Characteristic-Based Security Analysis of Personal Networks

Andrew Paverd[1], Fadi El-Moussa[2], and Ian Brown[3]

[1]Department of Computer Science, University of Oxford
[2]BT Research, BT Technology, Service and Operations
[3]Oxford Internet Institute, University of Oxford

June 2014

Abstract

The rapid increase in smart devices and the development of mobile broadband communication technologies have given rise to the *Personal Network* (PN). The PN is logical user-centric network of interconnected components belonging to and/or used by a particular individual. The components of the PN include devices from the home network, the Personal Area Network (PAN), and the Vehicular Area Network (VAN) as well as cloud-based services. Previous security analyses have focussed on the various physical networks that make up the PN but have not provided an overall view of the PN itself. By consolidating this previous work, we present a comprehensive security analysis for the PN. Based on recent literature, we identify the primary characteristics of the components that make up the PN and of the PN itself. We use these to develop an abstract asset model of the PN. From this asset model, we derive the primary attacker objectives and motivation and compile a list of common attack vectors for the PN. We then present a mapping between the identified attacks and the characteristics of the PN components. This can be used to determine the exact attack vectors to which a specific component is vulnerable. We argue that this characteristic-based approach is better suited for use in the PN because of the high degree of heterogeneity between the PN components. Our overall contribution is a comprehensive security analysis for the PN and a methodological process that can be used for future analyses of similar systems.

1 Introduction

Recently there has been a rapid increase in the use of smart, interconnected devices. In particular, smartphones and tablet PCs have become pervasive in the mobile sector. The home environment is also experiencing an increase in

network-connected smart devices and systems including smart TVs, set-top-boxes, games consoles and smart home appliances. The full functionality of these devices and systems can only be realized when they are interconnected to form networks.

In a personal context (as opposed to an enterprise environment), concepts such as the Home Network and the Personal Area Network (PAN) have been developed to facilitate the interconnection of PCs as well as other smart devices. More recently, other types of networks such as a Vehicular Area Network (VAN) have also been developed. The defining characteristic of these networks is that they are based on geographical locality. This means that the network only includes devices and systems that are in physical proximity. For example, by strict definition, the home network does not include mobile devices when they are not physically located in or near the home. Similarly, the PAN is limited to devices in close proximity to the user.

With the advent of new computing and communication technologies, it has become increasingly problematic to define networks based on geographical locality. For example, cloud-based services provide a significant amount of functionality to home networks. Personal cloud-based data storage means that data from the home network is now stored by the cloud provider at a separate geographic location. Furthermore, there is an emerging trend towards the use of devices in a PAN to control aspects of the home network. For example, modern smart home appliances can now be remotely controlled from a user's smartphone. This demonstrates that the networks formed through the interconnection of smart devices and systems are no longer defined by geographic locality or physical proximity. From a security perspective, it is important to take this into account, especially when undertaking security analyses of such networks. However, most security analyses are still focussed on geographically defined networks such as the home network or the PAN.

1.1 The Personal Network: A User-Centric Approach

A solution to this problem is to define the network using a user-centric approach. Niemegeers and De Groot [1] have used this approach to define the concept of a *Personal Network (PN)*. They envision the PN as a dynamic extension of the PAN to encompass the user's home network as well as other networks such as the user's VAN. They have also suggested that the PN could temporarily include resources that are not owned by the user. Subsequently, Niemegeers and De Groot [2] have pointed out that the PN will only inspire trust and be accepted by its users when a sufficient level of security is guaranteed. Similarly, Leung et al. [3] have presented a description of the PN that they call the Personal Distributed Environment (PDE). They define this concept as an overlay network or a virtual network consisting of the networked devices that the user owns or is authorized to use.

A recent example of the implementation of a PN is the *webinos* research project [4]. This project has developed and demonstrated an architecture for creating and using a network that spans across the home, mobile and vehicle

environments and also includes cloud-based functionality. The *webinos* project also presents a model for communicating between different PNs. In the context of this project, Lyle et al. define the PN as "a set of communicating devices belonging to and/or used by a particular individual" [5].

From the above definitions and examples, it can be seen that the term *personal network* does not refer to a physical network infrastructure but instead refers to a logical set of devices and systems as well as the communication links between them. Therefore, it is important to note that the security of a PN includes aspects of device security (end-point security) as well as network security (communication security).

In this paper, we expand the definition from Lyle et al. [5] to explicitly include cloud-based services. We therefore define the personal network as *"the set of interconnected devices and services belonging to and/or used by a particular individual."* In this context, we refer to the entities that make up the PN as the *components* of the PN. These components include physical devices such as smartphones and smart appliances and services such as cloud-based data storage or content streaming as well as all the communication links between them.

1.2 Security Analysis for the PN

In this paper, we present a security analysis of the PN based on a thorough review of recent scientific literature. Given the previous descriptions of the PN, we have identified a set of characteristics that can be used to describe the various components of the PN. Each PN component will exhibit a specific subset of these characteristics. The characteristics associated with a specific component are based on the component's designed functionality as well as its hardware and software capabilities. This set of identified characteristics is described in Section 3.

Previous security analyses have focussed on the various devices and physical networks that make up the PN but none have presented an overall view of the PN. For example, ITU-T Recommendation X.1111 *"Framework of Security Technologies for the Home Network"* [6] includes a security analysis for the geographically-defined home network. Many of the attack vectors identified for the home network are also applicable to the PN. Similarly, security analyses for PANs and mobile devices describe additional attacks that are also applicable to the PN but are not relevant to the home network. We have consolidated these previous analyses to compile a comprehensive list of attack vectors to the PN as presented in Section 6.

We have observed that certain attacks are only applicable to PN components that exhibit specific characteristics from the list in Section 3. By analysing each of the attack vectors, we have developed a mapping between specific attacks and characteristics of the PN components. This mapping is presented in Section 7. Since each component of the PN will exhibit certain characteristics, this mapping can be used to determine the set of attacks to which that particular component is vulnerable. The methodology used for this characteristic-based security analysis is somewhat different from that used in previous analyses as

explained in Section 8. However, due to the high degree of heterogeneity between the components of the PN, we argue that this approach is better suited for use in the PN context.

We envision that this security analysis will form the basis for further work to mitigate against the identified attacks and enhance the security of the PN. We also suggest that the methodology used in this analysis can be used in future analyses of similar systems. Our conclusions and recommendations for future work are presented in Section 9.

