a magnetizing device. But given that he can only create more cards for the same room as the two keys he’s been issued, that security flaw represents a fairly low risk compared with the ability to open any door arbitrarily.

**Implications for MXD:**

1. Intrusion of privacy and threats to personal safety.

**Mitigations:**

1. Protection of lock memory and cryptographic keys storeed therein.
2. Use of adequately secure encryption schemes.

**Source:** <http://www.forbes.com/sites/andygreenberg/2012/07/23/hacker-will-expose-potential-security-flaw-in-more-than-four-million-hotel-room-keycard-locks/>

### 4. Hacking into Internet Connected Light Bulbs

**Domain:** Home

**Description:** LIFX bulbs connect to a WiFi network in order to allow them to be controlled using a smart phone application. In a situation where multiple bulbs are available, only one bulb will connect to the network. This “master” bulb receives commands from the smart phone application, and broadcasts them to all other bulbs over an 802.15.4 6LoWPAN wireless mesh network.

In the event of the master bulb being turned off or disconnected from the network, one of the remaining bulbs elects to take its position as the master and connects to the WiFi network ready to relay commands to any further remaining bulbs. This architecture requires only one bulb to be connected to the WiFi at a time, which has numerous benefits including allowing the remaining bulbs to run on low power when not illuminated, extending the useable range of the bulb network to well past that of just the WiFi network and reducing congestion on the WiFi network.

**Device Specifications**

802.15.4 6LoWPAN wireless mesh network of bulbs that connect to a Wi-Fi network via a master bulb that receives commands from a smart phone application.

The PCB is made up primarily of two System-on-Chip (SoC) Integrated Circuits (ICs): a Texas Instruments CC2538 that is responsible for the 6LoWPAN mesh network side of the device communication; and a STMicroelectronics STM32F205ZG, which is responsible for the WiFi side of the communication. Both of these chips are based on the ARM Cortex-M3 processor.

**Details of exploit**

In order to monitor and inject 6LoWPAN traffic, a peripheral device which uses the 802.15.4 specification was used - ATMEL AVR Raven installed with the Contiki 6LoWPAN firmware image. This presents a standard network interface from which to monitor and inject network traffic into the LIFX mesh network.

The protocol observed appeared to be, in the most part, unencrypted. This allowed the researchers to easily dissect the protocol, craft messages to control the light bulbs and replay arbitrary packet payloads.

Monitoring packets captured from the mesh network whilst adding new bulbs, they were able to identify the specific packets in which the WiFi network credentials were shared among the bulbs.   
- The on-boarding process consists of the master bulb broadcasting for new bulbs on the network. A new bulb responds to the master and then requests the WiFi details to be transferred. The master bulb then broadcasts the WiFi details, encrypted, across the mesh network. The new bulb is then added to the list of available bulbs in the LIFX smart phone application.

Further analysis of the on-boarding process identified that we could inject packets into the mesh network to request the WiFi details without the master bulb first beaconing for new bulbs. Further to this, requesting just the WiFi details did not add any new devices or raise any alerts within the LIFX smart phone application.

An analysis identified that an AES implementation was being used. Which meant that if the pre-shared key can be obtained from one device, it can be used to decrypt messages sent from all other devices using the same key. In this case, the key could be used to decrypt encrypted messages sent from any LIFX bulb.

**Vulnerabilities:**

1. The protocol, in most part, was unencrypted, allowing for easy dissection and analysis of the protocol and subsequent packet injection into the network traffic.
2. Packets could be injected into the mesh network to request the WiFi details without the master bulb first beaconing for new bulbs. Further to this, requesting just the WiFi details did not add any new devices or raise any alerts within the LIFX smart phone application.
3. Armed with knowledge of the encryption algorithm, key, initialization vector and an understanding of the mesh network protocol an attacker could inject packets into the mesh network, capture the WiFi details and decrypt the credentials, all without any prior authentication or alerting of presence.

**Patched Vulnerabilities**

The fix, which is included in the new firmware encrypts all 6LoWPAN traffic, using an encryption key derived from the WiFi credentials, and includes functionality for secure on-boarding of new bulbs on to the network.

**Implications for MXD:**

1. Obtaining WiFi details by packet injection without prior authentication.
2. Possible entry point into network for spread of malware, launch of further attack.
3. Ability to cause chaos(blackouts).

It should be noted, since this attack works on the 802.15.4 6LoWPAN wireless mesh network, an attacker would need to be within wireless range, ~30 meters, of a vulnerable LIFX bulb to perform this attack, severely limiting the practicality for exploitation on a large scale.   
Source: <http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/>

**Mitigations:**

1. Provision to prevent packet injection into the mesh network to request the WiFi details, without the master bulb first beaconing for new bulbs.
2. Adequate encryption of the 6LoWPAN traffic.

**Source:**

1. <http://www.contextis.co.uk/blog/hacking-internet-connected-light-bulbs/>
2. <http://arstechnica.com/security/2014/07/crypto-weakness-in-smart-led-lightbulbs-exposes-wi-fi-passwords/>

### 5.Of course hackers made your smart fridge and TV send malicious emails

**Domain:** Home

**Description:** Waves of malicious email, typically sent in bursts of 100,000, three times per day, targeting enterprises and individuals worldwide were seen. Of those, more than 25% originated from Internet of things devices that were hacked for the purpose, instead of traditional “laptops, desktop computers or mobile devices.” No more than 10 emails were initiated from any single IP address, making the attack difficult to block based on location

In this case, hackers broke into more than 100,000 everyday consumer gadgets that were connected to the internet, such as home-networking routers, connected multimedia centres, televisions, and at least one refrigerator.

The botnet, which included Smart TVs and smart fridges, delivered more than 750,000 malicious emails. Hackers were apparently able to also compromise routers and multimedia centres connected to the web to deliver the attacks.

**Vulnerabilities:**

1. Misconfiguration and the use of default passwords left the devices completely exposed on public networks, available for takeover and use.
2. These devices are typically not protected by the anti-spam and anti-virus infrastructures.

**Implications for MXD:**

1. Use of devices in the home as bots in delivering a larger cyber attack

**Mitigations:**

1. Proper device configuration and use of strong passwords
2. Possibility of built-in anti-virus?

**Source:** <http://bgr.com/2014/01/20/smart-tvs-fridge-hacked/>

### 6. The gadget that can hack any CAR: Terrifying £12 tool can remotely control headlights, locks, steering and even brakes

**Domain:** Automotive

**Description:** Cars that come with built-in software running on an operating system are vulnerable to attack. The CAN Hacking Tool (a gadget that is smaller than a mobile phone) has four wires that are attached to the different outputs of a car’s Controller Area Network. The device can be fitted to any car’s Controller Area Network ‘within minutes’ and run malicious code through the vehicle’s system, gaining control of the locks, steering and brakes.

