Characteristic-Based Security Analysis of Personal Networks

Andrew J. Paverd
Department of Computer Science
University of Oxford
andrew.paverd@cs.ox.ac.uk

Fadi El-Moussa
BT Research
BT Technology, Service & Operations
fadiali.el-moussa@bt.com

Ian Brown
Oxford Internet Institute
University of Oxford
ian.brown@oii.ox.ac.uk

This research was conducted as part of the *Future Home Networks and Services* project at the University of Oxford, funded by BT.

UbiComp '14, September 13 - 17 2014, Seattle, WA, USA

http://dx.doi.org/10.1145/2638728.2641549

Abstract
The *Personal Network* (PN) is a logical network of interconnected components used by an individual. It encompasses the home network, the Personal Area Network (PAN), and the Vehicular Area Network (VAN) and includes cloud-based services. Previous security analyses, including ITU-T Recommendation X.1111, have focussed on the individual physical networks rather than the PN itself. By consolidating and structuring previous work, we propose an updated and enhanced security analysis for the PN. In our characteristic-based approach we identify the primary characteristics of the PN and its components and use these to develop an abstract PN asset model. From this, we derive the main attacker objectives and a list of attack vectors through which these could be achieved. We propose a mapping between the attack vectors and the PN component characteristics that can be used to determine the specific attacks to which a particular component is vulnerable. In this paper, we present a summary of this analysis and discuss its usage.

Author Keywords
Attack vectors; characteristics; home; threat model

ACM Classification Keywords
K.6.5 [Management of computing and information systems]: Security and Protection.

Introduction

The home environment is experiencing a rapid increase in smart, interconnected devices and systems ranging from smart appliances to building management systems. At the same time, smartphones and tablets are becoming ubiquitous user devices and an increasing number of systems are powered by cloud-based services. In a personal context (as opposed to an enterprise environment), concepts such as the home network, Personal Area Network (PAN) and Vehicular Area Network (VAN), have traditionally been used to represent the interconnection of devices and systems in a particular environment. The defining characteristic of these networks is that they are based on geographical locality and only include devices and systems in close physical proximity. However, it is becoming increasingly common for modern systems to transcend these physical network boundaries. Many in-home systems rely on cloud-based services and communicate with mobile devices outside the perimeter of the home network. For example, a Home Energy Management System (HEMS) could use a cloud service [5] and could be remotely controlled from the user's smartphone. This new paradigm is important from a security perspective, however most security analyses still focus on geographically-defined networks. For example, ITU-T Recommendation X.1111 *"Framework of security technologies for home network"* [3] presents a threat analysis for the geographically-defined home network. This overlooks the threats arising from mobile devices or cloud-based systems which are highly integrated with the home network even though they are outside the home.

An alternative approach is to consider the *Personal Network (PN)* which Lyle et al. define as *"a set of communicating devices belonging to and/or used by a particular individual"* [7]. Niemegeers and De Groot envision the PN as a dynamic extension of the PAN to encompass the user's home network as well as other networks such as VANs [10][11]. They have also pointed out that the PN will only inspire trust and be accepted by its users when a sufficient level of security is guaranteed [11]. Similarly, Leung et al. have described the Personal Distributed Environment (PDE) as an overlay network consisting of the networked devices that the user owns or is authorized to use [6]. A recent example of the implementation of a PN is the *webinos* research project which spans the home, mobile and vehicular environments and also includes cloud-based functionality [17]. These definitions and examples illustrate that the PN is not a geographically-defined physical network but rather a logical set of interconnected devices and systems.

To fill the gap left by other security analyses we have consolidated existing analyses and recent scientific literature in order to develop a security analysis for the PN. The full analysis is available as a technical report [13]. In this paper we present a summary of this report and discuss how this analysis can be used as a first step in mitigating security threats in the PN.

Overview of the Security Analysis

In this analysis we use the definition from Lyle et al. [7] and expand it to include cloud-based services. We refer to the devices and systems as *PN components*. Figure 1 presents the taxonomy used and shows the overall structure of this analysis. Based on previous descriptions of the PN, we have identified a set of fundamental characteristics of PN components. Each PN component will exhibit a subset of these characteristics based on its hardware and software capabilities. We have also defined a list of characteristics of the PN itself that distinguish it from other types of networks that have been investigated.

