information

Article

IoT Privacy and Security Challenges for Smart Home Environments

Huichen Lin and Neil W. Bergmann *

School of Information Technology and Electrical Engineering, University of Queensland, Brisbane 4072, Australia; waltlin@hotmail.com

* Correspondence: n.bergmann@itee.uq.edu.au; Tel.: +61-7-3365-1182

Academic Editors: Giovanni Russello, Muhammad Rizwan Asghar, Ashish Gehani, Changyu Dong and David Eyers

Received: 14 March 2016; Accepted: 4 July 2016; Published: 13 July 2016

Abstract: Often the Internet of Things (IoT) is considered as a single problem domain, with proposed solutions intended to be applied across a wide range of applications. However, the privacy and security needs of critical engineering infrastructure or sensitive commercial operations are very different to the needs of a domestic Smart Home environment. Additionally, the financial and human resources available to implement security and privacy vary greatly between application domains. In domestic environments, human issues may be as important as technical issues. After surveying existing solutions for enhancing IoT security, the paper identifies key future requirements for trusted Smart Home systems. A gateway architecture is selected as the most appropriate for resource-constrained devices, and for high system availability. Two key technologies to assist system auto-management are identified. Firstly, support for system auto-configuration will enhance system security. Secondly, the automatic update of system software and firmware is needed to maintain ongoing secure system operation.

Keywords: Internet of Things; cybersecurity; Smart Home

1. Introduction

The Internet of Things (IoT) has gained traction in recent years as a term to describe the connection of non-traditional devices, such as factory machinery, medical equipment or domestic appliances, to the Internet. Over the past few decades, the use of microprocessor-based controllers in applications from toasters to airliners has become ubiquitous. IoT can be seen as the next step in the evolution of these controllers by connecting them to the Internet. Additionally, RFID (radio frequency identification) tags are seen as an IoT technology for making the location and, potentially, the status of tagged objects available on the Internet. Atzori et al. [1], among many others, present a review of the range of applications of IoT technology.

Commentators vary in their understanding of the importance and depth of penetration of IoT technology. Cisco's Futurist, Dave Evans [2] subtitles his review as "How the Next Evolution of the Internet is Changing Everything". Others, such as Hurlburt et al. [3], worry that expectations are unrealistic. Since entering the Gartner Hype Cycle in 2011, IoT has been at the "peak of inflated expectations" for the past few years [4].

The European Commission has identified "Internet of Things" as one of its key work programs, supported by AIOTI—The Alliance for Internet of Things Innovation. This consortium acknowledge that IoT will be responsible for future disruptive technologies but also that new technologies need to be coordinated into a multi-vendor ecosystem: "The overall goal of the establishment of the AlOTI is the creation of a dynamic European IoT ecosystem to unleash the potentials of the IoT" [5]. As early as

2008, the US National Intelligence council listed the Internet of Things as one of "six technologies with potential impacts on US interests out to 2025" [6].

While debate still continues about the depth of impact and the rate of adoption of IoT technology into the next decade, it is clear that there are many areas where IoT penetration is rapid and disruptive. One emerging area of interest which is investigated in this paper is in the application of IoT to the Smart Home.

Like all areas of networked computing, security and privacy are primary requirements for trusted system operation in the Internet of Things. Many of the principles applied to safety critical systems and enterprise security are equally applicable to IoT security. However, while enterprises can dedicate specific professional resources to system security, and to system architecture designs, the Smart Home is often a relatively ad hoc system without dedicated system management resources, and without deep technical knowledge on the part of the householder. This presents particular challenges to security and privacy. Proposed solutions go some way to address security concerns, but there are still areas where further work is needed. The two main contributions of the paper are to summarize existing network techniques that can be used to secure Smart Homes, and then to present two areas of particular concern (system auto-configuration and security updates) where further work is needed.

The rest of the paper is structured as follows. In Section 2, a short introduction to privacy and security issues is given. In Section 3, the range of different application areas in which IoT technology is having an impact will be explored to show that IoT is not a "one-size-fits-all" technology set, and particular emphasis will be placed on IoT as applied to Smart Home applications. Section 4 describes security threats and vulnerabilities in the Smart Home, and Section 5 presents some existing solutions. Section 6 justifies our preferred system architecture and Section 7 presents our future research directions, before some final conclusions are drawn in Section 8.

2. Key Issues in Cyber Security and Privacy

The Internet has grown from a useful research tool for universities into a fundamental utility, as important as electricity, water and gas. Wherever there is a valuable resource, there is also crime which seeks to gain value from the illicit use of that technology, or to deny the use of that resource to others. The interconnected nature of the Internet means that Internet resources can be attacked from any location in the world, and this makes cybersecurity a key issue. Cybersecurity revolves around three main themes.

Confidentiality is about keeping data private, so that only authorized users (both humans and machines) can access that data. Cryptography is a key technology for achieving confidentiality.

Authentication is about verifying that data has not been tampered with, and that the data can be verified to have been sent by the claimed author. Non-repudiation (i.e., avoiding denial by a sender that they actually sent a message) is sometimes considered separately, but we include it here as a subset of authentication.

Access refers to only allowing suitably authorized users to access data, communications infrastructure and computing resources, and ensuring that those authorized users are not prevented from such access.

The Information Security Breaches Survey is an annual cyber threat report commissioned by the UK Department for Business, Innovation and Skills and conducted by PriceWaterhouseCoopers. The latest survey in 2015 [7] shows that security breaches are on the rise; 90% of large organizations experienced cyber breaches in 2015 compared to 81% in 2014, and 74% of small businesses also suffered security breaches, indicating a double-digit year-on-year growth rate of 14%.

Now that the Internet has become a mission-critical component of modern business, cybersecurity has become an indispensable component of information systems. However, as cybersecurity is enhanced, cybercrime is evolving to be more extensive, more destructive and more sophisticated. In Smart Homes, the ability of householders to manage their systems securely requires trusted and

intuitive automated systems to assist in network management. Without such systems, the security and privacy threats of the Smart Home are likely to outweigh the advantages.

3. IoT Application Domains

A number of application domains are particularly amenable to improved productivity through the deployment of IoT technology. Factory and plant automation applications are often grouped under the heading of Industrial Internet of Things. Xu et al. [8] review this application area. Reliability, including through redundancy, security, and suitability for harsh environments are some of the key issues.