**Vulnerabilities:**

1. Vulnerabilities in the CAN bus, the heart of the car that communicates with everything from the windshield wipers to the engine.
2. Lack of adequate authentication.
3. The computer code in cars is outdated. It’s similar to the on/off switches used in industrial controls. It’s easily manipulated.
4. Internet connectivity means that physical access will not be needed to hijack control of a car.

Car software is not built to the same standards as, say, a bank application. Or software coming out of Microsoft.   
Source: <https://sohommajumder.wordpress.com/tag/car-hacking/>

**Implications for MXD:**

1. Ease of bypassing encryption and obtaining control of the car’s Controller Area Network
2. Physical security implications of an attacker being able to disable the brakes, lock the car doors and disable the alarm.
3. Bluetooth bugs in the system which can be exploited to send remote code executions from a mobile device.

**Mitigations:**

1. Built-in firewalls to prevent malicious tampering.
2. Adequate authentication.

**Source:**

1. <http://www.dailymail.co.uk/sciencetech/article-2553026/The-gadget-hack-CAR-Terrifying-12-tool-remotely-control-headlights-locks-steering-brakes.html>
2. <http://money.cnn.com/2014/06/01/technology/security/car-hack/>

### 7. When ‘Smart Homes’ get hacked: I Haunted a complete stranger’s house via the internet

**Domain:** Home

**Description:** Compared with the houses many of us grew up in, smart homes are intellectual giants. With these homes, smartphones can control everything from the security system to the television, and doors can be unlocked with the touch of a fingerprint. In a hack on eight random homes, sensitive information was revealed – not just what appliances and devices people had, but their time zone (along with the closest major city to their home), IP addresses and even the name of a child.

**Vulnerabilities:**

1. Ability to see all of the devices in a home and control them.   
   - These systems are crawl-able by search engines.
2. Lack of authentication (usernames and passwords not required by default).   
   - No authentication between the handheld and any of the control commands.   
   - No authentication once access to Wi-Fi network has been gained.
3. Revelation of sensitive information- time zone (along with the closest major city to their home), IP addresses and even the name of a child.
4. Lack of authentication meant that anyone who figured out the IP address for vulnerable systems could get access to and control of people’s homes.
5. Storage of device configuration in the cloud.

**Implications for MXD:**

1. Ease of disabling alerts and creating fake alerts.
2. Physical security implications- burglary target.
3. Ability to turn attacked homes into haunted houses, energy-consumption nightmares, or even robbery targets. Opening a garage door could make a house ripe for actual physical intrusion.
4. Enough information to link the homes on the Internet to their locations in the real world.

**Mitigations:**

1. Requirement for password protection by default.
2. Secure storage of device configuration in the cloud.

**Source:** <http://www.forbes.com/sites/kashmirhill/2013/07/26/smart-homes-hack/>

### 8. Alarm bells ring for Internet of Things after smart TV hack

**Domain:** Home

**Description:** A team of scientists claim that hybrid smart TVs that blur the line between televisions and the internet are vulnerable to a simple hack. Smart TVs can be hacked using a cheap antenna and broadcast messages. The attack relies on an insecurity in the Hybrid Broadcast-Broadband Television Standard (HbbTV).

HbbTV allows the addition of interactive HTML content to DVB cable, satellite or terrestrial signals. This means that viewers can use their favourite web services via TV apps, and allows advertisers to serve up relevant ads.

The standard is vulnerable to an exploitation technique called the “Red Button attack”— named after the red button used on modern smart TV remotes to access additional content — that allows a hacker to intercept the sound, picture and accompanying data sent by the broadcaster using the data packets, and then takeover apps on the TV or even launch attacks across the Internet. On Facebook, for example, the hacker could log in and post messages to the social network on the person’s behalf.

**The Exploit**

Involves hacking the radio signal through the use of an antenna, hackers ‘become the broadcaster’ and even have the ability to hack into anything sent or received by the consumer.

This would be done by using a simple amplifier, costing as little as £150 ($250) on a rooftop to hijack networks across an area of 0.5 square miles (1.4 square kilometres). Alternatively, a transmitter could also be placed on a drone, which could hover outside the windows of houses to hijack TVs. The attackers could also set up a transmitter on a roof to potentially hijack tens of thousands of TVs across an entire city. In doing so, the hacker would have access to any websites the viewer was logged into on their smart TV. This could range from getting access to their Facebook accounts to writing fake reviews on websites for products.

**Vulnerabilities:**

1. While the impact of many of these attacks is exacerbated by poor implementation choices, for most attacks the core of the problem lies with the overall architecture, as defined in the specification itself.   
   This particular attack relies on an insecurity in the HbbTV standard.
2. This weakness could allow such attacks as man-in-the-middle, watering holes or the ability to change what users watch on TVs.
3. HbbTVs broadcasts can be hijacked because they are not linked to a web server, which also makes attacks virtually untraceable.

**Implications for MXD:**

1. MiTM attack, with hackers placing themselves between the consumer and the broadcaster and injecting their own information into the broadcast stream.
2. The attack does not require either an internet address or a server.
3. Attackers can use this insecure medium to get access to the target’s internet accounts.   
   - Someone using a smart TV could find their various internet accounts sending spam, printing coupons and writing fake reviews without their knowledge. Hackers could, in theory, also use these accounts to harvest personal information.
4. This enables a large-scale exploitation technique with a localised geographical footprint based on radio frequency (RF) injection.

This ‘requires a minimal budget and infrastructure and is remarkably difficult to detect.’ ‘In a dense urban area, an attacker with a budget of about $450 (£270) can target more than 20,000 devices in a single attack.’   
Source: <http://www.dailymail.co.uk/sciencetech/article-2652734/Is-smart-TV-risk-attack-Hackers-exploit-flaw-red-button-feature-hijack-web-accounts-steal-information.html>

After hacking the radio signal, hackers ‘become the broadcaster’ and even have the ability to hack into anything sent or received by the consumer. One problem with such an attack is that, since it would involve hacking into the radio signal through the use of an antenna, it would be difficult to track down the attackers.   
Source: <http://www.scmagazineuk.com/alarm-bells-ring-for-internet-of-things-after-smart-tv-hack/article/354900/>

**Mitigations:**

1. There are a number of possible solutions. The most drastic includes cutting all internet access to smart TVs.
2. Alternatively, broadcasters could begin to integrate smart TVs into a network that could see if they are being hijacked by monitoring for high spikes in signal strength.
3. The most simple solution, though, would be to have a confirmation box pop-up on screen when a viewer’s smart TV is trying to open an app such as Facebook.