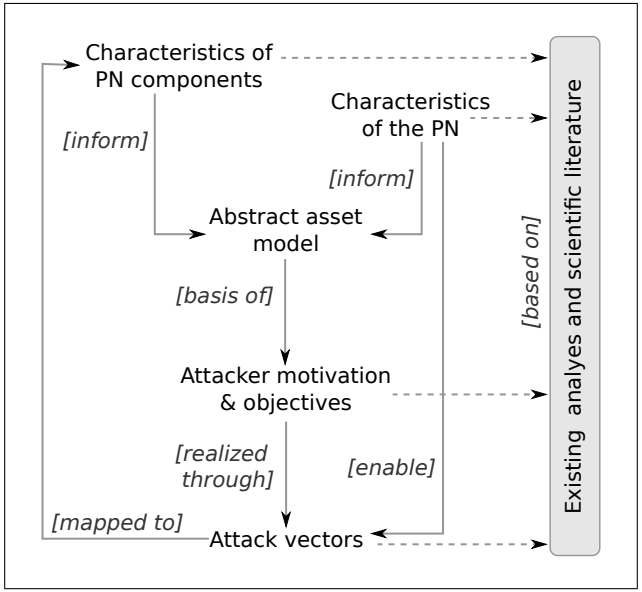

Figure 1: Overview of the security analysis.

Based on these two sets of characteristics, we have developed an abstract asset model of a generic PN and have proposed a set of possible threats in the form of attacker objectives. The details of the asset model and the attacker objectives are presented in the technical report [13]. By consolidating previous security analyses, we have compiled a list of possible attack vectors for the PN. These attack vectors are based on the characteristics of the PN and its components. We have observed that certain attack vectors are only applicable to PN components that exhibit specific characteristics and we have used this to create a mapping between attacks and component characteristics. This mapping can be used to determine the set of attacks to which a particular type of device or system is vulnerable. This methodology differs from previous security analyses that attempt to divide all components into non-overlapping categories. We argue that our characteristic-based approach is better suited to the PN context due to the high degree of heterogeneity between the PN components as described in the next section. Our contributions are therefore: a structured consolidation and systematization of the attacks against the PN; an improved methodology for mapping these attacks to specific devices based on characteristics rather than categories; and a proposal for this mapping.

Characteristics of PN Components

Most threat analyses for the PN have used a category-based approach in which the components are divided into non-overlapping categories. In ITU-T Recommendation X.1111 [3], the devices in the home network are divided into three device types, each of which is vulnerable to a particular set of threats. The categorization does not facilitate any distinctions between devices in the same category. However, various research efforts have shown that improvements in PN functionality result in new potential threats. Some of these threats are not applicable to all devices in a single category whilst others are applicable to multiple categories. For example, mobile devices such as smartphones (X.1111 Type A) are significantly more vulnerable to unauthorized physical access due to theft compared to desktop PCs (also Type A) secured in the home. On the other hand, smartphones (Type A) and smart TVs (Type C) are both vulnerable to software exploits. Therefore we argue that our characteristic-based approach is better suited to the PN context because it captures a higher level of detail by allowing flexible combinations of characteristics. Achieving this in a category-based approach would require a large number of categories to represent all the possible combinations. We have identified the following

characteristics of PN components from recent scientific literature as well as ITU-T X.1111 [3] and the NIST *"Guidelines on Cell Phone and PDA Security"* [9]:

Persistent Storage: *Does the component provide persistent storage capacity?* This characteristic encompasses storage of any type of data in the PN.

Processing Functionality: *Does the component process any information or data?* This characteristic is applicable to the majority of devices since it refers to any form of transformation or processing of data or information.

Communication Capabilities: *Does the component transmit or receive data?* By definition, this characteristic is applicable to all components of the PN since they communicate with each other or with external entities. This includes components that facilitate network communication such as the home network gateway.

User Interface (UI) Capabilities: *Does the component provide a local UI?* This characteristic includes all forms of user input or output that take place via a local UI on the component. This UI must not require any other component to achieve full functionality. For example, many smart home appliances can only be accessed via a web interface, thus providing remote accessibility but not a local UI. The component on which the user accesses this web interface provides its own local UI.

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.

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 is portable and also remains fully functional whilst moving.

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.

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.

Remote Accessibility: *Can the component be accessed or controlled by a remote entity?* This refers to any remote access, control or UI capability that does not take place via the component's local UI.

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 that provide value in the PN (e.g. any service that would have a negative impact on the PN if it becomes unavailable).

Consumption of Services: *Does the component consume services provided by other components in the PN or external entities?* This is applicable to all components that consume any type of service provided by another component or by an external entity.

Characteristics of the Personal Network

Although there is significant diversity between PN implementations, certain common characteristics are beginning to emerge. The following characteristics are important from a security perspective:

Absence of geographical locality *[10][11][7]:* Since the PN is not defined in terms of geographical locality, it must always be assumed that PN components might be in different areas. Although this does not affect the connectivity between devices, it means that this connectivity could be provided by third party networks. It also means that a device's location now represents a richer source of contextual information about the user (e.g. location-based services on the user's smartphone).

Device heterogeneity *[3][12][9]:* As described in ITU-T X.1111, the home network exhibits a high degree of device heterogeneity. As this is expanded to the PN, an even greater diversity of devices must be considered. The capabilities that could vary between devices include computational architecture and processing speed, data storage technology and capacity, communications capabilities, mobility, software and UI capabilities.

