A Survey of Smart House Security

Jaques Clapauch
University of British Columbia
2329 West Mall
Vancouver, B.C., Canada V6T 1Z4
jaquesc@ece.ubc.ca

ABSTRACT
Security is an important concern in day to day life, far augmented when related to sensitive data, such as private information. In a smart home scenario, where applications are constantly communicating with the outside world, previously private data suddenly becomes accessible through non-physical means. That accessibility to previously unreachable means brings forth new threats that must be tackled to ensure proper confidentiality is kept. Furthermore, proper accessibility of the physical devices must be engaged, due to their newfound non-physically accessibly nature. This paper surveys the security threats existent in smart home environments, along with possible solutions to mitigate the threats. Lastly, this paper attempts to integrate the solutions in a cohesive form to be applied to any smart home environment that wishes to best keep high confidentiality, availability and integrity.

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: Security and protection; C.3 [**Special-Purpose And Application-Based Systems**]: Real Time and Embedded Systems

General Terms
Management, Design, Reliability, Security, Human Factors, Standardization.

Keywords
Smart Home; Security; eHealth; Automation; Smart Applications; M2M; Confidentiality; Integrity; Availability.

1. INTRODUCTION
Given recent advances in technology, the use of internet connected smart devices is on the rise, [1] leading to a logical rethinking of the appliance paradigm. Along with technological advances, the idea of a connected home is rather an appealing concept to Americans according to a recent survey [2]. Furthermore, the notion of delegating challenging activities to smart appliances, from cooking to taking care of the elderly, seems rather an appealing development. Due to those factors, one would expect that a smart home would before long turn from a distant dream to a present commodity.

However, due to the large amount of data aggregation and transmission necessary for the proper operation of the smart home, developers must also concern themselves with the security risks involved: users would prefer their private data is not made public; nor would they like attackers to take control of their devices. With the advent of smart homes and appliances, one must then concern themselves with accommodating for these problems (and due to the mostly theoretical nature of smart homes, as they are yet to be widely deployed) and the devising of possible threat scenarios, coupled with solutions to these.

Moreover, smart homes, unlike office environments will not normally feature skilled administrators, but rather average, often technologically unskilled, people. As such, the designers cannot expect the user to spend much time learning complex interfaces or learning how to perform or delegate security tasks [3]. Owing to this, controls and security settings should be simple and unobtrusive, as well as secure.

The division of this paper will be as follows: Section 2 will present the average smart home setting; section 3 will present problems leading from the configurations present in the average smart home setting; section 4 will present currently present solutions to the presented problems; section 5 will conclude.

2. BACKGROUND
The smart house template to be evaluated consists of several devices interconnected to one or more central stations. Each device may serve the purpose of a sensor, a hotspot or a servant [4]. A sensor would comprise a device that merely accumulates data, whereas a hotspot would be a device used for inter-communication between devices, and servants are the devices used to compute results.

Devices within the smart house need not be fixed to the house, but may be able to be removed from the smart home environment and used in a mobile manner (for example a mobile phone or a health monitoring device, such as a heart rate monitor) [4]. Devices in the smart home, much like devices in our own present homes should exhibit features of ownership, such that an unauthorized user should not be able to access a device he does not have the rights to use (such as one's own personal computer, or even the door lock mechanism) [3]. Continuing on the previous point, devices should be enabled to be used by more than one user if necessary. It is further necessary to allow extraneous administrators and other outside users (such as policemen, repairmen, firemen, or simply network administrators) access to certain devices even when the users are not present [3].

It is also important to note that devices should be ultimately cost effective. As such, any device included in the house should not have any security feature severely impact its monetary cost [6]. Continuing in the cost paradigm, it is also assumed that not all devices can deal with high levels of computation (such as advanced encryptions) due to their embedded status, owing to primitive resources and battery powered condition [7].

From current trends in the industry it can be foreseen that not all devices in the house will be from the same manufacturer, and thus some devices may possess similar protocols for communications (such as a standard), but we cannot assume that all devices will do so [7].

Under the same previously stated assumption that we cannot presume users are tech-savvy, we must also allow for simple

interfaces with pre-defined customization abilities not only for security reasons, but for normal use as well [3].We should also assume that in such a template house, all electrical devices capable of exhibiting "smart" behavior will do so, and communications need not be solely within the house, but data may be transmitted outside (i.e.: not simply within devices). Lastly, though connections such as ZigBee and Wi-Fi are the norm in the smart home environment [8], other connections, such as wired connections or Bluetooth can be present [9].

3. THREATS

3.1 Ownership Threats

First and foremost, an important aspect in the implementation of the smart home is to enable the enhancing of some aspects of the applications (for instance, having a stove cook by itself, or a wardrobe sort itself, or temperature to adjust itself) without any detrimental aspects being added. Of those, one of the most important aspects is to keep proper ownership; that is to say, the disallowance of non-permitted users from using things that do not belong to them. Some unknown attacker as such, should not be able to control your stove from outside the house. This is indeed a problem in a smart house: an environment where outside connection is available and devices are made to provide external connections [2, 3, 4, 6, 7].

Another important point to consider is that of data: Within the smart house (especially those specializing in eHealth) data is continuously recorded, be it by means of a camera (for security or eHealth purposes), or credit card information (employed when the user utilizes an online store feature of a device), among other things. Data recorded through those devices could technically be extracted by a skilled adversary if proper protection is not instilled. This category of data can be used to execute a number of malicious dealings, such as directly stealing user funds, mining user data, or even determining user presence. [6, 7]

Data ownership threats also arise between house residents, rather than merely pertaining to outside attackers: in many cases, a resident of a smart-home will wish his actions to remain private from other residents in lieu of constant monitoring. The threat prominently arises in environments where film data is pervasive, and not merely processed in real time; for such environments, a specific resident would not want his house-mate covertly leaving a smart camera on in the room, and later querying and easily obtaining the other resident's actions. One's ownership of data should only extend as far as the data that is pertinent to him, and no more [23].

A further key threat is the possibility of malicious devices being introduced to the system. A malicious device could issue commands to hotspots demanding and propagating data the user may not wish to disclose. Furthermore, malicious devices may convert their non-malicious counterparts through several means, and thus monitor a non-consenting user [7, 24]

An ownership problem also arises upon third parties attempting to access private, though relevant information: A doctor may, for instance require access to patient data that the smart house possesses, which on its own is a harmless procedure. The dilemma arises, however, when the doctor does access the information database; in such a case, he should only have access to pertinent information and no more [25, 26]. That is to say, we do not wish a caregiver to know more information than that which is necessary to care for the patient. The smart home environment is after all, very different from that of the hospital, as the hospital is not a private location; in the patient's home, the patient may engage his environment differently, and may not wish the caretaker to have access to all of the information pertaining to his actions.