The networking of biomedical instruments and databases in hospitals has the potential to dramatically improve the quantity and availability of diagnostic and treatment decisions [9]. It also has substantial implications for rural and remote clinics, providing ready access to specialist opinions [10]. Extending medical instrumentation to the home has improved quality of life and reduced hospital readmissions [11].

The last two decades have seen a surge in the use of electronics in automobiles, based on dozens of networked microprocessors [12]. The next stage of development will be communication between vehicles, and between vehicles and infrastructure [13]. Standardization, security and cost are major drivers.

Transport and Logistics are already heavy users of RFID tags for the tracking of shipments, pallets and even individual items [14]. The research direction here is into smart tags which can log and report transport conditions such as shock, tilt, temperature, humidity and pressure [15]. Here the key driver is low cost, as well as orderly communication to hundreds or thousands of tags simultaneously.

IoT technology is having disruptive impacts on a very broad range of industries including entertainment, dining, public transport, sport and fitness, telecommunications, manufacturing, hotels, education, environmental science, robotics, and retail. In many of these industries, IoT is becoming a key enabler of innovation and success, and industries are willing to invest in new technologies. Specialist IT support can be provided on staff or from external providers to ensure that the security and availability of their systems is sufficient for their business needs.

IoT and the Smart Home

This paper deals with a very different environment—the Smart Home. Professional system design, installation and setup may be available when the smart electronics are included as part of a new home build. However, in most cases, Smart Home IoT technology is likely to be retrofitted to an existing home piece by piece as needs arise. Often, there is no ongoing professional support in either the design or operation phases of the IoT deployment in the Smart Home. While there are some reasonably widespread specialized Smart Home standards, such as X.10 powerline-carrier communications, these lack any type of security, and were designed before these home control networks were connected to the Internet [16]. There are now a plethora of networking standards that can be used in a home (Zwave, Insteon, Bluetooth, Zigbee, Ethernet, Wifi, RS232, RS485, C-bus, UPB, KNX, EnOcean, Thread) [17]. Each has its strengths and weaknesses, and expecting a heterogeneous network with many different protocols to be efficiently and securely managed by a non-expert presents significant challenges.

The Smart Home potentially provides additional comfort and security, as well as enhanced ecological sustainability. For example, a smart air conditioning system can use a wide variety of household sensors and web-based data sources to make intelligent operating decisions, rather than simple manual or fixed-schedule control schemes. The smart air conditioning system can predict the expected house occupancy by tracking location data to ensure the air conditioner achieves the desired comfort level when the house is occupied and saves energy when it is not.

In addition to enhanced comfort, the Smart Home can assist with independent living for the ageing. The Smart Home can assist with daily tasks such as cleaning, cooking, shopping and laundry. Low level cognitive decline can be supported with intelligent home systems to provide timely reminders for

medication. Home health monitoring can signal caregivers to respond before expensive and disruptive hospitalization is needed [11]. However, none of these benefits is likely to be taken up if the Smart Home system is not secure and trusted.

4. Security Threats in the Smart Home

4.1. Threats

Although the Smart Home is a very different environment, the overall nature of security threats is similar to other domains.

Confidentiality threats are those that result in the unwanted release of sensitive information. For example, confidentiality breaches in home monitoring systems can lead to the inadvertent release of sensitive medical data. Even seemingly innocuous data, such as the internal home temperature, along with knowledge of the air conditioning system operation parameters, could be used to determine whether a house is occupied or not, as a precursor to burglary. Loss of confidentiality in things such as keys and passwords will lead to unauthorized system access threats.

Authentication threats can lead to either sensing or control information being tampered with. For example, unauthenticated system status alerts might confuse a house controller into thinking that there is an emergency situation and opening doors and windows to allow an emergency exit, when in fact allowing illicit entry. One issue that will be raised later is automated software updates—if these are not appropriately authenticated problems can arise.

Access threats are probably the greatest threats. Unauthorized access to a system controller, particularly at the administrator level, makes the entire system insecure. This can be through inappropriate password and key management, or it could be by unauthorized devices connecting to the network. Even if control cannot be gained, an unauthorized connection to a network can steal network bandwidth, or result in a denial of service to legitimate users. Since many Smart Home devices may be battery operated and wirelessly networked with a low operational duty cycle, flooding a network with requests can lead to an energy depletion attack—a form of denial of service.

4.2. Vulnerabilities

A significant vulnerability is networked system accessibility. Because modern Smart Home systems are connected to the Internet, attacks can be conducted remotely, either by direct access to networked control interfaces, or by downloading malware to devices.

System physical accessibility is also an issue. For both wireless and power-line carrier technologies, the networks can be physically accessed from outside the house, even if the house itself is securely locked.

The next vulnerability is constrained system resources. Device controllers have traditionally been small 8-bit microcontrollers with very limited computational and storage resources, limiting their ability to implement complex security algorithms.

System heterogeneity is a vulnerability. Devices come from many manufacturers, with different networking standards and different software update capabilities. Often the devices have little or no documentation about their internal software, operating systems, and installed security mechanisms.

Fixed firmware is another issue. There are very few smart home appliances which provide any regular software update service to patch security vulnerabilities. One suspects that there is currently little incentive to continually patch software to stay ahead of security vulnerabilities for devices costing a few dollars.

Slow uptake of standards is a vulnerability. While some proprietary systems, such as a health monitoring sub-system, may have well-designed standards-compliant security, most current Smart Home devices implement few, if any, security approaches.

We consider the largest vulnerability to be the lack of dedicated security professionals who can manage the complexities of a Smart Home network. Few householders can afford professional ongoing

home network management assistance. Instead, amateur householders need to be able to self-manage their systems simply, safely and securely.