2 Characteristics of PN Components

In previous security analyses, it is often the case that the components of the network are divided into non-overlapping categories. For example, in ITU-T X.1111 [6], the devices in the home network are divided in three device types. Each type of device exhibits a specific set of characteristics (e.g. user interface or control capabilities) and is therefore vulnerable to a particular set of attackss. However, we argue that a category-based approach is not well suited to the high degree of device heterogeneity in the PN context. For example, using the device types defined in ITU-T X.1111 [6], the vast majority of modern smart devices would all fall under the same device type ('Type A/C') and would therefore theoretically all be vulnerable to the same attacks. This is not an accurate representation of the real situation because experience has shown that the different components of the PN are actually vulnerable to very different attacks.

To overcome these limitations of the category-based approach, we define a set of characteristics exhibited by the components of the PN. The advantage of our characteristic-based methodology is that it provides a greater level of detail by allowing flexible combinations of characteristics. If this same level of detail were to be obtained using a non-overlapping categorization, a very large number of categories would be required to capture all the possible combinations of characteristics.

The characteristics listed in this section are drawn from recent scientific literature as well as publications such as ITU-T X.1111 [6] and the NIST *"Guidelines on Cell Phone and PDA Security"* [7]. The following characteristics are applicable to specific components within the PN:

2.1 Persistent Storage:

Does the component provide persistent storage capacity? This characteristic encompasses storage for all types of data available in the PN. This includes information such as personal documents, media content or user preferences as well as data such as system configurations or software. For example, PCs provide significant persistent storage capacity using disk drives.

2.2 Processing Functionality:

Does the component process any information or data? This characteristic is applicable to the majority of devices in the PN since it refers to any form of transformation or processing of data or information. The only examples of PN components to which this characteristic is not applicable are basic sensor devices and networking components such as switches or wireless repeaters.

2.3 Communication Capabilities:

Does the component transmit or receive data? This characteristic is also broadly applicable as it refers to any component that communicates with other components or external entities. In particular, this characteristic is also applicable to components that facilitate network communication, such as routers or the home gateway.

2.4 User Interface Capabilities:

Does the component accept input from or provide output to the user? This characteristic includes all forms of user input or output that take place via a local UI provided by the component. This UI must not require any other component to achieve full functionality. For example, a smartphone provides rich UI functionality (both input and output) whereas a virtual server running in the cloud does not provide any UI functionality since it must be accessed remotely.

2.5 Direct Control of External Physical Infrastructure:

Does the component directly control or influence some external physical infrastructure? This characteristic refers to physical infrastructure that is not related to the computational functionality of the component. Direct control means that there are no intermediate systems between this component and the physical infrastructure (i.e. this component is the final Policy Enforcement Point (PEP) for infrastructure control policies). For example, smart lighting controllers or smart heating, ventilation and air conditioning (HVAC) systems directly control external physical infrastructure.

2.6 Physical Mobility:

Is the component designed to be mobile or portable? A portable component is designed such that it can easily be moved to a new geographical location and resume operation. A mobile component remains fully functional whilst it is changing location. For example, a notebook PC is a portable component and a smartphone is a mobile component.

2.7 Support for Third-Party Software:

Is the component capable of running software provided by a third-party that was not part of the original software environment? This characteristic is generally used to distinguish between smart and non-smart devices. For example, a smartphone can download and run apps from an app store whereas a sensor device is generally limited to its original software.

2.8 Control of Other Components:

Does the component have the capability to control other components in the PN? In this characteristic, control refers to any ability to affect, modify or influence the behaviour or state of another component. For example, a laptop PC can control a server system by executing commands and moving data to or from the server.

2.9 Remote Accessibility:

Can the component be accessed or controlled by a remote entity? This characteristic refers to components that can be accessed or controlled by other components or external entities (in a sense, it is the complement of the preceding characteristic). Remote accessibility or control refers to any access or control that does not take place via the component's local user interface.

2.10 Provision of Services:

Does the component provide services to other components in the PN or to external entities? This characteristic encompasses all types of services. For example, a smartphone or a home gateway device provides Internet connectivity to other components in the PN.

2.11 Consumption of Services:

Does the component consume services provided by other component in the PN or external entities? Similarly to the previous characteristic, this characteristic is applicable to all components that consume any type of service. This service could be provided by another component in the PN (as above) or by an external entity. For example, a smart media system consumes services in the form of media content from a media server or an external content provider.

2.12 Association of Characteristics and Devices

Each component (device or service) within the PN will exhibit a specific subset of the above characteristics. Specific characteristics can be associated with a particular component based on the component's intended functionality and its

hardware and software capabilities. Four examples of the association of characteristics to specific components are shown in Table 1. Each characteristic inherently makes the component vulnerable to a particular set of attacks. Section 7 explains how the identified attacks can be mapped to these characteristics.

Characteristic	Smartphone	Smart refrigerator	Wireless Access Point	Smart Energy Meter
Non-Volatile Storage	Y		Y	Y
Processing Functionality	Y			Y
Communication Capabilities	Y	Y	Y	Y
User Interface Capabilities	Y			Y
Direct Control of External Physical Infrastructure		Y		Y
Physical Mobility	Y			
Support for Third-Party Software	Y			
Control of Other Components	Y			
Remote Accessibility		Y	Y	Y
Provision of Services	Y	Y	Y	Y
Consumption of Services	Y	Y		

Table 1: Examples of associating characteristics to PN components.

3 Characteristics of the PN Environment

This section lists the defining characteristics of the PN environment from a security perspective. Due to the sheer diversity of possible implementations of personal networks, not all of these characteristics will apply to every implementation. However, it is expected that as personal networks continue to develop, they will increasingly tend to resemble the generalized model and so will exhibit the following characteristics:

3.1 Absence of Geographical Locality

As explained in Section 1, the PN is not defined using geographical locality. This characteristic was necessarily introduced by Niemegeers and De Groot [1] since, in their model, the user (and hence his or her PAN) can move to a different geographical location from the home network. This characteristic also forms one of the primary design considerations of the webinos project as explained by Lyle et al. [8]. Although not explicitly stated, this characteristic is implied in

ITU-T X.1111 through the inclusion of the"Remote home user" in their network model [6]. Due to this characteristic, it must always be assumed that devices in the PN may not be in the same area. This does not affect the connectivity between the devices, which would be provided by infrastructure such as mobile broadband networks and the Internet. From a security perspective, this use of third-party networks is important in itself. However, this characteristic does not mean that all elements of the network will be geographically dispersed. For example, the non-mobile devices in the home network or the devices carried by a mobile user will still exhibit a high degree of physical locality. Another implication of this characteristic is that the geographical location of the device now represents a richer source of context. For example, if a smartphone cannot detect (and authenticate) the home Wi-Fi network, the PN can infer that this device (and hence its owner) are not in the home environment and can take the appropriate actions.