3.2 Availability Threats

An important possible threat that should be addressed is that of denial of service: in many instances of smart houses, such as those related to eHealth, it is of the utmost importance that service is not halted, lest the patient being monitored be in danger. As such, any instance that disallows the service to the user should be meticulously protected against[1] [4, 6].

Correspondingly, since all existing items in the house are electronic, power or system failures poses serious real safety threats to the user, as a user may be locked in or out, without access to any supplies (such as water, food or facilities) [27].

On the same note, the fact that most devices are very limited in terms of resources, such as dependence on battery power, makes the devices target to attacks like that of "sleep deprivation," that is to say, continuous communication with the devices to exhaust battery. [28, 29]

Furthermore, though less common, it is also possible to target the wireless networks through jamming attacks, where radio frequencies in use may be super-saturated. In environments such as a smart house, where communication is key for any device access, a well-targeted jamming attack can be catastrophic, completely crippling the entire infrastructure. [29]

Similarly, the fact that many wireless protocols used by ubiquitous devices do not require re-authentication can be attacked via intermittent service failures, leading to man in the middle attacks [28]. A different, though relevant exploit was shown to target Vonage VoIP phones, where a short injection caused the service to shut down, and upon reset, the VoIP device was fooled into reconnecting to an attacker rather than the service provider [30].

3.3 Locality Threats

An additional threat brought forth due to the smart home environment is that of location information leaks. Due to constant monitoring within the house, the user's presence in specific locations can be determined with ease, be it through access to sensitive information (such as videos, or logs), or simply electrical monitoring of specific locations in the house[23, 31, 32]. An attacker can further determine a user's current interactions with specific devices from snooping the wireless connection, which though encrypted, can still leak source and destination information with an accuracy of up to 90% [33].

Additionally due to mobile monitoring, users may be followed and tracked through the clever placements of a number of devices meant to snoop a communicating mobile sensor [34]. Attacks such as these are already in existence, and have been proven to work: an example of such an attack is that of locating a runner

[1] It should be noted, however, that this is on a case by case basis: while it is important to protect against denial of service in an eHealth environment, it is not as important to protect one's toaster from being halted in producing toasted bread, for instance.

using the Nike+iPod Sports Kit, which communicates with a user's iPod to provide the user with their running information. The device does not, however, encrypt its unique ID, and therefore, an attacker using properly placed sensors, can easily determine a target's location [34].

This problem is further exacerbated with the eventual prevalence of large smart environments, with much farther reaches than those of houses. Smart work-places, and even smart cities are the logical consequent of the smart environment evolution, and with their progression, the use of monitoring equipment, as well as the use of wirelessly controlled personal identification will become more prevalent. Therefore, whereas currently an attacker might only be able to accurately locate a person within a house, in the future, it may be possible to accurately locate a person within a city [26, 23]. This is problematic even in cases where an ID is not actively coupled with a name or other identifiers, as an attacker can de-anonymize the ID by simply searching for the most prevalent ID in a target's house [26].

3.4 Data Leaks

With the increase of wireless communication, data can be more easily snooped. Though one would think current efficient encryption mechanisms would prove sufficient to halt this threat, it is not always the case. In one specific situation, it was proven that with a prior database of films and 10 minute traces of wireless data, one could determine with 73% certainty which film was being watched streaming through the Slingbox hardware, even though the transmission was encrypted. Given a 40 minute trace, the certainty rose to 89%, with some specific movies performing as well as 100% certainty [34]. The same paper that discusses this attack also notes that this threat does not simply lie with television information leakage, but rather that "one can infer the origins of encrypted web traffic or infer application protocol behaviors from encrypted data." Therefore, due to the high number of devices communicating wirelessly in a smart home, one can conclude that a larger number of data should be leaked, even given encryption.

In a similar attack as the one presented above, [35] determines that power supplies in modern television sets produce discernible signatures when it comes to electromagnetic interference, allowing for the determination of content being viewed. Through the analysis of electromagnetic interference using a prior database of films and 15 minute traces, a cross correlation of same content of upwards of 98% was yielded. Though the study reveals that this is not consistent over all television sets (some performed quite poorly, yielding no better than 60% cross correlation), the majority of the sets proved to be quite strong nonetheless, yielding over 90% cross correlation, even in the presence of considerable noise. The authors of this work further hypothesize that comparable attacks may be conducted to determine similar information in regards to computers, DVD players, printers, game consoles and washing machines. This attack is quite likely in a smart house that saves and propagates electrical information due to smart-grids.

Another similar attack shows the possibility of revealing the language spoken in a VoIP conversation from encrypted wireless data [36], further implying that as long as devices communicate wirelessly, even with encryption present, some private data is not safe.

3.5 Other Attacks

Following is a list of attacks that do not exactly fall into exactly one of the previous extensive categories (though they may be a combination of several categories of threats), yet are still important and should be tackled.

1. Through online or physical means, an adversary may impersonate a user, and with the user's credentials he may gain access to unauthorized appliances [7].
2. On the same track as the previous point, an adversary might create false credentials to respond to a patient alert in an eHealth smart home. Not only should this grant him access to the user's abode, but the user will likely not be rescued, because the system processed the fact as having already occurred [4].
3. Continuing on the same point, a user who may control appliances from a distance may pose physical danger to the user
4. Appliances might be compromised, and used as zombie machines [7].
5. Appliances might be compromised, and their trusted status may be used to issue an attack on the user's personal computer on the same network [7].
6. Compromised machines may misdirect their output, thus executing possible phishing attacks to the user [7].
7. Cameras and other recording devices may be compromised, and may be used for wiretapping purposes [7].
8. On the topic of confidentiality, and not as much an attack, the lack of credentials may lend a friend of a user (i.e.: one with physical access, but perhaps not direct permission from the user) the ability to see data he normally should not be able to[2] [3].
9. A trusted device may be manufactured with malicious code, thus compromising the entire house [7].

4. SOLUTIONS

For each possible threat and attack presented, solutions have been imparted, such as location awareness technologies, methods of authentication, encryptions, etc.