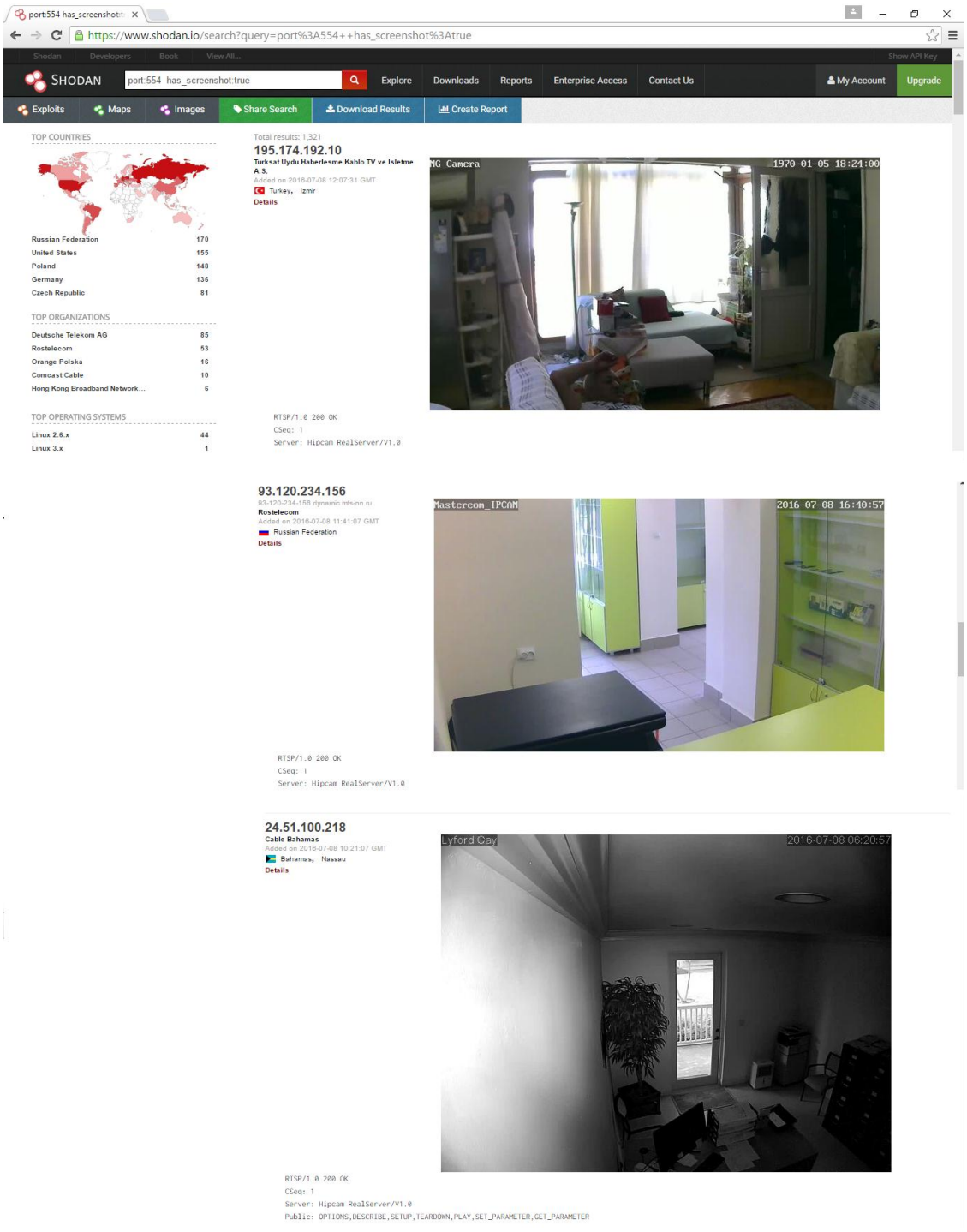

Figure 1. A list of home surveillance cameras from Internet device–scanning search engine Shodan.

4.3. Vulnerability Example

As an example, a householder might assume that their web cam is only accessible by users who have been given its host name and port number. However, with the help of Internet device–scanning search engines such as Shodan (https://www.shodan.io) [18] and Censys (https://censys.io) [19], which legitimately search for accessible sensors, many devices are suddenly known and visible.

The conventional search engines such as Google and Bing crawl the Internet by retrieving webpages and follow the hyperlinks in those pages to index webpages, pictures or some popular file types. Internet device–scanning search engines, on the other hand, work like a network scanner, scanning the open ports of Internet nodes and indexing the header or banner information returned by connected devices; the headers or banners of the reply often include the device type, model, vendor, firmware version and other information. Apart from HTTP and HTTPS protocols, Internet device–scanning search engines use a variety of protocols (FTP, SSH, DNS, SIP and RTSP, etc.) to connect to the open ports of nodes. To facilitate access, these search engines also provide an application programming interface (API) to access their search results programmatically. Attackers can take advantage of these search engines to find vulnerable devices on the Internet. For example, using the search keywords "has_screenshot:true port:554" in Shodan will return a list of home surveillance cameras with their IP addresses, geographic locations and screenshots, as shown in Figure 1.

5. Some Existing Security Support for IoT

Due to their low cost, IoT computing devices generally are not as powerful as traditional desktop and laptop computers. Most IoT devices are low energy, use a low-end microcontroller and have limited memory. Such controllers are well-matched to the requirements of standalone controllers in a washing machine or air conditioner.

However, these characteristics have made the move to networked IoT controllers more challenging as the existing Internet protocols are not typically designed for these embedded devices. Several Internet Engineering Task Force (IETF) working groups have been created to tackle these problems. IETF standardization work on IoT has played a vital role in the establishment of the necessary light-weight communication protocols for constrained environments over the existing IP network. These include IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN: RFC 6282) [20], IPv6 Routing Protocol for Low power and Lossy Networks (RPL: RFC 6550) [21] and Constrained Application Protocol (CoAP: RFC 7252) [22]. Figure 2 shows the comparison between IETF IoT and TCP/IP protocol stacks. Once devices are connected to the Internet, any of the security threats on the Internet could also compromise the security and privacy of IoT. In the following sections we review the current security implementations for these standard IoT protocols.

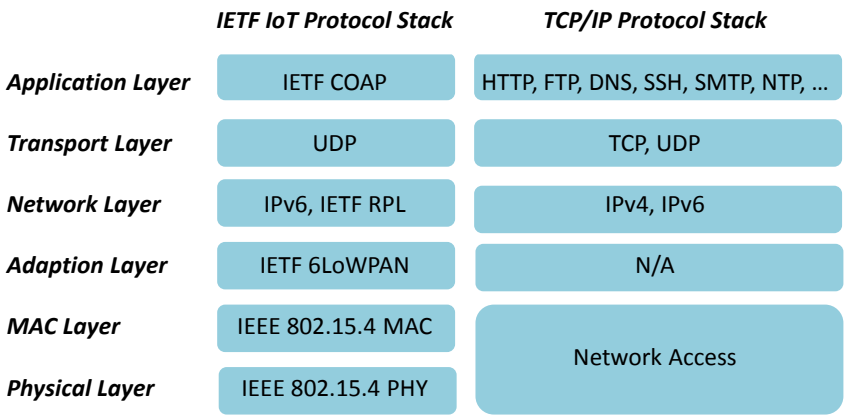

Figure 2. The comparison between IETF IoT and TCPIP protocol stacks.