**Source:**

1. <http://www.scmagazineuk.com/alarm-bells-ring-for-internet-of-things-after-smart-tv-hack/article/354900/>
2. <http://www.dailymail.co.uk/sciencetech/article-2652734/Is-smart-TV-risk-attack-Hackers-exploit-flaw-red-button-feature-hijack-web-accounts-steal-information.html>

### 9. Hacking Traffic Systems for fun and chaos

**Domain:** Automotive/Traffic control system

**Description:** Traffic control systems are vulnerable to a number of attacks and can be exploited quite easily from up to a mile or 2 away and perhaps could be used to spread malware from device to device.   
It’s also possible to cause electronic signs to display incorrect speed limits and instructions and to make ramp meters allow cars on the freeway faster or slower than needed. The attack was carried out by intercepting the signal between sensors in the pavement and the traffic control centre.

**The exploit:**

The hacker mounted a Sensys Networks wireless transmitter to a drone, and found he could intercept data being fed to traffic control systems from 50 metres away. He then attached an antenna to the USB-drive-sized transmitter and found he could be 500 metres from a light and still intercept the data.

The issue was found in devices that communicate with traffic control systems, not the actual systems controlling traffic lights themselves.

**Vulnerabilities:**

1. Unencrypted communications between devices that communicate with traffic control systems and the traffic control system itself.
2. Lack of authentication to access these devices(sensors on pavements).
3. Self-replicating malware can be used to infect the vulnerable controllers and spread device to device. The compromised systems can be used to launch attacks against traffic control systems at a later date.

It might be possible to create self-replicating malware (worm) that can infect these vulnerable devices in order to launch attacks affecting traffic control systems later. The exploited device could then be used to compromise all of the same devices nearby.   
Source: <http://blog.ioactive.com/2014/04/hacking-us-and-uk-australia-france-etc.html>

**Implications for MXD:**

1. Ease of compromising a traffic control system and injecting data in the system.
2. Ability to control and manipulate traffic lights, electronic signs on highways has dangerous implications on personal road safety.
3. An attacker could cause road chaos by launching an attack with a simple exploit programmed on cheap hardware ($100 or less). The attack could even be launched from a drone flying overhead.   
   - An attacker could potentially trick the system into changing lights or stalling on red lights.
4. These traffic problems could cause real issues, even deadly ones, by causing accidents or blocking ambulances, fire fighters, or police cars going to an emergency call.
5. Since the devices don’t require authentication, attackers can conceivably alter the firmware to make them unable to communicate with the rest of the system.

**Mitigations:**

1. Manual overrides and secondary controls could be used if anomalies are detected.

**Source:** <http://threatpost.com/hacking-traffic-systems-for-fun-and-chaos>

### 10. Philips Hue LED smart lights hacked, home blacked out by security researcher/ Welcome to the “Internet of Things,” where even lights aren’t hacker safe

**Domain:** Home

**Description:** Using a malware script, the Hue installation was hacked into and issued a blackout command through the bridge (the Hue’s router) turning the connected lights out entirely. In this case the malware script runs continuously, so the bulbs are commanded to turn off immediately after they are powered up. The highly connected Hue can be attacked through multiple vectors, including links on Facebook or by theoretically finding a flaw in the radio protocol (Zigbee Light Link).

**Vulnerabilities:**

1. The Hue, by design, is based on open APIs and the trust of local devices.   
   Hue lighting system was intentionally designed to grant access to any device connected to a user’s home network. Company designers went about doing this by using security tokens that are generated without requiring a user to press a special authentication button on the wireless bridge of the system.
2. The Philips wireless controller uses a weak authentication system to receive commands from trusted smartphones and computers.   
   It consists of a security token containing the device’s unique media access control identifier that has been cryptographically hashed using the MD5 hash algorithm. These hardware addresses are trivial to detect by anyone on the same network or often by people within radio range of a device, making them unsuitable for authentication.

**Exploit**

The exploit is in the form of Java code that can be delivered when browsing compromised websites or websites dedicated to serving attack pages. It combs through the address resolution protocol cache of a local network to find all connected devices. The exploit then runs the MAC address of each discovered device through the MD5 hash algorithm and includes the output in a security token used to send commands to the light controller. If a command is successfully executed, the exploit will repeat the successful command over and over. If a command doesn’t succeed, the malware will register a new token every second or so using a different MAC address until a valid one is found.

**Implications for MXD:**

1. Creation of a localised blackout   
   -the ability of an intruder to remotely shut off lighting in locations such as hospitals and other public venues can result in serious consequences.   
   - The vulnerability can be exploited to create a blackout that lasts as long as the lights are connected to the wireless control bridge. Even disabling the smartphone or computer the exploit abuses to take control of the system may not be enough to turn the lights back on if there are other devices on the network that have already been authenticated.

**Mitigations:**

1. Authentication each time a device connects to a local home network
2. Adequate authentication of devices

**Source:**

1. <http://www.extremetech.com/electronics/163972-philips-hue-led-smart-lights-hacked-whole-homes-blacked-out-by-security-researcher>
2. <http://arstechnica.com/security/2013/08/philips-hue-lights-malware-hack/>

### 11. It’s Insanely Easy to Hack Hospital Equipment

**Domain:** Health

**Description:** Drug infusion pumps that can be remotely manipulated to change the dosage doled out to patients; Bluetooth-enabled defibrillators that can be manipulated to deliver random shocks to a patient’s heart or prevent a medically needed shock from occurring; X-rays that can be accessed by outsiders lurking on a hospital’s network; temperature settings on refrigerators storing blood and drugs that can be reset, causing spoilage; and digital medical records that can be altered to cause physicians to misdiagnose, prescribe the wrong drugs or administer unwarranted care. These are just some of the things that could go wrong if a hospital is hacked into.

Attackers could also blue-screen devices and restart or reboot them to wipe out the configuration settings, allowing an attacker to take critical equipment down during emergencies or crash all of the testing equipment in a lab and reset the configuration to factory settings. Storage systems for X-rays and other images were equally vulnerable. These are generally backed up in centralized storage units that require no authentication to access.

**Vulnerabilities:**

1. Lack of authentication to access or manipulate the equipment.
2. Use of weak passwords or default and hardcoded vendor passwords.
3. Use of embedded web servers and administrative interfaces that make it easy to identify and manipulate devices once an attacker finds them on a network.
4. Inadequate/lack of proper air gapping of medical systems and devices.
5. Unauthenticated or unencrypted communication between the devices, leading to threat of misdiagnosis or wrong prescription.
6. Medical record backups are completely unprotected and there is no logging if you go in the backdoor way and grab those images.
7. An off-the-shelf vulnerability scanner against the software firewall of a surgery robot caused it to turn off.