4.1 Device Ownership

One of the first resolutions regarding the ownership threat dilemmas in ubiquitous computing was introduced by Stajano and Anderson in the form of "The Resurrected Duckling Security Policy Model" [29, 37]. Within this model, we are told to approach the problem analogously, identifying devices as a family of ducks: a master device is deemed a mother duck, whereas a slave device is a duckling. A duckling may be either imprinted or imprintable: an imprintable duckling may be granted a soul by the mother. A soul in this sense is a shared secret that binds the slave device to the master device. So long as the duckling is imprinted with this soul, he will obey the mother duckling and no other

[2] Another interesting point to note (albeit not entirely related to security), some users further find it embarrassing to reveal to their friends or acquaintances that they are not allowed access in specific devices, so credentials should desirably be as unnoticeable as possible [3]

devices. A soul is extracted upon completion, with the death of the duckling, at which time, the duckling is imprintable again, and may be resurrected by another potential mother duckling. Any number of mother ducks may simultaneously instill souls into ducklings, meaning a slave device may be controlled by more than one master at a time.

The granting of the soul is recommended to be done physically via a non-wireless channel, or at the very least through "a channel whose confidentiality and integrity are axiomatically guaranteed."[26] This is done in accordance to "the Big Stick Principle," which states that "whoever has physical control of the device is allowed to take it over" [26, 38]. This is appropriate as it corresponds to the manner through which we access devices outside of a smart home environment, that is to say, through physical presence.

Initially, the concept allowed ducklings to interact among themselves, but disallowed devices issuing orders to other devices they do not control; however, in a later paper, Stajano expands on the concept, allowing mother ducks to instill policies to ducklings through the same secure channel. These policies would define what actions are allowed and by whom, yielding, if necessary, full control of the duckling to any other devices [37].

A centralized equivalent is presented by Naqvi and Riguidel, where ownership of data is dealt with by an "Infosphere", and a "Security Domain" remains in charge of protection and control [28]. The authors further propose that encryptions be set by the user, allowing her to choose between performance and security for specific devices. Additionally, their implementation makes use of virtualization to disallow applications located within a servant device to interfere with one another. Another decentralized solution is provided by Lee et al [24], where each device must be authenticated through a "Security Manager," but their access control data is managed by a "Smart Portal Server." Though lacking virtualization of applications within a servant, the remainder of this solution is quite similar to Naqvi and Riguidel's.

After the Resurrected Duckling Model, a number of methods for distributed access control were defined for this medium, many expanding on the model, and others, taking tangential paths. Such means presented tend to have in common their necessity of a mobile method of authentication. Such methods for authentication range from biometrics to passwords, to devices (such as smartphones or pocket watches) to RFID tags [3, 4, 20, 18, 27]. Though the device which achieves authentication deviates, the elementary notion is always constant: the device is mobile and constantly placed alongside a user, be he a resident or guest, and achieves (through methods described in section 4.3) bounding of user location in relation to the device to be connected to[3]. Another commonality found within these works is that different levels of access are necessary for different users, thus requiring a policy, be it self-configuring or manually set.

Conwell et al provide an additional methodology that falls within the resurrected duckling model, wherein users use their smartphone devices to authenticate, configure and update access control lists [27]. The ubiquitous quality of smartphones and their ever-presence beside the user further allows the evolution of the model to easily permit reactive access control permissions; that is to say, the device may allow a user to respond to access grant requests from other users. Thus access list population may occur ad hoc, and rather than having to type out lengthy and complex lists, the population of the list is simply reduced to a modest prompt. The authors further present that such a method could be used for unlocking doors for guests in the house, and note that the commodity this provided was complimented by the subjects of the study, as it allowed them to "unlock doors without having to get out of their chairs."

Also following up on the Resurrecting Duckling Model, Argyroudis and O'Mahony develop AETHER, whereupon they establish more detailed connection methods and interactions [18]. In AETHER, devices would come pre-installed with asymmetric key pairs, and have their own policy lists, wherein rights are directly associated with actions. It is lightly hinted that one may use auto-configuration to evolve policy sets over time, but this approach is not given much attention. The binding of devices is specified as a key exchange through a secure location-limited channel (such as touch or infrared link); following such an exchange, policies are passed through a secure channel, and refreshed given a short time period. The refreshing method is used in lieu of certificate revocation lists. If a device is to come out of range and for longer than the validity period, the binding expires, and the devices must reconnect via the same secure location-limited channel.

In regards to policies, AETHER allows both positive and negative policies, establishing what is specifically allowed and disallowed. The policies further allow conditions, which specify restrictions related to time, location, and other factors. The concept of conditions seems to be quite common among other models [24, 28]. Moreover, AETHER allows a policy-maker to specify further policy-makers for devices, as well as their delegation depth; that is to say, to what extent the new policy making users may specify new policies.

Solutions such as these and other policy setting schemes similar to the Resurrected Duckling Model, though allowing decentralized management of devices and data, suffer from the requirement of onerous creation of policies, which is neither an easy feat for technologically untrained users, nor a much desired feat for those who are technologically able, due to the repetitiveness and laboriousness of the task.

Kim et al suggest a mechanism where access control policies are pre-set into groups, capturing most, if not all home owners and visitors [3]. Through this method, whenever a visitor or another newly introduced resident is within the home, a resident or administrator may place him within one of the pre-set groups (Full Control, Restricted Control, Partial Control, and Minimal Control). Any access made outside of the policies groups would have to be manually granted by a resident or administrator. It is also suggested that on top of that all accesses be logged to be audited to account for discrepancies.

Hoque et al tackle the problem in a tangential manner, rather than allowing for easy configuration, they attempt to create a self-configurable system, arguing that some elderly patients located within the e-health environments would find even simple policy creation unmanageable [6]. They further argue that common current policy configurations fail to account for intuitive intricacies of trust, merely focusing on an implicit, inaccurate view. In their approach, all devices possess a list mapping trust values for each service requested by a given neighboring device. Upon an interaction request, a device estimates and sets a trust

[3] That is to say, it helps the device being connected to identify that a user connecting to it through an authentication device is physically present.

level for the requesting device, based on the security level of the requested service, as well as a user's disposition value. Through proper use, trust values are increased, and more access is granted. Improper use leads to a decrease of trust, coupled with a decrease of access. This however, can be exploited with mimicry attacks such as those used to target on Intrusion Detection Systems, whereupon a malicious device can escalate its privileges by following the dictated set of rule, only to later attack undetected [39].

Likewise, Seigneur et al endeavor to mimic the process of human trust in an attempt to automate trust policy configurations [22]. They argue that the ease we achieve through Plug and Play technology should be attempted for later management. Within this auto-configuration arrangement, devices may recommend trust levels to other appliances. The installation of appliances within the home would be propagated to other appliances, and dependent on the installer, a level of trust would be assigned to this appliance by others. For instance, were the house owner to install a new door lock, other devices would assign that device a higher trust than if it were installed by a lesser source. Furthermore, dependent on the risk associated with the corruption of the already installed devices (which can be preset by the manufacturer), they will choose to follow the recommendations given by this new device differently. In the previous example, given that an owner installs a door lock, a television set will likely easily follow the door's recommendations, whereas more sensitive devices such as a safe or another door might not.