5.1. 6LoWPAN and Security

The Institute of Electrical and Electronics Engineers (IEEE) has defined the 802.15.4 standard for wireless personal area networks (WPANs). IEEE 802.15.4 defines how the physical and media access control layers should operate under the low-bandwidth, low-cost, low-speed and low-energy conditions typical of these networks. As such, 6LoWPAN [23] is a light-weight protocol designed by the IETF to allow IPv6 packets to be transferred over IEEE 802.15.4 wireless networks.

The Internet Protocol Security (IPsec) suite has defined Authentication Headers (AH) and Encapsulating Security Payloads (ESP) to enable data integrity, confidentiality, origin authentication and anti-replay protection for IPv6 packets. The authors in [24] proposed compressed AH and ESP features for 6LoWPAN to implement IPsec and thus provide end-to-end secure communications between wireless devices.

An enhanced authentication and key establishment scheme for 6LoWPAN networks (EAKES6Lo) has been proposed by the authors in [25]. EAKES6Lo is divided into two phases to improve the security of 6LoWPAN networks. The two phases are: (1) system setup; and (2) authentication and key establishment. In Phase 1, the symmetric cryptography mechanism Advanced Encryption Standard (AES) is used to encrypt the data transfer in the network. To verify the integrity of the data, hash function Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA) is employed. In Phase 2, six messages will be exchanged to finalize the authentication and key establishment process and establish a mutual authentication.

Thus, 6lowPAN provides a template for secure wireless communications, even for resource-constrained devices.

5.2. RPL and Security

Routing protocols are a core component of conventional networks, and this also applies to 6LoWPAN networks. RPL [21] is an optimized IPv6 routing protocol designed by IETF especially for Low power and Lossy Networks (LLNs) and is primarily used by 6LoWPAN networks. RPL is a distance-vector routing protocol, and its mapping topology is based on a Destination-Oriented Directed Acyclic Graph (DODAG) structure. A generic topology authentication scheme called Trust Anchor Interconnection Loop (TRAIL) for RPL has been presented in [26]. TRAIL can prevent the topological inconsistency attacks from spurious nodes by discovering and isolating the forged nodes. A round-trip message has been used by TRAIL to validate upward path integrity to the root node and help the nodes in the tree get genuine rank information. The innovation of TRAIL is that each node in the tree can validate its upward path to the root and detect any fake rank attacks.

In the DODAG tree, it is essential for nodes to select their correct parent nodes, since every node except the root must have a parent node. The RPL rank is used to describe a node's position in the tree topology. In [27], the authors present a secure selection scheme to help a child node to choose an authentic parent node. In its selection algorithm, a node's threshold value will be calculated based on average and maximum rank values from its neighbour nodes to exclude spoofing nodes from becoming its parent.

So existing solutions can ensure secure routing table generation in Smart Home networks.

5.3. CoAP and Security

CoAP [22] is a HTTP-like application layer protocol designed for constrained device networks. As there are some special requirements such as group communications in IoT networks, CoAP provides multicast support which HTTP does not have. To better suit the low-bandwidth connections and low-computational-power device environments, the User Datagram Protocol (UDP) protocol is adopted by CoAP. UDP is a simpler, low-latency and connectionless transport layer protocol compared with its counterpart Transmission Control Protocol (TCP). CoAP is a stateless protocol and is based on the client-server architecture model. It uses request/response-style operations to exchange messages between the client and server. Similar to HTTP, CoAP is also based on a representational state transfer (REST) model, where each resource on the server has its own Uniform Resource Identifier (URI), a client can access a resource by making a request to the server, and the request can be one of these four methods: GET, POST, PUT and DELETE.

Nowadays, Transport Layer Security (TLS: RFC 5246) [28] is the predominant encryption protocol for HTTP, but the implementation of TLS is overcomplicated for the resource-confined IoT devices. To secure communications, CoAP employs Datagram Transport Layer Security (DTLS: RFC 6347) [29]

as its security protocol. DTLS offers the same security services that TLS provides. The main difference between TLS and DTLS is that TLS is based on the TCP protocol and DTLS is based on the UDP protocol. The CoAP specification has defined four different security modes. A device can be in one of four security modes: NoSec, PreSharedKey, RawPublicKey and Certificate.

Again, IETF standards provide secure mechanisms for secure web-based communications within constrained networks.

5.4. Future IoT Security Directions

As indicated by the above three examples, there is already significant work underway to secure mission-critical IoT applications. A lot of effort has gone into developing IP-compatible secure communications networks which are suitable for resource-constrained devices, and which use state-of-the-art security techniques. However, many of these techniques require careful, unified, system-wide design, and experienced network engineers to design and maintain a secure IoT system. The emphasis of our work is not on this style of "technical" security, but rather it is on the system management aspect of Smart Home security, i.e., how to properly install and maintain the security enabled by these powerful tools.

6. A Suitable Smart Home Architecture for Security

There have been many different proposals for Smart Home architectures, each of which have particular security issues. Three of the most important and popular architectures are middleware, cloud and gateway architectures. The next sections investigate the security issues and implementation difficulties for these architecture styles.

6.1. Middleware Architectures and Security

Middleware is a software layer that sits between the low-level layer of devices and the high-level application layer. It usually provides a common interface and a standard data exchange structure to abstract the complex and various lower-level details of the hardware. When the middleware receives a request from a higher-layer application, it converts the high-level standardized resources access request to the corresponding device-specific methods. When the device responds back to the application, the middleware processes the low-level methods and data transformations, and then sends the related abstract commands and data back to the application. The application does not need to know the underlying details of the different implementations of the hardware, it can just simply invoke the commands and functions provided by the middleware. Security and privacy protection should be considered at all levels of the middleware, from the lower hardware interaction level to the higher common interface level.

VIRTUS Middleware [30] is a middleware solution based on the open eXtensible Messaging and Presence Protocol (XMPP) protocol. It adopts the Simple Authentication and Security Layer (SASL) protocol for authentication and the Transport Layer Security (TLS) for data security and privacy.