3.2 Device Heterogeneity

As explained in ITU-T X.1111 [6], the home network will exhibit a high degree of device heterogeneity. As this is expanded to the broader PN, an even greater diversity of devices must be considered. From a security perspective, the primary characteristics that could vary between devices are:

- Computational architecture and processing speed
- Data storage technology and capacity
- Communications capabilities (e.g. wired vs. wireless)
- Device mobility (e.g. fixed vs. mobile devices)
- Operating system and software environment
- User interface capabilities
- Cyber-Physical control capabilities

This device heterogeneity is important from a security perspective as explained in Section 6. For example, Botha et al. [9] provide a comparison between a desktop PC and a mobile device and conclude that various factors make it difficult to achieve an equivalent level of security on both devices. Similarly Oberheide and Jahanian examine the unique security challenges of mobile devices [10].

3.3 Communication Diversity

Along with device heterogeneity, the PN will also exhibit a high degree of communications heterogeneity. This means that the PN will utilize a combination of communication technologies based on different communication channels and

networking protocols. For example, ITU-T X.1111 [6] explains how the home network model uses a combination of wired and wireless network technologies. Niemegeers and De Groot [1] explain how the PN will also include communication links over public infrastructure networks such as mobile broadband networks and the Internet. IEEE 1905.1 is a draft standard for a "Convergent Digital Home Network for Heterogeneous Technologies". This standard defines a common abstraction layer which supports the use of various underlying networking technologies including IEEE 802.3 (Ethernet), IEEE 802.11 (WLAN) and IEEE 1901 (power-line networking) technologies. Schwiderski-Grosche et al. [11] also identify this as a characteristic of the PN and explain that this could also involve a combination of unicast, multicast and broadcast communication services. In the case of the home network, it was often assumed that wired networks are inherently private whereas wireless networks could propagate beyond the boundaries of the home. However, with recent technological developments and approaches such as wired networking over shared infrastructure, this assumption is not necessarily valid in all cases. For example, in some homes, the wired network may be provided using power-line communication technologies such as the IEEE 1901 (HomePlug) or ITU-T G.9960 and G.9961 (G.hn/HomeGrid) standards. Since power-line networking uses the electricity distribution infrastructure, transmitted data is not restricted to the boundaries of the home. Although they are technically wired network technologies, both existing power-line standards include security technologies very similar to those employed in Wireless Local Area Networks (WLANs).

3.4 Inclusion of Non-Private Elements and Infrastructure

In the previous paradigm of geographically defined networks, the most common case was that all elements of the network would be private. The move towards the user-centric PN introduces the possibility that the network will also include non-private elements or use non-private infrastructure. In a generalized model of the PN, the elements in different environments will use public infrastructure networks to communicate with each other. In the example presented by Niemegeers and De Groot [1] (explained in Section 1), the medical sensors in the users PAN would communicate with a server in the home network using public infrastructure networks. In this case, the communication would be routed over the mobile broadband providers network, over the Internet, to the home service providers network and finally via the home gateway to the home server. A more subtle example of this characteristic, discussed in the webinos security framework [4], is the concept of shared devices. Whilst these devices are not public, they are also non-private (i.e. they are not exclusive to a single individual). For example, an appliance in the home environment such as a smart TV may be shared between all home residents. This device still forms part of each users PN, but may sometimes be in use by another user. The trust relationships between the users play an important role in defining the usage policy for shared devices.

3.5 Multihomed Network Topology

A modern PN could have multiple connections to external networks such as the Internet. For example, in the home environment, Internet connectivity would normally be provided by the home gateway. However, many modern smartphones have the ability to share their mobile broadband connections through Wi-Fi tethering or similar mechanisms. If Wi-Fi tethering is used in the home environment then the home devices will have two different routes through which to connect to the Internet. Networks using this type of topology are often referred to as being multihomed. Although not explicitly stated, this characteristic is implied in the ITU-T X.1111 [6] network model since both the mobile user and the home gateway device have separate connections to the Internet. However, this characteristic does not imply that the networks will always be multihomed due to the dynamic nature of the PN.

3.6 Highly Dynamic Nature

Schwiderski-Grosche et al. [11] explain that the PN will be highly dynamic in nature for various reasons. Firstly, in order to maximise efficiency, services will be provided and consumed in an on-demand manner. This is particularly true of any services hosted in the cloud. It also applied to services provided by PN devices that are constrained in terms of processing power or stored energy (battery) capacity. For example, a location service that uses a smartphones Global Positioning System (GPS) receiver will usually only be activated when it is required because operation of the GPS receiver drains the smartphones battery. The second reason presented by Schwiderski-Grosche et al. [11] is that the inclusion of mobile devices in the PN often results in variations from a communications perspective. In terms of mobile devices, the physical location of the device influences the type of mobile wireless connection it can use and the characteristics of this connection. For example, when a user leaves the home environment, his or her smartphone would have to switch to a public mobile broadband network. Apart from the change from a private to a shared communication link, the mobile broadband connection may have lower bandwidth or higher latency. This move could necessitate changes to services. For example, if the user was streaming a video to the mobile device, this might need to switch to a lower bitrate stream to accommodate the change in communication bandwidth. A third example from Schwiderski-Grosche et al. [11] is that devices reliant on stored energy reserves (e.g. battery-powered devices) may be switched off periodically. From a network perspective, these devices are essentially leaving and later rejoining the PN. Similarly, if a mobile device moves into an area without communication coverage (e.g. a mobile network dead-spot), it would also become temporarily disconnected from the PN.