Temporal coexistence further augments trust between appliances, such that if two devices coexist within the home for extended periods of time, their trust levels towards each other rise. The authors further state that biometrics could further ease this classification of trust, allowing a process to place low trust users (such as guests) detected to interact with higher trust users (such as residents) at an escalated level of trust. Continuing on the previous example, a guest might enter the house through a key provided by a resident. As such, the house door would identify this user as trusted, as he possesses a house key, independent of the fact that he does not possess an owner's equivalent biometric equivalence. This trust level is propagated throughout the house, and as such, the guest is allowed to use minor devices, such as the television. However, the guest has no access to other rooms or the kitchen, since they are considered to be more sensitive locations. The guest then might proceed to watch television for some time, thus building trust with the television set. Since the television set has, over time built trust with the kitchen, and since the user has escalated his trust level with the television over use, he is now granted access to the kitchen. Additionally, were the guest to engage in a phone conversation with a resident, a biometric on the phone might recognize the resident's voice and further escalate the guests privilege due to the interactions with the user.

The approach of auto-configuration, however, fails to overcome a number of section 3's previously established vulnerabilities: One of the more severe threats this configuration fails to circumvent is that of malicious devices being integrated within the smart house. This specific class of threat is previously mentioned in section 3.5, and concerns either the existence of devices manufactured with malicious code, or compromised devices. The compromising of a number of trusted devices may lead to further corruption of appliances, at which point an adversary might gain control of trust assignments within the house, even though he may lack control of the majority of appliances. Such methods may give an adversary access to the house, or even in some cases may lock a legitimate user out. Falsification is another method through which an adversary might take advantage of this configuration: through the recording of specific biometrics, an adversary might escalate his trust, such as the replaying of a legitimate resident's voice [40, 41], or the use of masks or photos with the user's likeness [41, 42].

A similar approach is taken by Azman et al for automatic trust calculation [17]. Like Seigneur at al, trust escalates with interactions (be it with a house owner, or other devices), however, unlike Seigneur et al, this method also uses routing selections alongside temporal measurements to determine the trustworthiness of a user: In this approach, a user who detours from a normally traversed path, or presents temporal anomalies (that is to say, the user exceeds a temporal threshold in a location or activity), will be deemed suspicious and have his trust level decline.

Solutions such as IBM's SPARCLE, conversely, attempt to rather facilitate the entry of access control policy data, by creating a more human-readable interfacing language [19]. In such cases, one can grant access to people and devices by writing the rules in simple English, such as "guests may access the television," or "police may open the door." Though such entries might be time consuming, it is more likely that laymen may be able to enter and understand the policies. Furthermore, unlike automated and pre-fabricated access control lists, the resulting actions will more accurately follow the exact desired outcome.

4.2 On the Prevention of Data leaks

Kim, Beresford and Stajano propose that to limit availability to sensitive data, only summaries of present data are stored in any pervasive storage device [25]. As such, real time measurements can only give access to data occurring at that time window and no prior data, to disallow more sensitive data to purvey unwanted inferences (For instance a caregiver who monitors a patient's detailed heart rate might be able to imply details about a patient's more intimate encounters). In such cases, a summary of all data will be just as useful for the caregiver, and as such more minute details could be foregone. It is also suggested that any further data necessary that cannot be acquired through the summary necessitate the patient's consent.

It is additionally stated that any caretaker may only have access to data stored specifically in a temporary repository, out of which which it cannot be transferred.

The defense of direct data leaks from such sources as wireless and electrical signals, however, proves to be significantly trickier than the creation of policies: In their paper, Enev et al [35], upon expounding the possible leaks present in power line electromagnetic interference present as a possible solution the connection of each vulnerable switched-mode-power-supply-powered-device to an electrical isolator, so that high frequency noise is not propagated into the power line. This is however, somewhat a monetarily costly solution, as it requires the installation of a device behind every electronic appliance. Another solution proposed by the authors is that of high-energy broadband noise introduction into the power line. However, this solution also causes a number of complications, as noise introduced must conform to FCC regulations, and even then, it might interfere with legitimate power line-based communications. Selective frequency band filtering of only vulnerable switched-mode power supply powered device noise might be the more viable solution of those

presented, as it would achieve the same result as the former solution, but also prevents interference with power line communications.

In regards to wireless information leaks through encryption, Agarwal et al propose that constant rate data production might prevent an attacker from determining the movie being streamed [34]. However, the authors also argue that solutions such as the one presented may significantly affect bandwidth consumption, and would not prevent an attacker from still determining when and for how long the user watches movies. In their paper regarding language leaks related to VoIP conversations, Ballard et al present possible padding of packets to greater packet sizes [36]. Dependent on the amount of padding, the discernibility of language decreases from beyond 66% (with no padding) to 27% with 192 or 256 bits, and 6% with 512 bits. However, in the case of 192 or 256 bits padding this dimension of determinism is still quite above that of random guessing and is, as such, still undesirable. Furthermore, this solution still introduces a large overhead in terms of bandwidth, leading to nearly 42% overhead for padding to 512 bits. Libertore and Levine reach a similar conclusion in their paper of inferring the source of encrypted HTTP connections, wherein padding also dramatically decreases accuracy, but at a high cost to performance [33].

In their paper, Canny and Duan attempt to impede an attacker from gaining access to sensor data recorded in their absence [23]. To do so, they propose a scheme where all data pertaining to a user's presence (such as recordings and localization data) be encrypted with a randomly generated secret key, which in its turn is encrypted by the public keys of all users present during the recordings. Each different encryption is placed within a different tabular position, which is calculated via a hashing function that takes as input the user's public key. This function allows the location and placement of the encrypted secret key. All other empty locations are filled with random numbers. To allow access to privileged parties (such as policemen, repairmen, firemen, or network administrators), a master key is also saved, only decryptable by a matching private key in possession of the privileged parties.

An authentication device is a mobile device used to store a user's public key which interfaces with a smart location to grant access during physical presence; therefore, a user lacking his authentication device will not have access to data as a fail-safe default. This system also allows the exclusion of access control lists, and can thusly function without knowledge of the user's identity in situations where the user must interact with an untrusted smart environment. The authors further recommend that each smart location be equipped with a display which presents the current number of occupants within the room; if this number does not match the visible number of residents, it can be concluded that something is amiss and a rogue authentication device may be present.