**Implications for MXD:**

1. There are very few devices that are truly firewalled off from the rest of the organization. With initial entry into the network, one can scan and find almost all of the devices on the internal network.   
   Hackers could gain access to the devices by infecting an employee’s computer via a phishing attack, then exploring the internal network to find vulnerable systems.
2. A hacker who happens to be in the hospital could also simply plug his laptop into the network to discover and attack vulnerable systems.
3. Once in the system, an attacker can turn off the email pager notification features or alter the settings to change when an alert is sent.
4. Replay attacks of data passing from medical devices to patient records.
5. Embedded web services that allow devices to communicate with one another and feed digital data directly to patient medical records can have a serious impact on patient health.
6. Ease of turning off medical pager notification features or alter the settings to change when an alert is sent.
7. Disclosure of sensitive medical data/patient records.

**Mitigations:**

1. Proper configuration of firewalls and perimeter defense systems
2. Use of strong passwords
3. Air gapping of medical systems and devices.
4. Secure authentication of devices connecting to the network
5. Authentication of a device each time it connects to the network
6. Adequate encryption of network traffic
7. Backup and secure storage of medical record data

**Source:** <http://www.wired.com/2014/04/hospital-equipment-vulnerable/>

### 12. Renewable Energy’s Expansion Exposing Grids to Hacking

**Domain:** Energy

**Description:** The communication networks and software that link green energy sources to the grid as well as the electronic meters that send real time power usage to consumers and utilities are providing new back-door entry paths for computer hackers to raise havoc with the grid.

**Vulnerabilities:**

1. A multitude of energy inputs is forcing grid managers to run systems that communicate real-time data on power flows to consumers and power plants, bringing networks that were previously closely controlled into contact with computer and telecommunication systems used by millions.
2. Every meter being deployed in the U.K. has a “relay” that can disconnect a household from the power supply. This is controlled by the utility from a computer keyboard. Since the same code goes into all meters, it would take just one small piece of code inserted by a rogue programmer to disconnect the power from millions of meters and disable the remote connection to the utility.
3. Watering hole attack, where victims from the targeted company visit and pick up infected code. They were able to compromise industrial control systems and install malware that can replicate itself and spread to other computers.

**Implications for MXD:**

1. Ability to manipulate or disconnect the power from millions of meters and disable the remote connection to the utility.
2. Watering hole attack that leads to an exploit being downloaded onto a target system to be used in the spread of malware.
3. The malware can allow for monitoring of user’s energy consumption.

**Mitigations:**

1. Adequate air gapping of energy systems.

**Source:** <http://www.bloomberg.com/news/2014-07-01/renewable-energy-s-expansion-exposing-grids-to-hacking.html>

## - Black Hat/ DEFCON list of attacks

This section is still under development as these attacks are keynotes from DEFCON 2014 which at the time of writing hasn’t yet taken place. DEFCON takes place on August 6 & 7.

### 1. Home insecurity: No alarms, False alarms, and Sigint

**Domain:** Home

**Description:** A home security system with wireless connectivity allows for an increase in usability and minimal home modification. With a number of security flaws, however, it also opens up the home to greater potential for attack.

**Vulnerabilities:**

1. Lack of user authentication
2. Use of default passwords

**Implications for MXD:**

1. Ease of suppressing alarms and creating false alarms.
2. Monitoring of people within the home/user profiling

**Mitigations:**

1. Use of secure passwords

**Source:** <https://www.blackhat.com/us-14/briefings.html>

### 2. Learn how to control every room at a luxury hotel remotely: The dangers of insecure home automation deployment

**Domain:** Home

**Description:** A flawed home automation protocol (KNX/IP) that enables a remotely located attacker (even in another country) to control virtually every appliance in a hotel via a remote control: the lighting, temperature, music, TV etc. This can be done by exploiting flaws and reverse engineering the KNX/IP home automation protocol, as well as by scripting a Trojan which can send commands outside the hotel.

**Vulnerabilities:**

1. Insecure wireless connection
2. Use of insecure and unlocked commodity hardware
3. Use of legacy protocols

**Implications for MXD:**

1. Personal safety   
   The severity of these types of security flaws cannot be understated - from creating a chaotic atmosphere to raising room temperatures at night with fatal consequences.

**Mitigations:**

1. Use of a secured network
2. Use of protocols that are proven to have good enough security

**Source:** <https://www.blackhat.com/us-14/briefings.html>

### 3. Smart nest thermostat: A smart spy in your home

**Domain:** Home **Description:** Smart home automation devices, such as the Nest thermostat are designed to optimise power usage by learning user scheduling and power consumption patterns. Although equipped with OS level security checks, a hardware attack can bypass firmware signing and allow for a backdoor to be built into the Nest software, giving an attacker access to saved data, including WiFi credentials. The Nest can be rooted by loading a custom compiled kernel via a USB connection within a matter of seconds, allowing the attacker to monitor user behaviour and explore vulnerabilities in software protocols such as Nest Weave. A rooted device can also enable an attacker to plant rootkits, spyware and use rogue services and network scanning methods to study and further compromise the network.

**Vulnerabilities:**

1. Ease of rooting the Nest thermostat with a plugged in USB.
2. Bypassing firmware signing via a hardware attack.

**Implications for MXD:**

1. Use of a rooted device to install rootkits, spyware and launch other network scanning attacks
2. Ability to perform further attacks on the home network after gaining initial access to the network.
3. User profiling   
   Implications on personal safety.
4. Disclosure of personal data and saved WiFi credentials for easy access to devices connected to the home network.
5. Once access to the network has been gained, an attacker can explore the software protocols used in order to find potential vulnerabilities than can further be exploited.

**Mitigations:**

1. Use of strong passwords
2. Need for authentication for each device access on the home network

**Source:** <https://www.blackhat.com/us-14/briefings.html>

### 4. A survey of remote automotive attack surfaces

**Domain:** Automotive

**Description:** An attacker that hacks an automotive network can eavesdrop on communications by enabling a microphone, as well as perpetrate disaster by disabling the brakes. Examining the automotive network of different manufacturers enables exploring the security capabilities of the different automotive networks to build in better security controls.

**Vulnerabilities:**

1. Vulnerabilities in the Controller Area Network

**Implications for MXD:**

1. Personal safety
2. Potential for causing traffic chaos

**Mitigations:** TBD

**Source:** <https://www.blackhat.com/us-14/briefings.html>

### 5. Weaponizing your pets: The War Kitteh and the Denial of Service dog

**Domain:** Home

**Description:** A GPS device embedded collar can track a cat’s movements throughout a neighbourhood. Fitted with a WiFi sniffing device, this collar can now be used to intercept and steal data from IoT devices in homes. This basic premise can be adapted to load a doggie backpack with equipment such as a WiFi Pineapple to launch attacks such as a denial of service.

**Vulnerabilities:** TBD

**Implications for MXD:**

1. Security implications of the ease of affording readily available everyday objects with wireless data sniffing and attack capabilities.

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 6. Practical aerial hacking & surveillance

**Domain:** Home/ individual profiling

**Description:** Unmanned aerial vehicles (UAVs) with added hacking and surveillance devices can be used to track and profile individuals, as well as attack infrastructure. A drone like Snoopy can passively collect information leaked from wireless devices such as smartphones, as well as optionally interrogate devices for further information.