3.7 Energy Aware Systems and Technologies

Computational systems are increasingly becoming more energy aware than previous technologies. For example, in the vision of the future smart grid-connected smart home, the home devices and appliances can change their behaviour based on the availability of the prevailing cost of electrical energy. In this scenario, a home appliance such as a smart dishwasher might respond to signals from the smart grid and postpone its operation from a peak period to a time when there is a lower demand for energy (and potentially a lower energy price). Mobile devices are also becoming more energy aware due to limitations in energy storage technology. For example, mobile devices such as smartphones are rapidly increasing in terms of computational capacity (e.g. processing power, storage). These advances increase the power requirements of the mobile device. However, current energy storage technology (e.g. battery technology) has not improved at the same rate. Modern smartphones are limited by the energy density of the battery technology and so can only increase the amount of energy they store by increasing the size of the battery. This is usually infeasible and so alternative approaches are beginning to be used. For example, the concept of mobile cloud computing allows a mobile device to offload computational operations to the cloud in order to increase energy efficiency [12]. As illustrated by the above examples, future personal networks will become more aware of when and how energy is expended and will dynamically adapt their operation to minimize usage and maximize energy efficiency.

4 Personal Network Asset Model

This section presents an abstract asset model of the PN. This forms the starting point of the core security analysis in this report.

4.1 Introduction to an Abstract Asset Model

From a security modelling perspective, an asset represents something of value to the user. Assets can be tangible such as physical hardware or intangible such as information or services. As usual, the value of each asset can be characterized according to three well-known security properties:

Confidentiality: The confidentiality value of an asset indicates how important it is to prevent unauthorized disclosure of the asset. For example, a user's banking details are an informational asset with a very high confidentiality value.

Integrity: The integrity value of an asset indicates how important it is that the asset is protected from unauthorized modification. For example, a software package would have a high integrity value to ensure that it only performs its intended operations.

Availability: The availability value of an asset represents how important it is for the asset to be available for use by an authorized user when it is required. For example, physical assets such as PCs have high availability value because users expect that they will be operational when required.

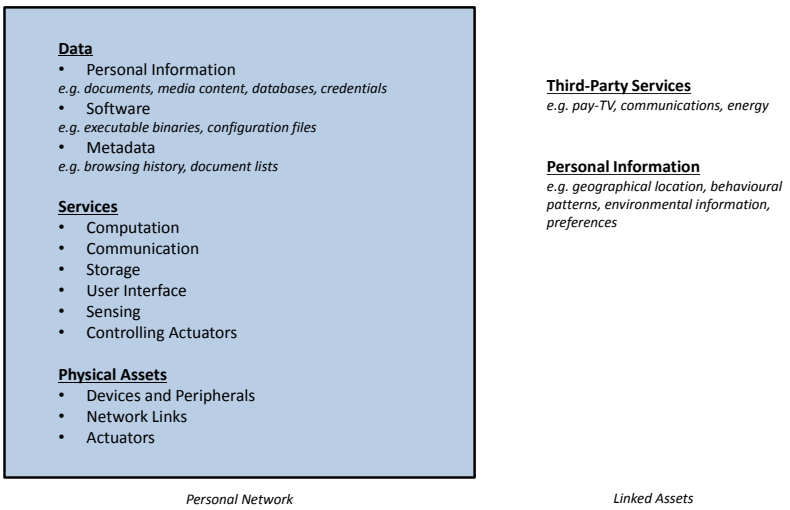

Figure 1: Abstract asset model of the personal network.

The asset model is said to be abstract because it groups the actual assets into broader categories based on their type. This is possible because assets of the same type will generally have a similar set of values according to the characteristics explained above.

4.2 Personal network Asset Model

Figure 1 shows the abstract asset model of the PN used in this security analysis. This model includes all the assets that could be part of a particular PN as defined in Section 1. The asset model is divided into two sections to distinguish between assets internal to the PN and those which are external but are directly linked to this network. As shown in the figure, this model identifies the following five primary types of assets in the PN:

4.3 Internal Information and Data

This asset type represents all forms of information and data stored, processed or transmitted by elements of the PN. There are three main subcategories of this type of asset: Firstly, this type of asset includes the user's personal information such as documents, media files, databases and credentials. This information usually has a high value in terms of all three aspects of confidentiality, integrity

and availability. Secondly, any software that runs on the system also falls under this type of asset since it is composed of executable files, scripts, libraries and configuration files. Software has a high value in terms of availability and integrity to ensure that it can be used when required and that it operates correctly. In general, the software binary files do not have a high confidentiality value but certain configuration files may be confidential. Compromise of software integrity can lead to compromise of the confidentiality of data to which it has access. Finally, this type of asset also includes any metadata associated with these previous two subtypes. For example, metadata in the PN context could include web browsing history or lists of recently opened documents. This metadata has a high confidentiality value but a low availability value since it can often be recreated by the system.

4.4 Internal Services

This asset type represents all types of internal services provided by the PN. These services could be provided by any element or combination of elements within the PN. These services could be provided to the primary user or to other elements of the PN or to external users and systems. In all cases, the availability of the service is a primary concern. Since the PN is dynamic in nature (as explained in Section 3), these services can be provided in an on-demand manner but must still be available when required. These services are also valued because of their integrity. This means that they will perform the intended operation or return the correct result whenever they are used. Although it cannot be represented in the abstract asset model, the use of some services requires expenditure of resources. For example, computation can be considered as an internal service that consumes energy (which is even more valuable on mobile devices).

4.5 Physical Assets

The physical assets category represents all physical hardware elements of the PN. This includes hardware such as PCs and smartphones but does not include the data stored on these devices or the services they provide (since these are covered by the previous two categories). This type of asset is valued for its availability and its integrity. For example, the user expects all hardware elements to be fully operational when required and to function according to their intended design. Since these are not information-based assets, confidentiality is not applicable.

4.6 External Services

External services are used by the PN but provided by external third parties. For example, a service provider could provide content services such as Internet Protocol Television (IPTV) to the PN. These external services are distinct from the internal services described above but could be used to support the internal services. For example, the mobile broadband connectivity provided to a user's

smartphone by the mobile network operator is an external service. The smartphone could then use this to provide an internal service to other elements of the PN through mechanisms such as Wi-Fi tethering. Similarly to the internal services, external services are valued for their availability and integrity. However, since this category is external to the PN, it is usually the responsibility of the service provider to ensure the availability and integrity of these services, often defined in a Service Level Agreement (SLA). They are therefore beyond the scope of this report.