4.3 Location Awareness

In order to circumvent outside users from using technology which they should not, Manish suggests that specific zones within the home should be created, and different features be enabled for each appliance within each zone. For instance, though you may check the temperature of a stove from a distance, you may not set it except when within the room. Locality can be established by using extra sensors, and for the more dangerous appliances, communications can only occur via shorter range signals (such as infrared, as opposed to Wi-Fi). [9] It is, however not an infallible technique to use communication range to represent physical locality, as Capkun et al [43] have shown; in their paper, they present a method of amplifying, and thus relaying signals from a keyless entry key onto an automobile, thus opening its doors and turning its engine on, when they key really is not physically present. It is feasible that such attacks could be adapted to the smart-home model, thus rendering locality establishment moot. As suggested in the paper, one must take immense care to ensure the distance bounding protocols are safe from relay, which according to the authors, can be achieved with a verifiable multilateration protocol.

The problem of locality does not only befall unto the device process of ascertaining the presence of a user, but also encompasses the charge of maintaining a user's location unknown in an environment where his presence is constantly checked. In their paper, Al-Muhtadi et al present the novel idea of mist routing to circumvent locality threats [31]. In their model, sensors are able to detect the presence of users, but lack the ability to identify the users. Furthermore, this is combined with a novel routing protocol to further protect the user's location. In this protocol, a sensor is identified as a leaf within a graph, where each node is populated by a "Mist Router." Each node level upwards represents a further level of physical locality (for instance, within a campus, a student's parent node would be his room's router, and that node's parent would be the floor's router, followed by the building's router, and then campus router, and so on).

Special Mist Routers that contain the true identity of a user, as well as partial knowledge as to how to route to them are called "Lighthouses." The closer to the root the Lighthouse resides inside the graph, the more private the user's location is (that is to say, if Alice chooses as a Lighthouse the campus router, though people will be able to find she is present in the campus, the will be unaware as to where), but the greater the hit on performance (since it will require more hops to communicate, as the router is physically farther). Further, the closer the Lighthouse is physically, the more relocation will be necessary for a highly mobile user (that is to say, if Alice chooses her present room's router as her Lighthouse, and moves to another room, she must choose a new Lighthouse upon relocation).

Upon Lighthouse setup, each Mist Router will maintain a relation containing the ID of the user and the link required to reach her; the lighthouse, along with that information will also couple the ID with the user's name, and a key to decrypt her messages. Note, however that intermediate Mist Routers are never aware of a user's Lighthouse, other than the fact that it resides upward. If a user wishes to communicate with another user, they must first send their message to their lighthouse, along with the other user's ID or other attributes. If an ID is unknown, a lookup based on attributes is commenced, and the searched user's Lighthouse will respond with an ID. If the ID is known, this lighthouse need only route to the Lighthouse containing that ID. After setup, communications are protected via asymmetric key encryptions, using a timestamp to prevent replay attacks. Through this, though the Lighthouses are aware of the identities of the endpoints of communication, they do not know their respective users' locations, maintaining their location privacy.

Stajano, however, suggests a method of that uses anonymous IDs to allow an attacker to determine which ID correlates to whom [26]: Through a check of the most predominant ID in a residence location, we can conclude who the resident is, thus pairing ID and

real identity. To circumvent this threat, he advises the creation of "mix zones" in populous locations, within which IDs will be scrambled, thus confusing an attacker. He finally suggests that the best way to truly prevent attackers from snooping one's communications and determining locations, is to maintain solely one-directional communications from extraneous devices to mobile devices (akin to how GPS devices communicate).

In their study of the Nike+iPod [34], Agarwal et al argue that communicating mobile devices can be a threat to one's locality, as a leak of its persistent unique ID may allow an attacker to track a user's precise location through sniffing. As such, the authors maintain that strong encryption such as AES, using randomized IDs, recomputed at each idle moment, should be sufficient to circumvent the attack, however it may prove to be difficult due to the limited performance and battery life available to mobile devices

4.4 Device Authentication

Authentication for devices is a necessity, as the configuration is meant to be elastic (that is to say, devices should be able to be added or removed at will), and in order for trust to exist, authentication methods are necessary. In one of the more interesting methods, items are connected via the physical interaction of checking the device for a physical code, and manually inputting it on a hotspot device, and vice versa. Furthermore, this method of authentication allows for different encryption for data transfer between all devices, as they each use their code as a key. [4, 6, 7, 24]

Han et al present a more detailed view of the method of authentication [24], wherein a user must register a device through a hotspot, which will issue a portal run by the device manufacturer a request to confirm the validity of a certificate issued by the device. Following such a check, a manual exchange of codes will be required by the user, to identify that the device being registered is indeed the one owned by the user. Following this step, the hotspot will manufacture a set of private and public keys and will exchange them with the device through an encrypted channel.

As per Pishva and Takeda, one of the greatest concerns in regards to device authentication and communication within a smart home is that of creation of standards [7]. Heterogeneity as it stands in regards to smart devices is quite prevalent[4], and if that quality carries on towards communications and authentications, it would present quite a problematic challenge in regards to security in an environment where collaborative communication is vital.

Lastly, as stated by Naqvi and Riguidel, common cryptography can be easily translated into this field to prevent eavesdropping, and protect authentications, and for all intents and purposes as it stands is enough for this problem, and should be utilized mostly unchanged [28].

4.5 Availability

In regards to circumventing sleep deprivation attacks, Stajano and Anderson propose data communication directed at devices with limited resources be directed through a reservation mechanism, which would prioritize actions and only enable them if their priority passes a threshold [29]. This could then be used for preventing communication from being flooded between devices, by only forwarding high priority messages, and sending a summary of other messages in a timely manner otherwise.

The authors also target jamming attacks by ascertaining that in their occurrence, devices may commence spread spectrum communications or frequency hopping to prevent them from achieving a denial of service. They however argue that in the commercial world, such attacks may be dealt with in a more physical manner, such as complaining to the authorities, and having the operator of the jamming station arrested.

Attacks such as those that target ubiquitous devices which do not require re-authentication and fall victim to man in the middle attacks, can be thwarted through periodical (though infrequent, due to limited resources) re-authentication [28]. Furthermore, devices can be kept from failing due to vulnerability exploits due to more extensive fuzz testing, and communications can be kept from being hijacked through encryption, such as SSL, TLS and SRTP [30].

Lastly, though we did not observe any resolution to the power and system failures conundrum in the literature, we advise that in order to protect the user, the system should default to relinquish use of essential devices in such circumstances. Namely, devices constituting survival necessity, such as water, food, restroom facilities, doors allowing access to these areas and exits (such as those from a room, or from a house to the outside), should default to function for anyone. Conversely, entries other than those leading to facilities or kitchen area should remain closed, unless they lead to an area known to contain a user[5].