**Vulnerabilities:**

1. Insecure wireless connections
2. Use of no/default passwords

**Implications for MXD:**

1. Tracking and surveillance capabilities that can both passively collect data and actively probe for further information wirelessly.
2. Disclosure of personal data
3. Personal safety implications

**Mitigations:**

1. Use of strong passwords
2. Use of proper encryption schemes

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 7. Attacking the internet of things using time

**Domain:**

**Description:** Slow, resource constrained IoT devices are the perfect target for network-based timing attacks, which allows an attacker to brute-force credentials one character at a time, rather than guessing the entire string at once.

**Vulnerabilities:** TBD

**Implications for MXD:**

1. Ease of conducting a timing based brute force attack on resource constrained IoT devices

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 8. Hack all the things: 20 devices in 45 minutes

**Domain:** Home

**Description:** Attacking internet connected IoT devices is a matter of running unsigned kernels on rooted devices. This means that everything from TVs, baby monitors, media streamers, network cameras, home automation devices and VoIP gateways are insecure.

**Vulnerabilities:** TBD

**Implications for MXD:**

1. Security implications of an attacker being able to root a target device and run an unsigned kernel

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 9. Just what the doctor ordered?

**Domain:** Healthcare

**Description:** With security standards not being a requirement for medical device manufacturers, healthcare devices (many of which are internet facing) are vulnerable to strategic attack with the potential loss for human life.

**Vulnerabilities:**

1. Lack of appropriate firewall configuration
2. Most medical devices on the internal network are internet facing.

**Implications for MXD:**

1. Potential injury or loss of life
2. Security implications of inadequate air gapping

**Mitigations:**

1. Proper air gapping of devices and systems.
2. Secure configuration of firewalls and perimeter defense systems.

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 10. Elevator hacking - From the pit to the penthouse

**Domain:** Home

**Description:** An elevator is virtually no different than an unlocked staircase as far as building security is concerned and is increasingly being used by attackers to bypass building security systems.

**Vulnerabilities:** TBD

**Implications for MXD:**

1. Ease of subverting security systems in various facilities.

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 11.USB for all!

**Domain:**

**Description:** With the prominence of USB in IoT devices and further capabilities such as Device Firmware Update, USB On-The-Go and debug over USB, the attack surface of USB enabled devices is ever growing.

**Vulnerabilities:** TBD

**Implications for MXD:**

1. Vulnerability of USB enabled devices to traffic interception and manipulation
2. Injection of packet data

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 12. The monkey in the middle: A Pentesters guide to playing in traffic

**Domain:**

**Description:** Mallory, a TCP/UDP MiTM proxy can run as a gateway for a victim network, collect session information and passwords, direct traffic to your proxy and edit traffic as it goes by.

**Vulnerabilities:** TBD

**Implications for MXD:** TBD

**Mitigations:** TBD

**Source**: <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 13.Home alone with localhost: Automating home defense

**Domain:** Home

**Description:** TBD

**Vulnerabilities:** TBD

**Implications for MXD:** TBD

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>

### 14.The Internet of Fails: Where IoT has gone wrong and how we’re making it right

**Domain:**

**Description:**

**Vulnerabilities:** TBD

**Implications for MXD:** TBD

**Mitigations:** TBD

**Source:** <https://www.defcon.org/html/defcon-22/dc-22-speakers.html>



The M2M industry is comprised of different segments such as automotive, smart city, building automation, smart energy, manufacturing, agriculture, security and safety, health, education etc. Although the use cases are quite different, one thing all these areas have in common is that they require not only connected devices able to communicate over a variety of network connections, but these devices also require remote configuration and control capabilities. For example, M2M devices may need to be remotely ‘woken up’, they will require several firmware updates during their lifetime, or devices need to be configured for a certain network bearer, or data reporting periods and measurement thresholds need be set, or the device’s location has to be provided to a tracking centre. It is commonly recognized that the millions of connected devices that make up M2M systems and are part of the Internet of Things need to be switched on, configured, provisioned for services, maintained, updated with software, possibly switched off and on again, recovered from error conditions, monitored, queried for data, repaired, their applications managed and finally the devices taken off their network connections at the end of their lifetime. And ideally, all this happens remotely.

### 1. Nest

The Nest Learning Thermostat is an electronic, programmable, and self-learning Wi-Fi-enabled thermostat that optimizes heating and cooling of homes and businesses to conserve energy. While the Nest Thermostat doesn’t require a Wi-Fi connection, additional features like remote control and automatic software updates are only available when the Nest Thermostat connects to the Internet.

The benefits of connecting the Nest Learning Thermostat to Wi-Fi include the use of features such as:

* Remote control.
* Automatic software updates.
* Nest Energy Reports.
* Weather awareness for heat pump auxiliary heat switchover temps.

**Device Enrolment**

1. After your Nest Learning Thermostat is installed for the first time and the power is turned on, the Nest Thermostat will begin setup.
2. When connecting the Nest Thermostat to your home Wi-Fi network, you’ll see a list of nearby Wi-Fi networks. Turn the ring to highlight your home network.
3. Once you’ve selected your network, the password screen will appear (if your network is secured). Use the onscreen keyboard to type out your password.
4. Turn the ring to highlight the letter, number or symbol in your password and press to select it.
5. Create a Nest account to be able to control Nest from your mobile/tablet/laptop
6. When you create a Nest Account your Nest Learning Thermostat will usually automatically detect it if it’s on the same network as the smartphone or computer you used to create the account. A message will pop up on the Nest display to ask if you’d like to pair your thermostat to this account. Just press the thermostat’s ring to confirm.

**Technical specifications**

User Interface:   
The Nest thermostat has an LCD color display and one needs to rotate the Nest’s outer ring to make selections and press in to confirm a selection.

If you need to find any technical information regarding your Nest Learning Thermostat, such your IP address or what software version you have, you can find it in Technical Info. Press the ring to access the menu and turn the ring to SETTINGS. Within Settings, select TECHNICAL INFO.

You’ll find information regarding your Nest Thermostat’s sensors, your Wi-Fi Network, the serial and model numbers associated with your device, the IP address and MAC address for your Nest Thermostat, the Subnet mask and router and name server details.

Wireless:  
802.11b/g/n @ 2.4GHz   
802.15.4 @ 2.4GHz

**MXD Implications:**

Connecting Nest to the home Wi-Fi network is relatively simple for a user. The Nest thermostat automatically detects available Wi-Fi networks and created network accounts on a smartphone or computer registered on the same network. Creation of a network account is a matter of downloading the nest app on a smartphone and registering with a valid email address or navigating to the nest.com website on a computer. Currently, the Nest Thermostat can connect to open (no-password) home networks or to networks that follow PSK (Pre-shared key mode) or personal security protocol, specially designed for the home and small business. These security systems are typically labeled WEP, WPA, and WPA2 Personal.