Communication diversity *[3][10][15]:* The PN also exhibits a high degree of communication heterogeneity since it utilizes a combination of communication technologies based on different communication channels and protocols. The PN could involve a combination of unicast, multicast and broadcast communication services.

Shared Components *[10][7]:* Since the PN is a user-centric construct, an individual's PN could include devices and/or communication infrastructure that are shared between multiple users. For example, smart home appliances could be shared between the residents or multiple applications could use the same cloud-based service. Depending on the system, users might be identified either as a group or individually. The identities of other users of the service may or may not be known. The identity model has an impact on the nature of the trust relationships between the users and is therefore important in defining the usage policy for shared devices.

Multihomed network topology *[3]:* A modern PN could have multiple connections to external networks such as the Internet. For example, home Internet connectivity is normally provided by the home gateway but most smartphones have the ability to share their mobile broadband connections with other devices (e.g. Wi-Fi tethering). Although not explicitly stated, this characteristic is implied in the ITU-T X.1111 model [3].

Dynamic nature *[15]:* The PN is dynamic in terms of the devices that are connected at any point in time and the communication links in use. Some services are provided and consumed in an on-demand manner, particularly those hosted in the cloud or provided by battery-powered devices. Furthermore, some devices might periodically leave and rejoin the PN or switch to a different type of communication network (e.g. a smartphone moving from home Wi-Fi to a public mobile network).

Energy-aware systems *[14]:* PN components are becoming increasingly aware of their energy use and are beginning to dynamically adapt their operation to minimize consumption or use energy at a more economical time. For example, in the smart energy grid, home devices and appliances dynamically change their behaviour based on the prevailing cost of electricity. Due to battery limitations, mobile devices are also becoming more energy aware and technologies such as mobile cloud computing are being developed to improve energy efficiency [14].

Attack Vectors of the PN

This section presents the primary attack vectors that are applicable to the PN. The references next to each heading indicate which analyses or publications include the attack. Only a subset of these attacks are included in ITU-T X.1111 [3] (those not included are indicated with an *):

Malicious Software * *[1][4][7][8][9]*: Malware can be defined as any undesirable software running on a device without the user's consent. This is arguably one of the most common attacks against end devices but could also be used for attacks on the network infrastructure.

Malicious Hardware * *[16]:* Malicious hardware is a much less common threat 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 for malicious purposes.

Exploitation of Flawed/Incorrectly Implemented Software * *[8]:* Another direct mechanism for achieving the attacker's objectives is the exploitation of design or implementation flaws in legitimate software in order to steal information, gain access or affect availability.

Exploitation of Flawed/Incorrectly Implemented Hardware * *[16]:* Similarly, it might be possible to exploit vulnerabilities in physical hardware systems in an attempt to steal information, gain access or affect availability.

Eavesdropping/Interception of Communication *[1][2][3][4]:* This is a common class of attack on networked systems, particularly those using wireless networks such as the PN.

Interruption of Communication *[3][16]:* Another potential attack on networked systems is interruption of communication which affects the availability of information and services and could be used to mount a denial of service attack in the PN.

Modification of Communication *[3]:* Modification of communication represents a class of attacks in which an attacker attempts to intercept communication messages, modify them and forward them to the intended recipient, whilst attempting to avoid detection.

Impersonation of Communicating Entity *[3]:* In a PN consisting of multiple communicating entities, another possible threat is the impersonation of one of these entities. If successful, the attacker gains the capabilities and permissions normally held by the impersonated device.

Unauthorized Remote Access *[3][7][9]:* For components that permit remote access, unauthorized use of this functionality could provide the attacker with access to all functionality available to a legitimate remote user.

Unauthorized Physical Access *[3][7]:* Unauthorized physical access to PN components is an attack vector that could be facilitated by various mechanisms including theft of a mobile device or misuse of a shared device.

Misuse of Device Interoperability * *[7]:* Lyle et al. argue that since security is a weakest-link problem, the least secure device in the PN could be used as a gateway to the rest of the network [7]. The increased replication of data between PN devices could also increase the probability of a data breach.

Exploitation of Flawed/Incorrectly Implemented Protocols * *[1]:* This threat includes various types of protocols especially those used for communication, authentication or access control.

Eavesdropping on User Interface *[3]:* An attacker could eavesdrop on the information transferred over a local UI. Examples include shoulder-surfing or entering login credentials on a shared device in view of other users.

Modification of Communication Routing *[1][3]:* An attacker could influence or modify the flow of information within the PN (e.g. modifying the routing configuration of the home gateway).

Mapping Attacks to Characteristics

As indicated in the previous section, certain attack vectors are only applicable to PN components that exhibit specific characteristics. 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 as a matrix in the technical report [13].