4.6 Guest Access Control

A newfound issue apposite the smart home is that of guest access control. Alongside the common problem of device utilization by habitual users, further dilemmas arise, such as that noted on Section 3.5: not only does a user wish to disallow a guest from a number of actions; he does not wish the guest to know he is deemed untrusted. Unless given some tool to properly circumvent such a social taboo, the user will tend to set looser policies of access controls to keep from disclosing his distrust [3].

Moreover, Johnson and Stajano argue that guests should not have to be given accounts [20], nor should they be dealt with as strangers would: Specifically, a guest should be able to access the television set, but he should not need to have to be registered as a permanent occupant to do so. They further maintain that in preserving past customs we should perhaps imitate the non-smart-environment instance wherein a guest is given possession of the house keys until they leave, by having certain rights granted upon entry and revoked upon exit.

Johnson and Stajano go on to provide a guest-specific[6] temporary access control scheme wherein a guest is authenticated manually rather than automatically, and without need of prior policy creations. Using this scheme, a guest would be required to press a physical button on the device to access it, which would in turn cause the device to produce a nonce, which the user would input

[4] As can be seen quite predominantly in the smartphone market in terms of iPhone vs. Android vs. Blackberry vs. Windows Phone, etc.

[5] This instance is presented in case children, or incapacitated users reside in a specific area, and cannot exit on their own

[6] As opposed to the schemes provided on section 4.1, which could be used for both users and guests.

on his authentication device to complete the pairing[7]. The authors continue, contending that the burden of guest access control policies be placed on the manufacturers. Such classes of actions to be provided by the manufacturers are subdivided, providing actions that any one physically present may perform, actions requiring physical presence and resident authorization once, actions requiring resident authentication at each access, and actions that may never be performed by non-residents. Lastly, if a guest is to reside for extended periods within the house, the guest will be given control of areas where he resides through a temporary account. Namely, if a guest is residing within a room, control of all devices within the room should be given to the user, however, the house owner will maintain administrative control over all devices, allowing him to remove the guest's access control capabilities, but not vice –versa.

5. FURTHER DISCUSSION AND CONCLUSION

In our exploration of the world of smart home security, we have encountered a number of imaginative and interesting solutions to tackle the problems this new medium carried. No lone solution, however, proves to solve all problems presented in the paper (and probably other unknown problems only the future will reveal). Also, although the tapestry of challenges is immense, few solutions exist due to the novelty of the field[8]. Very few areas of this vast topic have been fully explored, and though theoretical solutions exist, they are rarely implemented outside of a testing environment: though we will find select smart devices in the open, such as smartphones, smart TVs, VoIP enabled phones, among others; fully interconnected homes are rather rare outside of experimental settings.

We believe that we are, however, reaching an era where pervasive computing is becoming a prevalent paradigm, and as such, this topic will likely soon undergo an upsurge of the likes of those experienced as of late by the fields of mobile phone technology and portable media players. In order to reach that level, we must first establish proper security and usability pertinent to a field of this sensitivity; after all, one should not build a car when they don't know how to achieve stoppage. As can be seen by the literature, we seem to be reaching a point where the usability of this technology is accessible to non-experts, and the security is nearing a stage sufficient for the integration with living environments. In such a manner, it is best to incorporate dispersed concepts into a single model, to finally achieve a level of integration able to combat all possible vulnerabilities present in the current model of smart environments.

To begin with, though the Resurrected Duckling Model and its descendants do prove to be suitable, they are quite taxing for the layman. As such, Seigneur et al [22] and Azman et al's [17] evolution of the Resurrected Duckling Model should appropriately ameliorate circumstances, granting the layman user the ease of use necessary for home environments, as allowed due to intelligent automation. We do, nevertheless argue that these techniques should only be applied after an initial set up as specified by Kim et al [3], of factory pre-set policies as related to groupings of users; from this basis, auto-configuration should be able to properly augment or diminish access. All extraneous rules, which could not be determined through automation or pre-set policies, could be added via a policy creation human-readable interface language akin to IBM's SPARKLE. And what better authentication device than the ever prevalent smartphone, which predominates in the mobile markets encountered today [45]?

Data leaks can be prevented through the techniques presented in section 4.2, of only allowing the emergence of data from the smart home to outsiders in specific special occasions and usually only in summarized form. The padding of packets and the installation of special devices to prevent electrical leaks should further disallow sensitive data from being inferred from signals exiting sensors. Lastly, Canny and Duan's method of encryption [23] should make sensor data unavailable to those who are not present, as well as inform the present users who will be able to access that data.

The creation of physical assurance through localization, coupled with communication through shorter range signals (such as infrared) appears to be the more practical solution in terms of allowance of interfacing with devices. To disallow location pinpointing, the use of mist routers, coupled with fluctuating IDs seem to be a step in the right direction.

As echoed across a number of works, device pairing should perhaps include manual intervention rather than simple plug and play, where a user enters a set of digits printed upon a device or a nonce into a hotspot to ensure he is connecting to the device he really wants to connect. The further use of certificates to ensure the device is not malicious seems reasonable. Prioritized actions in devices to prevent sleep deprivation attacks, encrypted communications, and proper fuzzing and fault injections tests to prevent availability threats should all together be enough to help prevent a large class of denial of service attacks.

Lastly, it would be prudent to echo the words of Pishva and Takeda [7], in that it is vital that a standard be devised and followed by these devices to achieve proper security, lest these steps be for naught.

It is also paramount that these threats and their associated solutions presented as well as new threats be rethought and resynthesized occasionally, respectively. Only by frequently questioning our assumptions, can smart home security remain always one step ahead of attackers.

6. ACKNOWLEDGEMENTS

We would like to acknowledge the help and insight provided by Dr. Konstantin Beznosov, who not only provided us with the idea, but helped us every step of the way in acquisition and selection of literature, and providing valuable constructive criticism, to aid us in bettering our survey. We would also like to acknowledge the help of Dr. Sathish Gopalakrishnan, for the initial idea of a study on Smart Homes, as well as the constant help and support provided by him. Lastly we would like to acknowledge the support of Ildar Muslukhov, Yazan Boshmaf, and Shane Wang, in terms of constructive discussions and ideas for furthering this survey.

7. REFERENCES

[1] Shiels, M. 2011. Cisco Predicts Internet Device Boom *http://www.bbc.co.uk/news/technology-13613536*

[7] The observant reader will find some similarities shared between this method and that used in Bluetooth device pairings.