**Source**: <https://nest.com/thermostat/life-with-nest-thermostat/>

### 2. Hive

Hive Active Heating lets you control your heating and hot water remotely from your smartphone, tablet and laptop. Hive includes a wireless receiver, thermostat and a hub.

Thermostat   
The wireless thermostat enables you to turn the temperature up or down and set schedules when you’re at home.

Hub  
The hub plugs into your broadband router so that your thermostat can connect to the internet and be controlled remotely.

Receiver   
The receiver enables your thermostat and boiler to communicate with each other.

**Device Enrolment**

1. Install the hub   
   To install the hub there has to be a broadband connection with a spare network port and a power supply nearby. Connect the hub to the household’s broadband router using the network cable provided. Fit the power cable into the hub and plug it into a power socket. Wait for an amber flashing light. Multi-coloured lights and a red light will flash, followed by the amber light. This usually takes less than 30 seconds but can take up to 5 minutes if updates need to be downloaded.
2. Install the receiver  
   You should fit the receiver in a convenient location close to the boiler or central heating system.
3. Add the thermostat  
   Mount the thermostat in a suitable location. The hub is ready to connect if it is flashing amber. After inserting batteries into the thermostat, the display will show ‘FIND’ – meaning it’s searching for the hub and receiver. The thermostat will then display room temperature – meaning it’s connected successfully to the hub and receiver.
4. Online account setup  
   Hive Active Heating is now installed and ready to be registered. There are two ways to complete online setup:   
   a. Set up using a web browser  
   b.Set up using the smartphone app.

**Technical specifications**

User Interface:   
The hive has a screen and four buttons that allow you to increase or decrease the temperature and go forward and back through menus.

Geolocation is another clever feature from Hive. It alerts you when you’ve gone out and left your heating on, or when you’re returning home and the temperature’s set lower than you’d like. It’s optional to use and works with your mobile’s location services and wi-fi connection. Geolocation is now available on the Hive iOS and Android app.

**MXD Implications:**

British gas specifies that Hive installation should only ever be carried out by a qualified engineer. This involves setting up the receiver and Hive thermostat as well as the hub. The hub needs to be physically connected to your router using a network cable (like the one provided with your hub). The final step in the device enrolment process involves the online account setup wich can be done using a web browser or a smartphone app. This is done by logging in using the account details supplied in the order confirmation email and entering the hub ID( XXX-123 formatted) number on the underside of the hub.

**Source**: <http://www.britishgas.co.uk/products-and-services/hive-active-heating/how-it-works.html>

### 3. Fitbit Flex/Zip/One

Fitbit activity trackers are wireless-enabled wearable devices that measure data such as the number of steps walked, quality of sleep, and other personal metrics.

**Device Enrolment**

1. Install the software and run the installation file.   
   Fitbit’s Uploader software uploads your Tracker’s stats from your base station to your personalized dashboard on Fitbit.com, so you can track your activity, log food, and much more.
2. Set up an account.   
   During the software installation, you’ll be guided through a process to set up your Tracker device and register an account on Fitbit.com. If you already have an account, you will be able to sign in. Note that only one Fitbit tracker can be paired to an account. If you currently have a Fitbit tracker paired to your account, when prompted you can choose to replace your existing tracker and continue setting up the new tracker. Your synced data will remain intact.   
   After filling out your personal information, you’ll be asked which device you’re setting up. Select the appropriate tracker to continue.
3. Plug the wireless USB sync dongle into your computer (this is the smaller USB device—not the charging cable), and bring your tracker near to it to begin pairing.  
   **Tracker Pairing:**   
   The tracker will display a number which ensures that the tracker is the device that the software is communicating with.   
   Force, One, or Zip: You will see a pairing number that appears on your tracker’s display once your device has been located; enter this number on your computer. Flex: Follow the onscreen instructions and rapidly tap the device when instructed, then confirm its vibration.   
   The base station wirelessly syncs data from your Tracker to your computer, whenever you are within about 15 feet. You’ll also use it to charge the Tracker’s battery every 5-7 days.
4. After clicking Next, your tracker will connect to your Fitbit.com account. This can take up to a minute. Once your tracker has connected to Fitbit.com, you may be prompted to enter a greeting (depending on which tracker you have). This can be your name or any 8-character combination of letters or numbers.   
   When your tracker is linked with your Fitbit account, Fitbit Connect will notify you and present some basic instructions on using your device.  
   You can now log into your account dashboard to view your synced data.   
   You will not need to repeat these steps once they have completed—you can simply login to [http://fitbit.com](http://fitbit.com/) to access your dashboard.

**Technical specifications**

Fitbit’s trackers offer Bluetooth Low Energy connectivity. Syncing occurs automatically any time the Fitbit tracker is within about 20 feet of the wireless sync dongle and is relatively motionless. The dongle plugs into your Mac or PC’s USB port. Syncing and uploading require use of the Fitbit uploader application. The tracker features a display that shows the pairing number when the tracker has been located (paired up with wireless USB dongle). Data synced from the Fitbit tracker to the Fitbit app is then loaded to the Fitbit.com dashboard via the device’s internet connection.

The Fitbit One and the Fitbit Zip were the first wireless activity trackers to sync using Bluetooth 4.0 or Bluetooth SMART technology.

**MXD Implications:**

Enrolling a Fitbit tracker involves a number of steps. After setting up an account on fitbit.com, the tracker is synced to the installed software by pairing the tracker with a wireless USB dongle that plugs into the computer running the software.

**Source**: <http://www.fitbit.com/uk/manual#section-start>

### 4. iKettle

With the iKettle you can start boiling your kettle from anywhere in the house. The iKettle tells you when your hot water is ready to pour, reminds you to refill and tells you when the kettle is empty.

**Device Enrolment**

1. After installing the iKettle app on your smartphone, to set up the iKettle, ensure that you are within range of your home network. Also ensure that your iKettle is plugged in and filled with water. Then press next on the app.
2. The app will automatically connect to the iKettle network on an Android device. To connect to the iKettle network on an iOS device, select the network manually by navigating to the network settings.   
   This process allows your iKettle to have a more stable connection and ensures that you can use the internet at home as well as your iKettle. You won’t need to switch between the two as you would on some wireless printers for example. The iKettle is allocated a spot on your router where it will stay connected. By entering your home network name and password you are giving permission for your router to allow the iKettle to connect.
3. Enter your Wi-Fi password(if password protected) and press next.   
   The iKettle will now connect to your home network.

**Technical specifications**

The iKettle comes with a built in smart chip, which contains a state of the art wifi module. This allows you to connect your smartphone via your home network so you can access all the features remotely.