Secure Middleware for Embedded Peer-to-Peer systems (SMEPP) [31] is a middleware focusing on providing peer-to-peer security communication between smart nodes. Before a device can communicate with others, it needs to join a group by providing a valid credential. There are three different security levels, but only level 1 and level 2 take up the security mechanisms. There is no security implementation under level 0. SMEPP implements pre-shared key cryptography under level 1 and public-key cryptography under level 2 for group admission. On the other hand, SMEPP adopts authentication under level 1 and authentication together with encryption approach under level 2 to protect data security.

While middleware has been extensively used in corporate systems with desktop-class machines to manage complex heterogeneous networks, currently proposed IoT middleware solutions require substantial additional complex software layers and cryptographic routines to be implemented on devices which have neither the memory nor the computational power to host them. Apart from the

performance problems, another concern for middleware architecture is that the coding defects in middleware inadvertently introduced by developers may potentially pose security threats to the IoT devices. So we reject middleware solutions as presently infeasible for many IoT-class devices.

6.2. Cloud Architectures and Security

Collaboration between devices is an important aspect of IoT. Such interoperable functions require high processing power which most IoT devices are not capable of. To solve the performance problem of IoT devices, researchers have proposed cloud-based solutions for IoT. The cloud has the resources to monitor, collect, store and process data from IoT devices. By analyzing this data, the cloud can trigger actions according to user-defined policies to achieve complex Smart Home control. The cloud-based architecture of IoT is also known as the Cloud of Things (CoT).

The authors in [32] propose an IoT cloud architecture based on the IETF's CoAP protocol [22]. The architecture consists of three decoupled stages which are the network, protocol and business logic stages. Each stage includes an incoming event queue, a thread pool and an event handler that processes the stage logic. The lightweight DTLS [29] is used by this architecture as its security protocol for authentication and communication.

A secure scheme for the Home Area Network (HAN) based on cloud computing has been introduced in [33]. A Home Management System (HMS) manages devices and policies, and provides the access point for users. In the paper, the authors implement the HMS functions in the cloud and the HMS interfaces with the cloud services. This scheme employs symmetric key encryption to apply confidentiality between end-to-end communications and each smart object is assigned a unique key.

The cloud-based solution removes the need for a separate home controller and provides a good way for IoT to connect and cooperate; however, it replaces the need for local computation with a need for substantial Internet communication. Due to the resource-limited nature of IoT, large amounts of raw data generated by IoT devices have to be transferred to the cloud without pre-processing; therefore, devices in the home need a high-speed, low-latency, always-on Internet connection, but such always-on high-speed Internet connections are not always available, especially in rural or remote areas. Control latency is increased, especially if the servers are overseas or the network is congested.

All devices must be accessible via the Internet which presents a broad attack surface, and each device needs to have sufficient resources to implement full network security protocols. Denial of service attacks, based on limiting access to the broader Internet, or occasional network outages may cause mission-critical tasks such as home healthcare and physical security systems to fail. Furthermore, because users do not have the full control of their cloud services, they have to trust cloud providers to implement appropriate and sufficient security measures for their data, but it is not always the case.

Because cloud-based systems fail without always-on network connectivity, we do not believe that they can provide a secure and available Smart Home system by themselves, and they also expose all network devices to network attacks.

6.3. Gateway Architectures

An IoT gateway is a relatively resource-rich network processor working on the same LAN with the other IoT endpoints. It can not only be a central management point to deal with the coordination of IoT devices, but it can also improve interconnection and interoperability between smart devices from different manufacturers. In addition, it can act as a bridge to connect the local IoT infrastructure to the cloud. Since the gateway has more computing power and resources, high computation and memory-rich tasks can be offloaded from IoT devices to the gateway. In terms of security, the gateway can centralize user authentication and apply access control to guard against unauthorized access or modification of restricted data. It also acts as a firewall to protect the smart devices and privacy from cyber threats, and to reduce the attack surface.

In [34], the authors present an integrated access gateway (IAGW) architecture to support various application nodes through standard interfaces for Smart Home environments. The architecture

comprises the ubiquitous sensor networks layer, the network layer and the service layer. IAGW includes a security module to implement the authentication, authorization and encryption. One of the benefits of this architecture is that it has a Quality of Service (QoS) module to prioritize traffic and guarantee resources for mission-critical operations.

A systematic concept called Server-Based Internet-Of-Things Architecture (SBIOTA) [35] is a proposed gateway server to provide an effective, efficient, secure and cooperative integration solution for IoT. This conceptual architecture includes a novel auto-configuration service on the gateway to facilitate the device's deployment and management process so that a device can be plugged into a network and be fully functional on that network with a minimum of manual configuration. Its initial approach is that the authentication and communication between the gateway and devices take place through a separate network port or a short-range antenna physically adjacent to the server. Before connecting the devices to the network, the user needs to place them in physical proximity to the gateway to be authenticated and exchange related information to ensure only legitimate devices are allowed to connect to the network.

A gateway can implement sophisticated management algorithms on a reasonably powerful processor, and it can operate the critical Smart Home functions. Even in the temporary absence of an Internet connection, it can provide sophisticated firewall and proxy support to IoT devices so that they have minimal exposure to direct network attacks, and it can work with resource-constrained IoT devices without complex middleware. Therefore, this is our preferred Smart Home architecture.

7. Future Smart Home Security Challenges

Our research is currently investigating two enhancements that are needed for a gateway-based Smart Home architecture to make it sufficiently secure for widespread adoption. Our work is still in the early stages, so we present the problems, and overall system architectures, as a first step towards solutions.

7.1. Auto-Configuration Support

It is expected that more and more smart household appliances will be interconnected to Smart Home networks. A lack of technical support is the biggest challenge in the household environment. Householders will be burdened by tedious, repetitive and error-prone manual tasks for adding and managing these smart devices on their home network, which can pose a major security risk. Therefore, for the successful implementation of a Smart Home, a secure auto-configuration approach should be further studied not only to simplify Smart Home device installation and maintenance but also to enhance the security in the auto-configuration process.

Our approach requires functionality in the gateway and cloud-based services. When a new device is attached to the network, the gateway will use the device ID to interrogate a trusted web service to discover the details of the device—what its functionality is, what its commands are, what encryption and networking protocols it understands, and any essential firmware updates that are now available. This is a different approach to most auto-configuration approaches which require a lot of this information to be stored on the devices themselves, and for the devices to be able to already implement a deep protocol stack. With our approach, a simple device ID and a web service ensures this information is easily available and remains up-to-date.