[8] Though the notion of electrified and automated homes have existed far prior, the idea of interconnected ubiquitous computers within the house was only first publically proposed by Mark Weiser in 1991 [44]

[2] Dawson, M. 2005. Smart Kitchens Could Cook Up a Strong Future *http://realtytimes.com/rtpages/20050222_smartkitchens.htm*

[3] Hyun-Jin Kim, T., Bauer, L., Newsome, J., Perrig, A. and Walker J. 2010. Challenges in Access Right Assignment for Secure Home Networks. Usenix HotSec '10.

[4] Compagna, L., El-Khoury, P., Massacci, F., and Saidane, A. 2010. A dynamic security framework for ambient intelligent systems: a smart-home based eHealth application. In Transactions on computational science X, Marina L. Gavrilova, C. J. Kenneth Tan, and Edward David Moreno (Eds.). Springer-Verlag, Berlin, Heidelberg 1-24.

[5] Busnel, P., El-Khoury, P., Giroux, S., and Li, K. 2008. Achieving Socio-technical Confidentiality Using Security Pattern in Smart Homes. In Proceedings of the 2008 Second International Conference on Future Generation Communication and Networking - Volume 02 (FGCN '08), Vol. 2. IEEE Computer Society, Washington, DC, USA, 447-452. DOI= http://dx.doi.org/10.1109/FGCN.2008.227

[6] Md. Endadul Hoque, Farzana Rahman, Sheikh Iqbal Ahamed, and Lin Liu. 2009. Trust based security auto-configuration for smart assisted living environments. In Proceedings of the 2nd ACM workshop on Assurable and usable security configuration (SafeConfig '09). ACM, New York, NY, USA, 7-12. DOI= http://doi.acm.org/10.1145/1655062.1655065

[7] Pishva, D., Takeda, K. 2006. A Product Based Security Model for Smart Home Appliances. Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International , vol., no., pp.234-242, Oct. 2006

[8] Yan, Y., Qian, Y., Sharif, H. 2011. A Secure Data Aggregation and Dispatch Scheme for Home Area Networks in Smart Grid. Global Telecommunications Conference (GLOBECOM 2011), 2011 IEEE , vol., no., pp.1-6, 5-9 Dec. 2011

[9] T. I. Manish. 2008. A Location Based Security Implementation in Smart Home. In Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications (HPCC '08). IEEE Computer Society, Washington, DC, USA, 1007-1011. DOI= http://dx.doi.org/10.1109/HPCC.2008.174

[10] Kim, H., Oh, J., and Choi, J. 2006. Analysis of the RFID Security Protocol for Secure Smart Home Network. In Proceedings of the 2006 International Conference on Hybrid Information Technology - Volume 02 (ICHIT '06), Vol. 2. IEEE Computer Society, Washington, DC, USA, 356-363. DOI= http://dx.doi.org/10.1109/ICHIT.2006.80

[11] Perrig, A., Szewczyk, R., Tygar, J. D., Wen, V., and Culler, D. E. 2002. SPINS: security protocols for sensor networks. Wirel. Netw. 8, 5 (September 2002), 521-534. DOI= http://dx.doi.org/10.1023/A:1016598314198

[12] Agarwal, S., Peylo, C., Borgaonkar, R., and Seifert, J. 2010. Operator-based over-the-air M2M wireless sensor network security. Intelligence in Next Generation Networks (ICIN), 2010 14th International Conference on , vol., no., pp.1-5, 11-14 Oct. 2010

[13] Hongsong, C., Zhongchuan, F., Dongyan Z. 2011. Security and trust research in M2M system. Vehicular Electronics and Safety (ICVES), 2011 IEEE International Conference on , vol., no., pp.286-290, 10-12 July 2011

[14] Lee, H., Lee, H., and Han, J. 2007. The Efficient Security Architecture for Authentication and Authorization in the Home Network. In Proceedings of the Third International Conference on Natural Computation - Volume 05 (ICNC '07), Vol. 5. IEEE Computer Society, Washington, DC, USA, 713-717. DOI= http://dx.doi.org/10.1109/ICNC.2007.723

[15] Busnel, P. and Giroux, S. 2010. Security, privacy, and dependability in smart homes: a pattern catalog approach. In Proceedings of the Aging friendly technology for health and independence, and 8th international conference on Smart homes and health telematics (ICOST'10). Springer-Verlag, Berlin, Heidelberg, 24-31.

[16] Kim, G. W., Lee, D. G., Han, G. W., and Kim, S. W. 2007. Security technologies based on home gateway for making smart home secure. In Proceedings of the 2007 conference on Emerging direction in embedded and ubiquitous computing (EUC'07). Springer-Verlag, Berlin, Heidelberg, 124-135.

[17] Nasution, S., Hartel, P., Suryana, N., Azman, N., and Sahib, S.. 2010. Trust Level and Routing Selection for Mobile Agents in a Smart Home. In Proceedings of the 2010 Second International Conference on Computer Modeling and Simulation - Volume 03 (ICCMS '10), Vol. 3. IEEE Computer Society, Washington, DC, USA, 445-450. DOI= http://dx.doi.org/10.1109/ICCMS.2010.463

[18] Argyroudis, P., and O'Mahony, D. 2004. Securing communications in the smart home in Proceedings of International Conference on Embedded and Ubiquitous Computing.

[19] Brodie, C. A., Karat, C.-M., And Karat, J. 2006. An Empirical Study of Natural Language Parsing of Privacy Policy Rules Using the SPARCLE Policy Workbench. In Proceedings of the Usable Privacy and Security (SOUPS).

[20] Johnson, M., And Stajano, F. 2006. Usability of Security Management: Defining the Permissions of Guests. In Proceedings of Security Protocols Workshop.

[21] Kostiainen, K., Rantapuska, O., Moloney, S., Roto, V., Holmstrom, U., and Karvonen, K. 2007. Usable Access Control inside Home Networks. Nokia Research Center Technical Report NRC-TR-2007-009.

[22] Marc Seigneur, J., Jensen, C. D., Farrell, S., Gray, E., and Chen, Y. 2003. Towards Security Auto-Configuration for Smart Appliances. In Proceedings of the Smart Objects Conference.

[23] Duan, Y., and Canny, J. 2004. Protecting user data in ubiquitous computing environments: Towards trustworthy environments. In Workshop on Privacy Enhancing Technology.

[24] Lee, D.G., Kim, G.W., Han, J.W., Jeong Y., Park, D. 2008. Smart Environment Authentication: Multi-domain Authentication, Authorization, Security Policy for Pervasive Network. In Ubiquitous Multimedia Computing. UMC '08. International Symposium on , vol., no., pp.99-104, 13-15 DOI=10.1109/UMC.2008.28

[25] Kim, J., Beresford, A.R., and Stajano, F. 2006. Towards a security policy for ubiquitous healthcare systems. In Proceedings of the 1st international conference on Ubiquitous convergence technology (ICUCT'06), Frank Stajano, Hyoung Joong Kim, Jong-Suk Chae, and Seong-Dong Kim (Eds.). Springer-Verlag, Berlin, Heidelberg, 263-272.