4.7 External Information

This category of asset represents information that is not part of the PN but is directly related to this network. This refers to abstract information that can be obtained by elements of the PN and stored as internal information. For example, if the PN contains a GPS receiver, the user's location can be considered to be external information. Although it may not necessarily take place, the PN could obtain the user's location and store it as internal information. Another example of external information is the immediate surroundings of a smartphone since this could be obtained using the smartphone's cameras or microphone. Due to the nature of the PN, this information is likely to be highly specific to the primary user. This means that external information has a very high value in terms of confidentiality. Without confidentiality, this information could be used to track the user or observe his or her immediate surroundings resulting in a serious breach of privacy. Since this information is external to the PN, it is not evaluated in terms of its integrity or availability. However, it is still important to ensure that the PN cannot be used to breach the confidentiality of this information.

5 Attacker Objectives

This section lists the primary objectives that could motivate an attack on the personal network. These objectives are based on the abstract asset model presented in the previous section. Since every implementation of a PN will be different, it is not necessarily the case that all of these attacker objectives will be applicable to every implementation. However, if the PN implementation conforms to the abstract asset model, then the motivation for any attack can be categorized according to the attacker objectives presented in this section. These attacker objectives are largely based on a modified version of the "Result-centric taxonomy" presented by Dagon et al. [13].

5.1 Theft or Abuse of Information

As explained in the abstract asset model, the information assets, both internal and external to the PN, have a high value in terms of their confidentiality. This generally implies that this information would also have some value to an

attacker (although it would likely be a different value from that of the user). One possible objective of an attacker would therefore be to obtain this information. Assuming the attacker is not authorized to access this information, this constitutes theft of information. For example, an attacker might try to obtain a user's personal documents from a device in the PN. It must be noted that due to the nature of these assets, theft of information does not necessarily imply that the information is no longer available to the legitimate user. Arguably the most common occurrence is for an attacker to make a copy without modifying the original information in order to avoid detection. Modification and deletion of this information is discussed as a separate objective. If the information itself it not valuable, an associated attacker objective would be to misuse or abuse the information. For example, an attacker might misuse a device's private key to allow a rogue device to connect to the PN.

5.2 Modification or Deletion of Information

The information assets in the PN also have a high value in terms of their integrity and availability. If the attacker either cannot or does not want to obtain the information, a related objective could be the modification or deletion of this information. For example, since software is categorized as an information asset, an attacker could attempt to modify the software running on a PC for a variety of reasons, thus compromising its integrity. Similarly, deletion of information such as access logs could be one of the attacker objectives as part of a larger attack.

5.3 Theft or Abuse of Services

As shown in the abstract asset model, the PN both provides and consumes internal services as well as consuming external services. By definition, these services provide some value to the user or the other elements of the network. An objective of the attacker could be to obtain the benefit provided by these services. Again, assuming the attacker is not authorized to use these services, this would constitute theft of service. As explained in the asset model, certain services require expenditure of some resource. Therefore, theft of services could essentially amount to theft of resources. An example of theft of an external service would be smartphone malware that uses the device's mobile broadband connection, for which the user may be billed. Since computation can be considered to be an internal service, an example of theft of this service would be an attacker using a target device to perform computational operations such as mining cryptocurrency. In this case, theft of computation increases the device's energy usage which is becoming an increasingly important consideration in modern computational systems. In cases where the PN provides services, these could also be misused or abused by an attacker. For example, if the home network provides Wi-Fi connectivity to external entities (possibly under an agreement with the service provider), excessive usage of this service could be viewed as an abuse of the service.

5.4 Modification or Denial of Services

As explained in the abstract asset model, services are also valued in terms of their integrity and availability. Modification of a service is an attack on its integrity whilst denial of service is an attack on the service's availability. For example, elements in the PN such as smartphones could use cloud-based services such as virus scanning [14]. A possible objective of the attacker could be to modify this service to present inaccurate information to the user in order to conceal malicious software on the device. At present, denial of service is arguably one of the most common types of attack. In the PN context, denial of service could affect either internal or external services. For example, communication jamming caused by a rogue wireless device is an attack on the availability of the internal communication service provided by the Wireless LAN Access Point (WLAN AP).

5.5 Unauthorized Cyber-Physical Control

A relatively recent possible objective of the attacker is unauthorized control of cyber-physical systems. In the context of the PN, the term cyber-physical refers to any computational system that forms part of the network but also has the capability to control external physical infrastructure. Cyber-physical systems would all be labelled with the "Direct control of external physical infrastructure" characteristic explained in Section 2 and would most likely also have the "Remote accessibility" characteristic. For example, cyber-physical systems include various types of (future) smart home appliances such as smart refrigerators, lighting controllers or heating, ventilation and air-conditioning (HVAC) systems which can control aspects of the physical environment. These systems themselves would fall under the physical assets category in the abstract asset model. Cyber-physical systems are designed to enable to user to control his or her physical environment and usually provide this functionality through the PN. Therefore, unauthorized control of cyber-physical infrastructure would be a possible objective for an attack on the PN. At this time, the most well-know attacks with this objective have been targeted at industrial systems. However, as the number of smart cyber-physical systems increases, this attack objective is likely to become a relevant concern in the future PN.

6 Attack Vectors in the Personal Network

This section presents a consolidated list the primary attack vectors applicable to the PN. These are drawn mainly from existing security analyses. Although the previous analyses have not focussed specifically on the PN context, the attacks they identified are applicable to devices and services that form part of the PN. This section also draws on publications such as ITU-T X.1111 [6] and the NIST *"Guidelines on Cell Phone and PDA Security"* [7]. Some of these attacks represent direct mechanisms for achieving the attacker's objectives, whilst others describe a class of related mechanisms. As technology continues

to develop, it is expected that some of these mechanisms will change whilst the threats themselves remain constant. Where applicable, the description of each attack highlights the specific characteristics that would make a component vulnerable to it. The following primary attack vectors are applicable to the PN:

6.1 Malicious Software

At present, malicious software (malware) is arguably one of the most common threats to computational devices. In the PN context, this attack is explained by Baugher and Lortz [15], Lyle et al. [5], Landman [16] and Miller [17]. Malware is also listed as one of the attacks in the NIST *"Guidelines on Cell Phone and PDA Security"* [7]. Malware could be defined as any software running on a device which the user would not want to be running. By definition, this means that the device is capable of running software that was not included in its original design. For example, attacks of this type could include all forms of computer viruses and spyware. Malware is primarily a mechanism for attacking end devices but this could also lead to attacks on the networking infrastructure. For example, theft of network keys from a specific device could allow a rogue device to circumvent network access controls. Malware is highly diverse and could be used by an attacker to achieve various objectives.