Connectivity:  
Wireless 802.11b/gx  
WPA/WPA2  
Requires a 2.4Ghz router

**MXD Implications:**

When you first turn on the kettle it acts as a wifi hotspot and the iKettle app for Android and iPhone reconfigures the kettle to then connect to your local wifi hotspot instead. The app then communicates with the kettle on your local network enabling you to turn it on, set some temperature options, and get notification when it has boiled.

**Source**: <http://wifikettle.com/support/>

### 5. Lockitron

Lockitron is a device which can lock and unlock deadbolt locks via remote control, typically a smartphone. The device fits over the lock control mechanism on the inside of a door, and the door can then be unlocked via an app on the phone, or via web page control.

**Device Enrolment**

1. To get Lockitron set up on your WiFi network, you will need to use the Lockitron Android or iOS app. With the Lockitron app installed, head to “Setup New Lockitron”.
2. Enter your account information and click login. Select the wifi network you would like to connect Lockitron to. If your wifi network has a password, enter the wifi password.
3. Lockitron is added to your WiFi network using a process called “BlinkUp”.   
   This is done by holding your phone close to Lockitron’s top right corner(optical sensor) during BlinkUp.
4. When you tap “Send BlinkUp”, the app will “Blink” the credentials( WiFi and user account) over to Lockitron.

**Technical specifications**

Connectivity:   
Lockitron connects to your local-area-network (LAN) using WiFi (802.11b/g/n @ 2.4 GHz) and has a range around 300 ft from your router.

Phones with Bluetooth Low Energy (4.0) can also automatically unlock a door when an authenticated device is nearby. A supplied NFC tag can be read to trigger a command to toggle the state of the lock.

**MXD Implications:**

Inside of every Lockitron is an Electric Imp WiFi module that contains a WiFi chip. Upon entering your WiFi network information into the iPhone or Android Lockitron app, these credentials are transferred from the phone’s screen onto Lockitron via BlinkUp (Optical transmission?).

The Electric Imp currently supports WEP, WPA, WPA2.

**Sources**:

1. <http://help.lockitron.com/article/59-connecting-lockitron-to-your-wifi-network>
2. <http://electricimp.com/docs/gettingstarted/1-blinkup/>

### 6. Wireless Sensor Tags

Wireless Sensor Tags allow monitoring temperature/RH and open/closed status of gate/doors in your home or office, from anywhere with Internet access. Attach them to easy to lose items and locate them through beeping sounds. Data logging, out-of-range and back-in-range notification features come standard on all types of sensor tags.

**Device Enrolment**

1. Install the iPhone/iPad app. Use the 12 digit serial numbers on your Ethernet Tag Manager to create a login.
2. Associate each new Tag with the Tag Manager   
     
   For water/moisture sensors, please activate by shorting the tip using a metal object (scraping the tip using a coin, for example) or dipping the tip into water. A red light should start flashing on the sensor every few seconds for about 2 minutes, before the sensor goes into sleep again. Search and associate other tags while the light is flashing.   
   An unassociated tag periodically broadcasts information about itself when powered on. Tap the “Search an Unassociated Tag” button to receive this information.
3. When a new tag is found, the information associated with it is displayed. Assign a name to the tag and click “Associate”. The new tag name is assigned to the tag and is automatically propagated to all other devices accessing the same tag list.

**Tag Manager Ethernet port specifications**

10Base-T Requires DHCP server Firewall must allow outgoing HTTP (port 80) and port 6667 connection.

The tag is powered by a single CR2032 button cell Lithium battery. The onboard processor is a Microchip PIC16LF720 micro-controller that draws about a fifth of the current than the Amtel ATmega micro-controllers used in the Arduino boards. Wireless operations for the tags is provided by the Microchip MRF 49XA radio, which operates in the sub-GHz MHz ISM bands. While this can be changed, the tags ship and by default operate at 436 MHz.

**MXD Implications:**

The system is based around an Ethernet Tag Manager which connects directly to the home router and manages all the associated tags. It acts as a bridge between the wireless tags themselves and the Cloud backend which manages the tags.

Setting up the system is a fairly simple procedure. Plug the tag manager into your router and let it grab a DHCP address and announce itself to the mytaglist.com server. The tags included with the tag manager in your shipment should come pre-associated. If not, pull out the battery tab. If you have a flashing LED that means the tag is unassociated. Go to the web app and click on the button to add a new tag. The tag then shows up in the list on the web backend.

**Sources**:

1. <http://wirelesstag.net/>
2. <https://www.mytaglist.com/index.html>

### 7. GreenWave Reality LED bulb

The GreenWave Reality Connected Lighting Solution consists of high-quality, connected LED bulbs, a hand-held remote controller, and an optional Gateway that allows for complete remote lighting control. Each light bulb contains a wireless antenna that allows for high quality reliable communication between the bulbs using the wireless network. The network connects all lamps together, allowing flexible wireless control of all devices in a house. Each end node has an IPv6 address and can be controlled either individually or as part of a group.

**Device Enrolment:**

1. Install the Gateway   
   Make sure your router is already connected to your home network. Connect the Gateway to any available port in your router using the included Ethernet cable.
2. Download and Install the Smart Device Application   
   Make sure your smart device is connected to and in range of your wireless router, and then start the application on your smart device. When the application starts, it automatically searches for your Gateway through your wireless router. If the application finds a Gateway on your local network, it automatically connects to the associated lighting network.   
   If you want to have access to your lighting kit remotely through the Internet or a mobile data connection, you must first set up an online account. This account will provide authentication for you when you access your lighting kit remotely. You must remain connected locally to your lighting network when you create your account.
3. Install Light Bulbs on the Network   
   The light bulbs in your lighting kit already come pre-connected to the Gateway; however, you must still install the light bulbs so that the Gateway can find them on the network.   
   To connect lightbulbs to the gateway, follow these steps:   
   a. When you turn power on, the light bulbs will brighten and dim while attempting to connect wirelessly to your Gateway.   
   b. Press the sync button on the Gateway once to enable the connection. The activity indicator begins to display a clockwise rotating pattern.
4. Set up Light Bulbs in Application With the light bulbs, Gateway, and application installed, use your smartphone to set up the lights on the network.   
   a. Open the application on your smart device. The application automatically finds the light bulbs connected to the Gateway and prompts for set up.
5. Tap Yes. Your smart device then walks you through setting up each new light bulb.
6. Look for the light bulb that is dimming and fading. This is the light bulb you are currently configuring on your smart device.

**Technical specifications:**

NXPs network software provides the ultra-low-power wireless connectivity for the GreenChip iSSL and GreenChip iCFL modules. JenNet-IP is a 6LoWPAN mesh-under tree network with low memory footprint. The bulbs are IP enabled by a 6LoWPAN stack option used on top of JenNet.