Figure 3 shows the typical network architecture and the series of steps needed to initiate this auto-configuration.

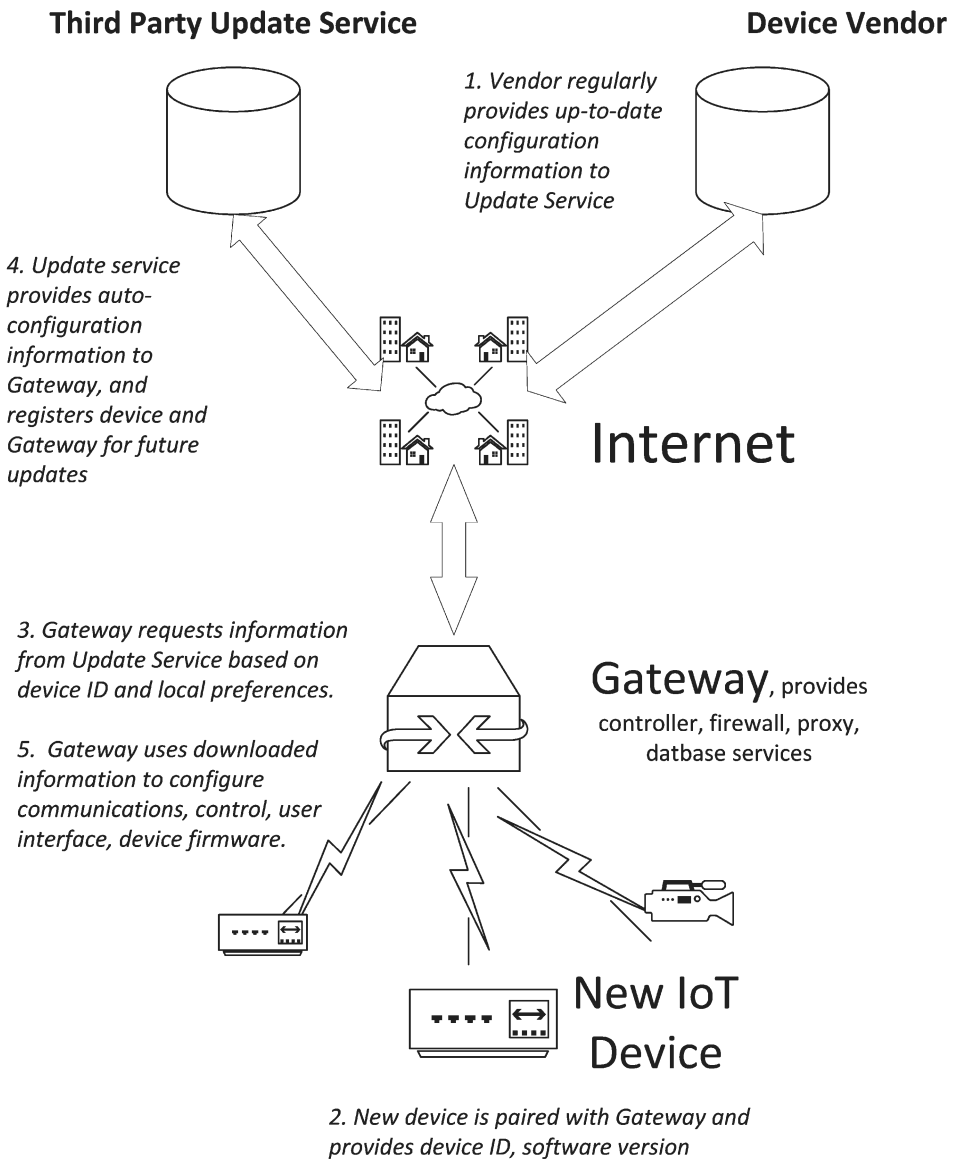

Figure 3. Auto-configuration architecture.

7.2. IoT Software and Firmware Updates

Desktop operating systems are updated regularly and automatically as security vulnerabilities are identified and patched. Mobile devices such as smart phones also receive regular software updates, including mechanisms to verify the authenticity of the changes. Such systems are economically viable because the number of operating system variants and operating system manufacturers are small, and deployed devices are in the millions. No such regular update service is available for the hundreds of different IoT devices.

An IoT device is a combination of hardware and software to perform specific, dedicated tasks. Firmware is a type of software that is programmed into the non-volatile memory of a smart device. It is an essential part of any IoT system since firmware is the program that directly interfaces with the hardware, controlling the system's operations and functions, from initializing the device, interfacing with users, processing of the requests and performing tasks. As a consequence, it is vital that smart device firmware is kept up-to-date to resolve security vulnerabilities, improve functionality, add new features and fix other bugs. Unlike the enterprise-scale environment which has its own dedicated IT department or technical team to manage and deploy the software updates, the Smart

Home environment usually lacks technical support. The IoT devices for Smart Homes should have mechanisms to implement safe and secure firmware updates automatically, with little or no user intervention. Such functionality can be managed by the home gateway.

To ensure the integrity and authenticity of the updates and to prevent possible firmware tampering such as malware injection, certificate-based digital signatures should be applied for the updates. Prior to updating, each update must be verified against its digital signature and the digital certificate should be checked to ensure it is valid and is issued by vender or a trusted third party. The methodologies used to download new updates also require careful thought. If the update-checking mechanisms are compromised, a hacker could block the new updates from being installed and conduct an attack on unpatched firmware. Attackers could also disguise a legitimate old version of firmware with security vulnerabilities as the latest version, resulting in the firmware reverting back to a faulty version. Therefore, the device vendor or manufacturer should encrypt and digitally sign the updated release information without providing cybercriminals an opportunity to interfere with the update version maintenance process. Due to the low bandwidth and resource-limited nature of many smart devices, delta updates greatly improve efficiency and cut down on installation task time, as the delta updates only contain the data that have changed. This can significantly diminish the possibility of update failure, especially for the battery-operated devices because of battery power exhaustion during the time-consuming firmware upgrade process.