6.2 Malicious Hardware

Malicious hardware is a much less common attack than the software equivalent but still represents a possible attack against the PN. Malicious hardware refers to any hardware component that has been introduced into the PN (or one of its constituent components) for malicious purposes. Examples of malicious hardware include rogue wireless access points that allow an attacker to gain network access. It is conceivable that peripherals such as add-on cards for PCs could exhibit malicious behaviour, for example, by misusing Direct Memory Access (DMA) technology. Malicious hardware could conceivably be used to achieve the attacker's objectives by breaching either device or network security. However, it is suspected that the most likely objectives will be theft of information, theft of services and unauthorized cyber-physical control.

6.3 Exploitation of Flawed/Incorrectly Implemented Software

Another direct mechanism that can be used to achieve the attacker's objectives is the exploitation of flaws in legitimate software. These vulnerabilities could be due to either flawed software design or bugs in the software implementation. In the context of smartphones, this attack is explained by Miller [17]. Common examples of this type of attack are exploits of web browsers or operating systems. Since these pieces of software have a very large installed base, they are attractive targets for exploits. Software exploits would not usually give an attacker the same degree of control as an attack using dedicated malware but could still be

used to achieve various attacker objectives. However, this type of attack could also affect the software used on cyber-physical systems, especially those using a common OS and software applications. Due to the increasing capabilities of cyber-physical systems, the potential consequences of a software exploit are becoming more severe. These consequences could include physical damage or potentially fatal injury of the users.

6.4 Exploitation of Flawed/Incorrectly Implemented Hardware

Similarly to the previous attack, it may be possible to exploit vulnerabilities in certain physical hardware systems. For example, if executing a particular sequence of instructions or processing a specific data value caused some kind of hardware error, this flaw could be deliberately exploited by an attacker. This would most likely be used as an attack on the availability of physical assets, which could also result in loss of information or denial of services. This type of attack is identified and explained by Shabtai et al. [18].

6.5 Eavesdropping/Interception of Communication

A common attack on networked systems is eavesdropping or interception of communication. This attack is identified and explained in ITU-T X.1111 [6] and by Baugher and Lortz [15]. Further explanation in the context of mobile devices is provided by Friedman and Hoffman [19] as well as Landman [16]. This type of attack is usually passive and the attacker attempts to remain undetected for as long as possible. This is primarily used for theft of information or theft of services. For example, by eavesdropping on an unprotected home Wi-Fi network, an attacker could obtain information such as a users personal documents or could gain access to services such as media content being streamed within the PN.

6.6 Interruption of Communication

Another threat to networked systems is the potential for interruption of communication. This is also identified as an attack by ITU-T X.1111 [6] and Shabtai et al. [18]. This type of threat is an attack on the availability of information and services and in particular could be used to achieve the denial of service attack within the PN. For example, if a home network uses Wi-Fi communication, a device that generates electromagnetic interference could be used to interrupt the communication channels. Similarly if the network uses power-line communication, an attacker could introduce interference to block or degrade the quality of the communication links. This type of attack is not only limited to the physical communication channel as in the two previous examples. An attacker could also modify the device or network configuration to achieve a denial of service objective.

6.7 Modification of Communication

Modification of communication represents a class of threats to networked systems. The most common sequence of events would be for an attacker to intercept communication messages from a legitimate device and modify them in some way before forwarding them to the intended recipient. The attacker's objective is for the recipient to believe that the modified message has not been altered since it was sent. This attack would most likely be used to achieve attacker objectives related to modifying information or services. It could also be used to provide the attacker with some degree of unauthorized control of cyber-physical infrastructure. This is identified as an attack in ITU-T X.1111 [6]. It is important to note that this attack does not necessarily imply that the attacker is able to fully understand the information that is being modified (this would fall under the eavesdropping threat described above). In networked communication, a common form of this threat is the Man-in-the-Middle (MitM) attack.

6.8 Impersonation of Communicating Entity

In an environment such as the PN that consists of multiple communicating entities, another possible attack is the impersonation of one of these entities. For example, an attacker could attempt to introduce a rogue device into the PN and have it masquerade as a legitimate device. This device could be either a sender or receiver of information and/or services. If the attacker succeeds in impersonating a communicating entity, he or she gains all the capabilities and permissions that would normally be held by the impersonated device. Depending on the configuration of the PN and the entity impersonated, this type of attack could be used to achieve various attacker objectives. This threat could also be viewed as a mechanism for the previous attacks of interception, interruption or modification of communications.

6.9 Unauthorized Remote Access

For components that permit remote access, a possible attack is the unauthorized use of this functionality. ITU-T X.1111 [6] and the NIST guidelines [7] both include this in the broader category of unauthorized access threats. Lyle et al. [5] separate this from unauthorized physical access, which is discussed as a separate attack. An attacker could generally gain access to a system by either obtaining the authentication credentials of a legitimate user (e.g. through phishing or social engineering attacks) or by circumventing the authentication or access control mechanisms of the system (e.g. through software exploits). Once an attacker has access to a device or system, he or she can use the functionality that system would provide to a legitimate remote user. Depending on the configuration of the network and the device, this functionality could range from very limited permissions through to full control of multiple devices and systems. For example, if an attacker can establish a remote connection to a super-user account on a home server, he or she would essentially have full con-

trol of this system and any other systems under its control. This type of attack can be used to achieve any of the attacker objects listed in the previous section. If the attacker's objective is theft of information or services, it is likely that he or she will try to remain undetected by not making noticeable changes to the system. Other attacker objectives could also be feasibly achieved through this type of attack but would inherently be detectable by the user.

6.10 Unauthorized Physical Access

As distinct from unauthorized remote access, Lyle et al. [5] have identified that unauthorized physical access to components of the PN could constitute an attack. Aspects of this attack have been identified in ITU-T X.1111 [6] as the threats of lost or stolen mobile devices. This type of attack can be facilitated by various mechanisms including theft of a physical device (e.g. most likely a mobile device) or misuse of a shared device (e.g. a smart TV in a shared house). Similarly to unauthorized remote access, the amount of control gained by the attacker through this type of attack will depend on the configuration of the device. For example, a mobile device such as a smartphone may have a screen lock or PIN to prevent unauthorized use if the device is stolen but an appliance in the home environment, such as a smart TV, may not always request user authentication.