The GreenChip smart lighting solution is available in two versions – GreenChip iCFL for compact fluorescents and GreenChip iSSL for LEDs – and currently includes:

1. The GreenChip iCFL or GreenChip iSSL chipsets, which function as highly efficient, dimmable drivers for smart lamps such as the UBA2027 and the SSL21081.
2. An ultra-low-power standby supply controller with 10mW no-load capability; standby power is particularly critical in smart lighting applications where lamps are continuously “listening” for the command from the user and/or network.
3. A 2.4-GHz IEEE 802.15.4 standard-compatible wireless microcontroller with a Tx/Rx current below 17mA.
4. The hardware components are complemented by NXP’s JenNet-IP software stack, which provides true IP connectivity. Every light bulb has its own IP address, so the system can be controlled by smartphones, tablets, PCs, and other IP-enabled devices.

Other software stacks, including ZigBee, are available as options.

Lighting Gateway and Remote

The lighting Gateway is the hub that connects the smart bulbs to your home network. It passes control between your Smart Phone/Tablet and your lamps. The Gateway can do this locally on your Home Network or through a cloud server.

The Lighting Remote control can control four groups of bulbs and can turn the lights on and off, or dim them. The Lighting Remote can be used with or without the gateway.

Handheld remote allows for control of lighting without a gateway or Cloud-service. Adding the Gateway provides powerful Smart Controls and remote access.

**MXD Implications:**

Each light bulb sports a NXP module that wirelessly connects it to the network of bulbs and to a remote control via a JenNet-IP mesh, an ultra-low-power IPv6 wireless network. The heart of the JenNet mesh is the Greenwave wireless controller, which connects to your home network to bridge your WiFi to the lighting WLAN and provide anywhere, anytime access to your lights.

The NXP solution also includes 128-bit AES encryption.

**Sources**:

1. <http://www.greenwavereality.com/solutions/connected-lighting-solution/>
2. <http://www.homedepot.com/catalog/pdfImages/2c/2c1afc12-4b5a-4213-8287-c27cc8cc601a.pdf>

### 8. Loc8ter Pet GPS

Loc8tor Pet GPS technology uses global satellites to track your pet and it uses a SIM card to report your dogs location. Loc8tor Pet GPS’s detailed tracking panel on your computer, tablet or mobile phone lets you see exactly where your dog is on the map. Using the online tracking panel you can not only track your dog but see exactly where they’ve been. You can also set up safety zones and as soon as your dog steps outside it, you’ll receive a text message or email telling you where they are.

**Device Enrolment**

1. Plug in the tracker to give it a power top up and it is ready to work straight out of the box.
2. To use your mobile phone to follow the tracker, go to mytrackingpanel.com/#map from any internet enabled mobile device including a tablet and enter in your IMEI.

**MXD Implications:**

All Loc8tor Pet GPS trackers come supplied with a SIM card which is locked to that device.

**Sources**:

1. <http://www.loc8tor.com/uk/pets/dogs/loc8tor-pet-gps.html/>

### 9. Savannah Tracking GPS-GSM Wildlife collar

The GPS-GSM collar obtains positions via GPS at user defined intervals. In addition to GPS positioning the unit can be set to record accelerometer based activity recording either continuously or at defined sample intervals.

**Setup of the Savannah Tracking data manager**

1. Download the Savannah Tracking Data Manager setup file “sdm.exe” from drop box on <http://dl.dropbox.com/u/49101503/sdm.exe>.
2. Run the sdm.exe which will take you though the steps to install the application.
3. Use the suggested installation locations and setting or specify alternatives.
4. Once the program starts you will receive a downloading error as you have not yet entered your credentials.
5. Go to “Settings” in the tool bar and select and enter the username and password provided to you at time of collar delivery.

**Technical specifications**

Position acquisition: GPS   
Data Transmission: GPRS via GSM network. Data downloaded via free data manager software.   
Activity recording: 3D Accelerometer based activity recordings which are linked to a mortality alarm system providing you with an alert SMS in case of mortality or unusual activity.   
Communications: Two way communication enabling you to reschedule data collecting interval, activity recordings and mortality alarm settings (assuming animal with GSM coverage)

**MXD Implications:**

Data is send from the unit via GPRS to a server and can be downloaded by the user using the free accompanying software. If the unit is outside GSM coverage the data will be sent as soon as the unit returns to coverage.

**Sources**:   
<http://www.savannahtracking.com/index.php?id=5>

### 10. ioBridge

ioBridge makes it easy to monitor and control nearly anything via your smart phone or web app using general purpose web gateways.

Web Gateways

ioBridge offers a range of web gateways or modules that connect products and devices to the Internet. Ethernet or Wi-Fi options are available, allowing for plug-and-play configuration and operation.

Sensors and Actuators

These sensors and actuators are typically small circuits that plug directly into one of the web gateway channels. ioBridge classifies its sensors and actuators into two types: Function Boards that use the analog input or digital inputs and outputs, and Smart Boards that extend the functionality of the web gateway.

**Device Enrolment**

1. Connect one of the sensors or actuators to one of a range of available web gateways.
2. Connect the gateway to Ethernet and Power.  
   The web gateway connects to the internet automatically.
3. Open up your computer’s web browser or smartphone to link to the dashboard and create widgets to monitor and control your device from anywhere.

**Technical specifications**

ioBridge standard web gateways require an Ethernet connection and custom Wi-Fi. Zigbee and other wireless options are also available.

Network

Gateways requires a 10/100/1000Base-T auto-negotiated Ethernet connection. Because of the way gateways communicate with the server, no additional ports need to be opened on the firewall or router.

MAC Filtering

If the network uses MAC address filtering, the module’s MAC address will need to be added to the router’s “allow” table. The MAC address of the module is configurable via the ioBridge.com Interface.

IP Addressing

If the network uses DHCP, the module will request an IP address and obtain an IP automatically by default. If DHCP fails, the module sets itself to an IP address of “169.254.19.77”. By using the telnet menu, the IP Address, Subnet Mask, Gateway, and DNS Addresses are configurable.

**MXD Implications:**

Connecting sensors/actuators to the internet is a matter of plugging in the sensors to the web gateway that is in turn connected to the router and internet at large via Ethernet/Wi-Fi.

ioBridge Web Gateways are input-output (I/O) routers that act as the interface between local devices and ioBridge’s servers on the internet (ioBridge cloud servers). The ioBridge web-gateway has an Ethernet connection like a home computer that plugs into a local network and creates a connection to ioBridge’s cloud servers. The ioBridge Web Gateways have I/O channels that enable the control and monitoring of digital inputs, analog inputs, serial data, servos, relays, and digital outputs using web-interfaces provided by ioBridge.

**Sources**:

1. <http://connect.iobridge.com/docs/#IO-201_Wi-Fi_Web_Gateway_for_Internet_of_Things_Applications>
2. <http://connect.iobridge.com/gateway-configuration>