Using the Security Analysis

In this section we present a scenario illustrating the use of this analysis to assess the possible attack vectors for two PN systems commonly found in the home: a tablet PC and a home energy management system (HEMS). The first step is to identify the characteristics of each device. Both provide non-volatile storage, processing and communication. The HEMS usually does not have a local UI but provides remote accessibility (e.g. via a web interface). It has direct control of external physical infrastructure (e.g. controlling smart appliances), and provides services (e.g. energy management). In contrast, the tablet has local UI capabilities, physical mobility and support for third party software, It can control other components and consume services (although in this example, it is assumed not to provide any services). The mapping described in the previous section can be used to determine the primary attack vectors for each device. In addition to the attacks common to both devices, the tablet's mobility makes it more vulnerable to unauthorized physical access (especially if it is a shared device), whilst the HEMS is vulnerable to unauthorized remote access due to its remote accessibility. The tablet is vulnerable to eavesdropping on its local UI and is more vulnerable to malicious software because of its support for third party software. However, both are still vulnerable to software exploits. In terms of the defined characteristics, these two devices are relatively similar but are clearly vulnerable to different attack vectors. More striking differences can be observed by contrasting embedded devices (e.g. wireless sensor nodes) with full-featured devices. Overall, it is anticipated that this analysis will have two primary use cases. The first is the assessment of existing PN implementations in order to determine the primary attack vectors and improve security by deploying appropriate defences or mitigation strategies. The second is in the design of new PN components and technologies. By identifying the primary attack vectors based on the component's characteristics, the relevant mitigation strategies can be included in the design phase.

Conclusion and Future Work

Various security analyses have focussed on specific devices or geographically-defined networks but few have considered the emerging paradigm of the *Personal Network* (PN). We have consolidated and systematized previous work into a comprehensive security analysis of the PN. In particular, our work enhances the framework of security technologies presented in ITU-T X.1111. Our characteristic-based approach makes it possible to associate specific characteristics with each PN component and thus identify the set of possible attack vectors for that component. Compared to the category-based methodology used in ITU-T X.1111, our approach

captures more detail and is therefore better suited to the high degree of heterogeneity in the PN context. Based on recent research, our analysis also includes new attack vectors in addition to those addressed in ITU-T X.1111. We suggest that this analysis can form the basis for future work towards mitigating the identified threats and thus enhancing the security of the Personal Network.

References

[1] Baugher, M., and Lortz, V. Home-network threats and access controls. In *Proceedings of the 4th international conference on Trust and trustworthy computing - TRUST '11* (June 2011), 217–230.

[2] Friedman, J., and Hoffman, D. V. 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 (2008), 159–180.

[3] International Telecommunication Union. ITU-T Recommendation X.1111 - Framework of security technologies for home network. Tech. rep., International Telecommunication Union, 2007.

[4] Landman, M. Managing smart phone security risks. In *Information Security Curriculum Development Conference* (Oct. 2010).

[5] Lee, J. I., Choi, C.-S., Park, W.-K., Han, J.-S., and Lee, I.-W. A study on the use cases of the smart grid home energy management system. In *ICTC 2011*, IEEE (Sept. 2011), 746–750.

[6] Leung, A., Yau, P.-w., and Mitchell, C. J. Using Trusted Computing to Secure Mobile Ubiquitous Environments. *Security and Privacy in Wireless and Mobile Networking* (2009), 303–335.

[7] Lyle, J., Paverd, A., King-Lacroix, J., Atzeni, A., Virji, H., Flechais, I., and Faily, S. Personal PKI for the smart device era. In *9th European PKI Workshop: Research and Applications* (2012).

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

[9] National Institute of Standards and Technology (NIST). SP800-124 Guidelines on Cell Phone and PDA Security. Tech. rep., 2013.

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

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

[12] Oberheide, J., and Jahanian, F. When mobile is harder than fixed (and vice versa). In *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications* (Feb. 2010).

[13] Paverd, A., El-Moussa, F., and Brown, I. Characteristic-Based Security Analysis for the Personal Network. Tech. rep., 2014. https://www.cs.ox.ac.uk/people/andrew.paverd/home.

[14] Paverd, A. J., Inggs, M. R., and Winberg, S. L. Towards a Framework for Enhanced Mobile Computing Using Cloud Resources. In *Proceedings of the Southern Africa Telecommunications, Networks and Applications Conference* (2011).

[15] Schwiderski-Grosche, S., Tomlinson, A., and Irvine, J. Security challenges in the personal distributed environment. In *IEEE 60th Vehicular Technology Conference*, vol. 5, IEEE (2004).

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

[17] Webinos. Phase 1 - Architecture and Components. Tech. rep., 2011. http://webinos.org/downloads/.