6.11 Misuse of Device Interoperability

Misuse of device interoperability is a relatively new attack, which has been explained by Lyle et al. [5] as part of the *webinos* project. They argue that since security is a weakest-link problem, the weakest device from a security perspective in the PN could be used as a gateway to the rest of the network. This is a direct consequence of the increased connectivity between devices and the improved level of device interoperability provided by the PN. Another possible impact of this attack described by Lyle et al. [5] is that the increased replication of data between devices in the PN could increase the impact of any security compromise (e.g. by replicating malware to all devices or propagating a tainted configuration file throughout the network). Depending on the configuration of the PN, this type of attack could be used to achieve any of the attacker objectives listed in Section 5.

6.12 Exploitation of Flawed/Incorrectly Implemented Protocols

As explained by Baugher and Lortz [15], a possible attack vector is the exploitation of flawed or incorrectly implemented protocols. This attack could include various types of protocols such as communication protocols or authentication/access control protocols. Similarly to the exploitation of software or hardware vulnerabilities, this attack relies on the fact that a protocol may be flawed in terms of its design or its implementation. Depending on the type

of protocol targeted, this type of attack could be used to achieve various attacker objectives. For example, exploiting vulnerabilities in a communications protocol could facilitate the other types of communication-oriented threats including interception, interruption or modification or communications messages or impersonation of a communicating entity. A further example is the recently revealed flaw in the Wi-Fi Protected Setup (WPS) protocol [20], which could allow an attacker to mount a brute-force attack and succeed in introducing a rogue device in a matter of hours. At the time of writing, many modern home network gateways include the WPS protocol.

6.13 Eavesdropping on User Interface

For devices that provide local UI capabilities, a potential attack is that an attacker could eavesdrop on the information transferred over this interface. An example of this type of attack is shoulder-surfing which is identified as a threat in ITU-T X.1111 [6]. The attacker's objective for this type of attack would be theft of information. In most cases, the attacker attempts to obtain information that could be used for further gain. For example, when a username and password is entered using a tablet PC in a public area, it is possible that an attacker could see these details and identify the service to which they belong (e.g. a webmail password). The attacker could then use the credentials to gain access to this service or network. A related example is a user entering login credentials in a shared device such as a smart TV. If the input is not completely hidden, any other viewers of the TV could obtain this information. If the common approach of masking the characters with asterisks is used, viewers could still obtain related meta-information such as the number of characters in the user's password. From a software perspective, key-logging malware could also be categorized under this type of attack vector.

6.14 Modification of Communication Routing

ITU-T X.1111 [6] identifies abnormal packet forwarding as one of the threats in the home network environment. This refers to the more general threat of modification of communication routing in which an attacker influences or modifies the flow of information within the PN. For example, as explained by Baugher and Lortz [15], modification of the configuration settings on a home network gateway could result in messages being routed to an attacker instead of their intended destination. This type of attack could be used to facilitate the other communication-oriented attacks of interception, interruption or modification of communications.

7 Preliminary Mapping of Attack Vectors to Characteristics

We have observed that certain attack vectors are only applicable to PN components that exhibit specific characteristics from the list in Section 3. By analysing each of the attack vectors, we have developed a mapping between specific attacks and characteristics of the PN components as shown in Table 2. In this table, a **Y** indicates that a component exhibiting a particular characteristic is vulnerable to that specific type of attack. Since this is the first of its kind, Table 2 is proposed as a initial formulation of this mapping and will likely be refined through collaboration with the community at large.

8 Related Work

As previously discussed, ITU-T Recommendation X.1111 [6] includes a threat analysis for home networks. Our analysis extends the scope of the ITU-T analysis to focus on the PN rather than just the home network. Furthermore, in the ITU-T analysis, all devices in the home network are placed into one of three non-overlapping device types. The identified threats are associated with a particular device type or with the communication links between device types. Although our analysis does not focus on the communication links between devices, our

	Persistent Storage	Processing Functionality	Communication Capabilities	User Interface Capabilities	Control Physical Infrastructure	Physical Mobility	Support Third-Party Software	Control of Other Components	Remote Accessibility	Provision of Services	Consumption of Services
Malicious Software	Y	Y					Y				
Malicious Hardware	Y	Y	Y	Y	Y			Y			
Software Exploits		Y					Y				
Hardware Exploits	Y	Y	Y	Y	Y		Y				
Interception of Communication			Y						Y	Y	Y
Interruption of Communication			Y						Y	Y	Y
Modification of Communication			Y						Y	Y	Y
Impersonation of Communication			Y					Y	Y	Y	Y
Unauthorized Remote Access									Y		
Unauthorized Physical Access				Y		Y					
Misuse of Device Interoperability					Y			Y			
Protocol Exploits		Y	Y					Y			
Eavesdropping on User Interface				Y							
Modification of Communication Routing			Y								

Table 2: Mapping attacks to characteristics.

characteristic-based approach provides a significantly more accurate mapping between the threats and specific components of the PN.

Various related work on the security of the PN has been carried out as part of the MAGNET (*"My Personal Adaptive Global Net"*) project. Prasad [21] has presented a threat model framework and methodology for PNs. In this framework, the advantages and disadvantages of various existing threat models are compared. Prasad has also proposed a new methodology for creating threat models specifically designed for use in PNs. Whilst this methodology explains the process of identifying threats, it does not describe how threats should be associated with particular components in the PN. Prasad does not continue to present an actual threat model. Our work is essentially the next step in the process because we have consolidated the threats that have already been identified through these type of methodologies and have proposed a method for associating the threats with specific components.

Stango et al. [22] have proposed a similar threat analysis methodology. In their approach, they identify the possible threats to the system and then explicitly specify an *'Asset Mapping'* step in which the threats are mapped to particular assets such as components within the network. However, they do not specify the methodology that should be used in this particular step. We have demonstrated that the characteristic-based threat mapping methodology could be used in this step of the process.

Various security architectures and systems have been proposed for use in the PN. As part of the MAGNET project, Mihovska and Prasad [23] have presented an adaptive security architecture for PNs. Jehengir and De Groot have presented a different PN security architecture [24] as well as an architecture for securing PN clusters [25]. However, these security architectures are only designed to mitigate against limited subsets of threats to the PN since they are not based on comprehensive threat analyses. We therefore propose that there is scope for further work using our security analysis to enhance the security of the PN as described in the next section.