[26] Stajano, F. 2010. Security Issues in Ubiquitous Computing. In H. Nakashima, H. Aghajan, J. C. Augusto (Eds.). Handbook of Ambient Intelligence and Smart Environments, Springer.

[27] Cornwell, J., Fette, I., Hsieh, G., Prabaker, M., Rao, J., Tang, K., Vaniea, K., Bauer, L., Cranor, L., Hong, J., McLaren, B., Reiter, M., and Sadeh, N.. 2007. User-Controllable Security and Privacy for Pervasive Computing. In Proceedings of the Eighth IEEE Workshop on Mobile Computing Systems and Applications (HOTMOBILE '07). IEEE Computer Society, Washington, DC, USA, 14-19. DOI=10.1109/HOTMOBILE.2007.21 http://dx.doi.org/10.1109/HOTMOBILE.2007.21

[28] Naqvi, S., Riguidel, M. 2005. Security and trust assurances for smart environments. In Mobile Adhoc and Sensor Systems Conference. IEEE International Conference on , vol., no., pp.8 pp.-234, 7-7 DOI=10.1109/MAHSS.2005.1542804

[29] Stajano, F., and Anderson, R. J. 1999. The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks. In Proceedings of the 7th International Workshop on Security Protocols, Bruce Christianson, Bruno Crispo, James A. Malcolm, and Michael Roe (Eds.). Springer-Verlag, London, UK, 172-194.

[30] Zhang, R., Wang, X., Farley, R., Yang, X., and Jiang, X. 2009. On the feasibility of launching the man-in-the-middle attacks on VoIP from remote attackers. In Proceedings of the 4th International Symposium on Information, Computer, and Communications Security (ASIACCS '09). ACM, New York, NY, USA, 61-69. DOI=10.1145/1533057.1533069

[31] Al-Muhtadi, J., Campbell, R., Kapadia, A., Mickunas, M.D., and Yi, S. 2002. Routing Through the Mist: Privacy Preserving Communication in Ubiquitous Computing Environments. In Proceedings of the 22nd International Conference on Distributed Computing Systems (ICDCS'02) (ICDCS '02). IEEE Computer Society, Washington, DC, USA, 74-.

[32] Spreitzer, M. and Theimer, M. 1993. Providing location information in a ubiquitous computing environment (panel session). In Proceedings of the fourteenth ACM symposium on Operating systems principles (SOSP '93). ACM, New York, NY, USA, 270-283. DOI=10.1145/168619.168641 http://doi.acm.org/10.1145/168619.168641

[33] Liberatore, M. and Levine, B. N. 2006. Inferring the source of encrypted HTTP connections. In Proceedings of the 13th ACM conference on Computer and communications security (CCS '06). ACM, New York, NY, USA, 255-263. DOI=10.1145/1180405.1180437 http://doi.acm.org/10.1145/1180405.1180437

[34] Saponas, T. S., Lester, J., Hartung, C., Agarwal, S., and Kohno, T. 2007. Devices that tell on you: privacy trends in consumer ubiquitous computing. In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07), Niels Provos (Ed.). USENIX Association, Berkeley, CA, USA, , Article 5 , 16 pages.

[35] Enev, M., Gupta, S., Kohno, T., and Patel, S. N. 2011. Televisions, video privacy, and Powerline electromagnetic interference. In Proceedings of the 18th ACM conference on Computer and communications security (CCS '11). ACM, New York, NY, USA, 537-550. DOI=10.1145/2046707.2046770 http://doi.acm.org/10.1145/2046707.2046770

[36] Wright, C.V., Ballard, L., Monrose, F., and Masson, G.M.. 2007. Language identification of encrypted VoIP traffic: Alejandra y Roberto or Alice and Bob?. In Proceedings of 16th USENIX Security Symposium on USENIX Security Symposium (SS'07), Niels Provos (Ed.). USENIX Association, Berkeley, CA, USA, , Article 4 , 12 pages.

[37] Stajano, F. 2000. The Resurrecting Duckling - What Next?. In Revised Papers from the 8th International Workshop on Security Protocols, Bruce Christianson, Bruno Crispo, and Michael Roe (Eds.). Springer-Verlag, London, UK, 204-214.

[38] Stajano, F. 2002. Security for Ubiquitous Computing. John Wiley & Sons, Ltd. DOI= 10.1002/0470848693.fmatter_indsub http://dx.doi.org/10.1002/0470848693.fmatter_indsub

[39] Wagner, D. and Soto, P. 2002. Mimicry attacks on host-based intrusion detection systems. In Proceedings of the 9th ACM Conference on Computer and Communications Security (Washington, DC, USA, November 18 – 22, 2002). V. Atluri, Ed. CCS '02. ACM, New York, NY, 255-264. DOI= http://doi.acm.org/10.1145/586110.586145

[40] Lindberg, J. and Blomberg, M. 1999. Vulnerability in speaker verification - a study of technical impostor techniques. In Proceedings of the European Conference on Speech Communication and Technology, volume 3, pages 1211-1214, Budapest, Hungary.

[41] Faundez-Zanuy, M. 2004. On the vulnerability of biometric security systems. In Aerospace and Electronic Systems Magazine, IEEE , vol.19, no.6, pp. 3- 8. DOI= 10.1109/MAES.2004.1308819

[42] Akhtar, Z., Fumera, G., Marcialis, G.L., Roli, F. 2011. Robustness analysis of likelihood ratio score fusion rule for multimodal biometric systems under spoof attacks. In Security Technology (ICCST), 2011 IEEE International Carnahan Conference on , vol., no., pp.1-8, 18-21. DOI= 10.1109/CCST.2011.6095935

[43] Francillon, A ., Danev, B., and Capkun, S. 2010. Relay attacks on passive keyless entry and start systems in modern cars. In Proceedings of NDSS.

[44] Mark Weiser. 1999. The computer for the 21st century. SIGMOBILE Mob. Comput. Commun. Rev. 3, 3 (July 1999), 3-11. DOI=10.1145/329124.329126 http://doi.acm.org/10.1145/329124.329126

[45] Nielsen Wire. 2012. More US Consumers Choosing Smartphones as Apple Closes the Gap on Android. http://blog.nielsen.com/nielsenwire/consumer/more-us-consumers-choosing-smartphones-as-apple-closes-the-gap-on-android/