The authors in [36] proposed a new software update mechanism for resource-confined IoT devices called Generic extension for Internet-of-Things ARchitectures (GITAR) that can be applied to the existing IoT operating systems. According to the authors, this architecture is able to use standard file structures, tools and methods to apply the partial code updates (delta updates) for protocols and applications during run-time. This architecture comprises three levels: the static system level, the dynamic component level and the kernel level. The core operating system components and hardware drivers are implemented at the system level. For the purpose of improving software portability, the system level is divided into a hardware abstraction (HAL) and a hardware interface (HIL) layer. The static code at the system level only can be updated by upgrading the whole firmware. As opposed to the system level, the applications and network protocol components run at the component level, and the code at the component level is flexible, which means this code can be updated dynamically instead of replacing the entire firmware. The kernel level is the interface between the system and component levels. It binds dynamic components to one another and to system functions. The authors have demonstrated their approach with the popular open-source IoT operating system Contiki without requiring major modifications to the source code in existing network protocols and applications.

Our proposed approach, similar to auto-configuration, relies on two key components. The first is implemented as a web-based service. Either the manufacturer or a trusted third party (as identified during the auto-configuration) maintains the latest versions of the software and firmware, which can be pushed to gateways identified during the auto-configuration process. The web-service can distinguish between vulnerabilities in the operating system or the specific device application code, and can download patches for either. The gateway manages the update process locally. The gateway can auto-schedule these updates at locally convenient times. The gateway can also manage the update of the rollback information if the update installation results in an unexpected loss of functionality when the gateway undertakes automated testing of the updated software. The gateway can also respond automatically to critical vulnerabilities, for example by blocking network access to an insecure device until a patch is available.

8. Conclusions

Internet of Things is not a single application domain, and the security approaches used in a domestic Smart Home application are quite different to those that can be afforded by mission-critical applications in industry or utilities. A particular issue is that the security of the network depends on

installation and configuration by largely untrained staff. This makes effective security policies and mechanisms much more difficult to develop, implement, enforce and maintain, unless this can be done automatically. A Smart Home gateway architecture supported by web-services for automatic device and network configuration and automatic system updates is our preferred approach for solving these problems.

Acknowledgments: This work is supported by the School of Information Technology and Electrical Engineering at the University of Queensland.

Author Contributions: Huichen Lin has researched and written Sections 2, 4–7. Neil Bergmann has written Sections 1, 3, and 8 and provided editorial support for the other sections. Both authors have read and approved the final manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

6LoWPAN	IP version 6 Low power Wireless Personal Area Network protocol
AES	Advanced Encryption Standard
AH	Authentication Headers
AIOTI	The Alliance for Internet of Things Innovation
API	Application Programming Interface
CoAP	Constrained Application Protocol
CoT	Cloud of Things
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DODAG	Destination Oriented Directed Acyclic Graph
DTLS	Datagram Transport Layer Security
EAKES6Lo	Enhanced authentication and key establishment scheme for 6LoWPAN networks
ECC	Elliptic Curve Cryptography
ESP	Encapsulating Security Payloads
FTP	File Transfer Protocol
GITAR	Generic extension for Internet-of-Things ARchitectures
GPS	Global Positioning System
HAL	Hardware Abstraction Layer
HAN	Home Area Network
HI	Host Identity
HIL	Hardware Interface Layer
HIP	Host Identity Protocol
HIPDEX	Host Identity Protocol Diet Exchange
HIT	Host Identity Tag
HMS	Home Management System
HRA	Home Registration Authority
HTTP	HyperText Transport Protocol
HTTPS	HyperText Transport Protocol Secure
IAGW	Integrated Access Gateway
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IPv6	Internet protocol version 6
IT	Information Technology
MAC	Media Access Control/Message Authentication Code
MTU	Minimum Transmission Unit
NIST	National Institute of Standards and Technology
QoS	Quality of Service
RA	Registration Authority
REST	Representational State Transfer
RFC	Request For Comment
RFID	Radio Frequency Identification
RPL	Routing Protocol for Low-Power and Lossy Networks

RSA	Rivest Shamir Adleman
RTSP	Real Time Streaming Protocol
SASL	Simple Authentication and Security Layer
SBIOTA	Server-Based Internet-Of-Things Architecture
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMACK	Short Message Authentication ChecK
SMEPP	Secure Middleware for Embedded Peer-to-Peer systems
SSH	Secure Shell
TACIoT	Trust-aware access control system for IoT
TCP	Transmission Control Protocol
TLS	Transport Layer Security
TRAIL	Trust Anchor Interconnection Loop
UDP	User Datagram Protocol
UK	United Kingdom
US	United States
WPAN	Wireless Personal Area Networks
XMPP	eXtensible Messaging and Presence Protocol

References

1. Atzori, L.; Iera, A.; Morabito, G. The internet of things: A survey. *Comput. Netw.* **2010**, *54*, 2787–2805. [CrossRef]
2. Evans, D. The internet of things: How the next evolution of the internet is changing everything. 2011. Available online: http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf (accessed on 8 July 2016).
3. George, F.H. The internet of things: A reality check. *IEEE Comput. Soc.* **2012**, *14*, 56–59.
4. Gartner Inc. Hype cycle research methodology. Available online: http://www.gartner.com/technology/research/methodologies/hype-cycle.jsp (accessed on 8 February 2016).
5. European Commission. The alliance for internet of things innovation (AIOTI). Available online: https://ec.europa.eu/digital-single-market/alliance-internet-things-innovation-aioti (accessed on 11 January 2016).
6. National Intelligence Council (NIC). *Disruptive Civil Technologies Six Technologies with Potential Impacts on Us Interests out to 2025*; Conference Report CR; National Intelligence Council (NIC): Washington, DC, USA, 2008.
7. PricewaterhouseCoopers (PwC). *Information Security Breaches Survey 2015*; HM Government: London, UK, 2015.
8. Xu, L.D.; He, W.; Li, S. Internet of things in industries: A survey. *IEEE Trans. Ind. Inform.* **2014**, *10*, 2233–2243. [CrossRef]
9. Yu, L.; Lu, Y.; Zhu, X. Smart hospital based on internet of things. *J. Netw.* **2012**, *7*, 1654–1661. [CrossRef]
10. Mars, M. Telemedicine and advances in urban and rural healthcare delivery in africa. *Prog. Cardiovasc. Dis.* **2013**, *56*, 326–335. [CrossRef] [PubMed]
11. Wade, V.; Soar, J.; Gray, L. Uptake of telehealth services funded by medicare in australia. *Aust. Health Rev.* **2014**, *38*, 528–532. [CrossRef] [PubMed]
12. Fleming, B. Advances in automotive electronics (automotive electronics). *IEEE Veh. Technol. Mag.* **2014**, *9*, 4–19. [CrossRef]
13. Karagiannis, G.; Altintas, O.; Ekici, E.; Heijenk, G.; Jarupan, B.; Lin, K.; Weil, T. Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions. *IEEE Commun. Surv. Tutor.* **2011**, *13*, 584–616. [CrossRef]
14. Attaran, M. Critical success factors and challenges of implementing RFID in supply chain management. *J. Supply Chain Operat. Manag.* **2012**, *10*, 144–167.
15. Zou, Z.; Chen, Q.; Uysal, I.; Zheng, L. Radio frequency identification enabled wireless sensing for intelligent food logistics. *Philos. Trans. R. Soc. Lond. A Math. Phys. Eng. Sci.* **2014**, *372*. [CrossRef]
16. Ricquebourg, V.; Menga, D.; Durand, D.; Marhic, B.; Delahoche, L.; Loge, C. The Smart Home Concept: Our Immediate Future. In Proceedings of the 2006 1st IEEE International Conference on E-Learning in Industrial Electronics, Hammamet, Tunisia, 18–20 December 2006; pp. 23–28.
17. Alam, M.R.; Reaz, M.B.I.; Ali, M.A.M. A Review of Smart Homes—Past, present, and future. *IEEE Trans. Syst. Man Cybern. Part C (Appl. Rev.)* **2012**, *42*, 1190–1203. [CrossRef]