9 Conclusions and Recommendations for Future Work

Recent advances in smart devices and mobile broadband communication technologies have facilitated the advent of the *personal network* (PN). Although the PN is a logical network rather than a physical network, it is useful to investigate the security threats that are directly applicable to the PN. Previous security analyses have focussed on specific devices or geographically-defined networks that form part of the PN but none have provided a comprehensive overview of the PN itself. We have consolidated various aspects of these previous analyses to provide a comprehensive security analysis of the PN. We use a characteristic-based methodology in which the identified attack vectors are mapped to specific characteristics of PN components. By listing the characteristics of a specific

component, this mapping makes it possible to identify the relevant types of attack for that component. Compared to the category-based approach used in other security analyses, our approach can provide a higher degree of accuracy in mapping attack vectors to components because of the high degree of heterogeneity between the components of the PN. This characteristic-based security analysis is therefore well suited for use in the PN context. We suggest that this analysis can form the basis for future work towards mitigating the identified threats and enhancing the security of the PN. However, this analysis does not yet include the social aspects of the PN and the potential threats that could arise from these aspects such as social engineering. Therefore, there is scope to extend this analysis in the future.

References

[1] I G Niemegeers and S M de Groot. From Personal Area Networks to Personal Networks: A User Oriented Approach. *Wireless Personal Communications*, 22(2):175–186, 2002.

[2] I G Niemegeers and S M de Groot. Research Issues in Ad-Hoc Distributed Personal Networking. *Wireless Personal Communications*, 26(2-3):149–167, 2003.

[3] Adrian Leung, Po-wah Yau, and Chris J Mitchell. Using Trusted Computing to Secure Mobile Ubiquitous Environments. *Security and Privacy in Wireless and Mobile Networking*, pages 303–335, 2009.

[4] Webinos. Phase 1 - Architecture and Components. Technical report, 2011.

[5] John Lyle, Andrew Paverd, Justin King-Lacroix, Andrea Atzeni, Habib Virji, Ivan Flechais, and Shamal Faily. Personal PKI for the smart device era. In *9th European PKI Workshop: Research and Applications*, 2012.

[6] International Telecommunication Union. ITU-T Recommendation X.1111 - Framework of security technologies for home network. Technical report, International Telecommunication Union, 2007.

[7] National Institute of Standards and Technology (NIST). Guidelines on Cell Phone and PDA Security. Technical report, 2008.

[8] John Lyle, Shamal Faily, Ivan Flechais, Andre Paul, Ayse Goker, Hans Myrhaug, Heiko Desruelle, and Andrew Martin. On the design and development of webinos: a distributed mobile application middleware. In *Proceedings of the 12th IFIP WG 6.1 international conference on Distributed applications and interoperable systems*, DAIS' 12, pages 140–147, 2012.

[9] R A Botha, S M Furnell, and N L Clarke. From desktop to mobile: Examining the security experience. *Computers & Security*, 28(3-4):130–137, 2009.

[10] Jon Oberheide and Farnam Jahanian. When mobile is harder than fixed (and vice versa). In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications - HotMobile '10*, page 43, New York, New York, USA, February 2010. ACM Press.

[11] S. Schwiderski-Grosche, A. Tomlinson, and J.M. Irvine. Security challenges in the personal distributed environment. In *IEEE 60th Vehicular Technology Conference, 2004. VTC2004*, volume 5, pages 3267–3270. IEEE, 2004.

[12] Andrew J. Paverd, Michael R. Inggs, and Simon L. Winberg. Towards a Framework for Enhanced Mobile Computing Using Cloud Resources. In *Proceedings of the Southern Africa Telecommunications, Networks and Applications Conference - SATNAC '11*, East London, 2011.

[13] D. Dagon, T. Martin, and T. Starner. Mobile Phones as Computing Devices: The Viruses are Coming! *IEEE Pervasive Computing*, 3(4):11–15, October 2004.

[14] Andrew James Paverd. *Enhanced Mobile Computing Using Cloud Resources*. PhD thesis, University of Cape Town, 2011.

[15] Mark Baugher and Victor Lortz. Home-network threats and access controls. In *Proceedings of the 4th international conference on Trust and trustworthy computing - TRUST '11*, pages 217–230, June 2011.

[16] Max Landman. Managing smart phone security risks. In *2010 Information Security Curriculum Development Conference on - InfoSecCD '10*, page 145, New York, New York, USA, October 2010. ACM Press.

[17] Charlie Miller. Mobile Attacks and Defense. *IEEE Security & Privacy Magazine*, 9(4):68–70, July 2011.

[18] A. Shabtai, Y. Fledel, U. Kanonov, Y. Elovici, S. Dolev, and C. Glezer. Google Android: A Comprehensive Security Assessment. *IEEE Security & Privacy Magazine*, 8(2):35–44, March 2010.

[19] J Friedman and D V Hoffman. Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information-Knowledge-Systems Management*, 7(1, 2):159–180, 2008.

[20] Stefan Viehböck. Brute forcing Wi-Fi Protected Setup, 2011.

[21] N R Prasad. Threat Model Framework and Methodology for Personal Networks (PNs). In *Communication Systems Software and Middleware, 2007. COMSWARE 2007. 2nd International Conference on*, pages 1–6, 2007.

[22] A Stango, N R Prasad, and D M Kyriazanos. A Threat Analysis Methodology for Security Evaluation and Enhancement Planning. In *Emerging Security Information, Systems and Technologies, 2009. SECURWARE '09. Third International Conference on*, pages 262–267, June 2009.

[23] A Mihovska and N R Prasad. Adaptive Security Architecture based on EC-MQV Algorithm in Personal Network (PN). In *Mobile and Ubiquitous Systems: Networking Services, 2007. MobiQuitous 2007. Fourth Annual International Conference on*, pages 1–5, 2007.

[24] Assed Jehangir and Sonia M Heemstra de Groot. A Security Architecture for Personal Networks. In *Mobile and Ubiquitous Systems: Networking Services, 2006 Third Annual International Conference on*, pages 1–8, July 2006.

[25] Assed Jehangir and Sonia M de Groot. Securing Personal Network clusters. In *Security and Privacy in Communications Networks and the Workshops, 2007. SecureComm 2007. Third International Conference on*, pages 320–329, 2007.