18. Patton, M.; Gross, E.; Chinn, R.; Forbis, S.; Walker, L.; Hsinchun, C. Uninvited connections: A study of vulnerable devices on the Internet of Things (IoT). In Proceedings of the 2014 IEEE Joint Intelligence and Security Informatics Conference (JISIC), The Hague, The Netherlands, 24–26 September 2014; pp. 232–235.
19. Durumeric, Z.; Adrian, D.; Mirian, A.; Bailey, M.; Halderman, J.A. A search engine backed by internet-wide scanning. In Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, Denver, CO, USA, 12–16 October 2015; pp. 542–553.
20. Thubert, P. *Compression Format for Ipv6 Datagrams over IEEE 802.15.4-Based Networks*; RFC 6282; Hui, J., Ed.; Internet Engineering Task Force: Fremont, CA, USA, 2011.
21. Brandt, A.; Hui, J.; Kelsey, R.; Levis, P.; Pister, K.; Struik, R.; Vasseur, J.P.; Alexander, R. *RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks*; RFC 6550; Winter, T., Thubert, P., Eds.; Internet Engineering Task Force: Fremont, CA, USA, 2012.
22. Shelby, Z.; Hartke, K.; Bormann, C. *The Constrained Application Protocol (Coap)*; RFC 7252; Internet Engineering Task Force: Fremont, CA, USA, 2014.
23. Shelby, Z.; Bormann, C. *6lowpan: The Wireless Embedded Internet*; John Wiley & Sons: New York, NY, USA, 2011; Volume 43.
24. Raza, S.; Duquennoy, S.; Chung, T.; Yazar, D.; Voigt, T.; Roedig, U. Securing Communication in 6lowpan with Compressed Ipsec. In Proceedings of the 2011 International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS), Barcelona, Spain, 27–29 June 2011; pp. 1–8.
25. Yue, Q.; Maode, M. An authentication and key establishment scheme to enhance security for m2m in 6lowpans. In Proceedings of the 2015 IEEE International Conference on Communication Workshop (ICCW), London, UK, 8–12 June 2015; pp. 2671–2676.
26. Perrey, H.; Landsmann, M.; Ugus, O.; Schmidt, T.C.; Wahlisch, M. Trail: Topology Authentication in RPL. **2013**, arXiv:1312.0984v2.
27. Kenji, I.; Matsunaga, T.; Toyoda, K.; Sasase, I. Secure parent node selection scheme in route construction to exclude attacking nodes from rpl network. *IEICE Commun. Exp.* **2015**, *4*, 340–345. [CrossRef]
28. Dierks, T.; Rescorla, E. *The Transport Layer Security (Tls) Protocol Version 1.2*; RFC 5246; Internet Engineering Task Force: Fremont, CA, USA, 2008.
29. Rescorla, E.; Modadugu, N. *Datagram Transport Layer Security Version 1.2*; RFC 6347; Internet Engineering Task Force: Fremont, CA, USA, 2012.
30. Conzon, D.; Bolognesi, T.; Brizzi, P.; Lotito, A.; Tomasi, R.; Spirito, M.A. The virtus middleware: An xmpp based architecture for secure iot communications. In Proceedings of the 2012 21st International Conference on Computer Communications and Networks (ICCCN), Munich, Germany, 30 July–2 August 2012; pp. 1–6.
31. Caro-Benito, R.J.; Garrido-Márquez, D.; Plaza-Tron, P.; Sanz-Martín, N.; Serrano-Martín, J.L.; Castro, R.R. Smepp: A secure middleware for embedded p2p. In *Proceedings of ICT-MobileSummit*; ScienceOpen: Frankfurk, Germany, 2009; Volume 9.
32. Kovatsch, M.; Lanter, M.; Shelby, Z. Californium: Scalable cloud services for the internet of things with coap. In Proceedings of the 2014 International Conference on the Internet of Things (IoT), Cambridge, MA, USA, 6–8 October 2014.
33. Alohali, B.; Merabti, M.; Kifayat, K. A secure scheme for a smart house based on cloud of things (cot). In Proceedings of the 2014 6th Computer Science and Electronic Engineering Conference (CEEC), Colchester, UK, 25–26 September 2014; pp. 115–120.
34. Ding, F.; Song, A.; Tong, E.; Li, J. A smart gateway architecture for improving efficiency of home network applications. *J. Sens.* **2016**, *2016*. [CrossRef]
35. Bergmann, N.W.; Robinson, P.J. Server-based internet of things architecture. In Proceedings of the 2012 IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, USA, 14–17 January 2012; IEEE: New York, NY, USA; pp. 360–361.
36. Ruckebusch, P.; de Poorter, E.; Fortuna, C.; Moerman, I. Gitar: Generic extension for internet-of-things architectures enabling dynamic updates of network and application modules. *Ad Hoc Netw.* **2016**, *36*, 127–151. [CrossRef]