Rethinking Home Network Security

Conference Paper · April 2018

DOI: 10.14722/eurousec.2018.23011

CITATION
1

READS
25

2 authors, including:

Norbert Nthala
University of Oxford
3 PUBLICATIONS **4** CITATIONS

SEE PROFILE

Rethinking Home Network Security

Norbert Nthala
University of Oxford
norbert.nthala@cs.ox.ac.uk

Ivan Flechais
University of Oxford
ivan.flechais@cs.ox.ac.uk

***Abstract*—The continued rise in the number of managed and unmanaged devices connected to home networks has expanded the threat surface in the home. We have seen increases in the number and impact of attacks targeting network and IoT devices in the home, yet effective mitigations targeting the home are still too few. Approaches have been proposed to holistically secure the home network, but such proposals also face a number of challenges in their practical uptake. More empirical research needs to be done to understand the context of use and needs of the stakeholders involved in securing home networks in order to rigorously evaluate and inform these solutions.**

As a step in this direction, we conduct a Grounded Theory exploration of context aimed at 1) understanding current security practice in the home to identify the areas that need improvement or support, and 2) identifying security-related practices in the home that could be leveraged to improve network security. We found evidence that current security practices in the home are focussed on securing endpoints; home users assess risk by evaluating the impact of a successful attack, and also the value of gain for the attacker; identification of security problems in the home is done through visibility of harm, security alerts and warnings, and intuition; incident management in the home is mostly done through social networks and often undertaken by trusted individuals as an informal duty of care. We discuss these findings and provide recommendations for improving network security in the home.

I. Introduction

The world has seen, and will continue to witness, growth of networked and network services in homes. Internet Live Stats reveals that over 46 percent of the world's population (3.4 billion) had Internet access in their homes by July 2016, up from 29 percent in 2010 [31]. Similarly, homes have seen a spike in the number of connected devices, partly attributable to the advent of smart and IoT devices. While there are several immediate benefits to the home brought by this growth, several negative consequences have also arisen. News about large scale cyber-attacks targeting connected homes have regularly made headlines in recent years, and the impact from such attacks is not only felt by the home user, but the wider community too.

In 2011, an attack affecting 4.5 million DSL modems (for both individual and business users) in Brazil was brought to light by Kaspersky Lab [2]. The attacker(s) managed to compromise modems from 6 different manufacturers, and affected major Internet Service Providers (ISPs) in the country. The attackers configured malicious DNS servers in the modems, *"where several domains running fake pages of Brazilian banks were hosted. Other bad guys took advantage of the redirections to install malware on the victims machines."* As part of understanding the vulnerabilities that were exploited in this attack, blame was placed on the *"neglect of ISPs, blunders from hardware manufacturers, under-educated users and official apathy" [2].*

In March 2014, security firm Team Cymru discovered that over 300,000 home routers in the UK were hijacked by attacker(s) who then re-routed traffic to different DNS servers over the Internet [30]. In December the same year, the Lizard Squad managed to take down two of the world's biggest networks: Microsoft Xbox Live and Sony PlayStation Network, through a DDoS attack that is believed to have largely been enabled by thousands of compromised home routers [22], [28]. In November & December 2016, home routers in Germany and UK were targeted by Mirai malware which led to service outage for approximately 900,000 home customers in Germany, and an unidentified number of homes in the UK [10].

Attackers have not only targeted core network devices in the home. The October 2016 attack on DNS provider Dyn, for instance, is thought to have been enabled by insecure IoT devices in connected homes [4], despite efforts from different stakeholders to encourage home users to secure their endpoints. Some of these IoT devices have no management interfaces and bring their own vulnerabilities into the home network. As growth in this sector is expected to continue (a forecast by Statista indicates that the global smart home market is to grow to $40.9 billion by 2020), the rising number of connected devices in the home network and the evolving threat landscape that is increasingly targeting the home are heightening the importance of effective security in the home [8], [16].

Efforts to improve security in the home have centred on the provision of awareness, and technical solutions focussing on endpoint security: antivirus, patching, data backup, and parental controls. Even so, evidence [3], [13], [24], [29] shows that most home users do not follow such recommended practices. While endpoint security is important, Stawowski [32] notes that network safeguards provide the first line of defense for IT system resources against attacks, both internal and external. The key challenge facing home network security proposals is that they require a high level of security expertise to understand and implement, and yet home networks are administered by inexperienced users as indicated in [15], [25].

To help address the home data security problem, different approaches have been proposed [8], [11], [14], [16], [23], [33]–[36] (a summary of these approaches is presented in section II-B). The basis of these proposed approaches is to remediate

European Workshop on Usable Security (EuroUSEC) 2018
23 April 2018, London, England
ISBN 1-891562-54-1
https://dx.doi.org/10.14722/eurousec.2018.23011

a *lack of expertise of the home user* with designs informed by an understanding of the *threat model* for home networks. The tools and infrastructure propounded aim to take security responsibility away from the *inexperienced* home user.

Our view is that the security needs of the home user are much more intricate and nuanced than has been assumed. Home users exist in different environments, with different infrastructures and security needs. In each of the varying contexts, their requirements might differ. The importance of the context in security has been highlighted before [12], [17], [27]. In addition, most of the proposed approaches recommend major changes to the current infrastructure, interventions that might be costly, complex, and inapplicable in most current environments. Supporting network security in the home should be based on a grounded understanding of the current security practices in the home and their constraints.

As a step in this direction, we conducted a qualitative Grounded Theory study of 50 home users and two Internet Service Providers (ISPs). The aim of our study is twofold: a) to understand current practice of home network security from which we identify areas that need improvement or support, and 2) identify other security-related practices in the home that could be leveraged to improve home network security. As Taylor et al. [33] observe, enterprise networks follow best practices and security measures (discussed in section III-A), and we draw from these to explore home network security practices.

Our analysis reveals the absence of a systematic approach and appropriate tools to managing network security in the home. The following are our core findings:

- ISPs implement cost effective, and scalable solutions (for securing connected homes) that respect responsibility boundaries and have business value.
- Understanding of risks in the home is based on a light evaluation of the perceived gain of the attacker, and the perceived value of impact from a successful attack.
- Security problems in the home are identified through the visibility of harm, alerts and warnings, and intuition.
- Social networks offer a strong reference point (or support function) for incident response and security management in the home.

We discuss work that has been carried out on home network security in section II, followed by a brief review of recommended network security practices in section III. We present the methodology adopted in our study in section IV. The results of our study are presented in section V, and finally the discussion of the results and conclusion are in sections VI and VII respectively.

II. Related Work

In this section, we review prior work in understanding and improving the security of data and systems in the home. We present an overview of past approaches to security in the home, and review recently proposed techniques to improve security practice in the home.

A. Security in the Home

Evidence [3], [13], [24], [29] and the proliferation of attacks targeting unmanaged endpoints and home network devices [2], [10], [22], [30] show the insufficiency of endpoint-focussed security solutions. This has driven research into ways of securing the home holistically through network security to complement endpoint security.

Niemietz and Schwenk [26] investigate how fingerprinting attacks can compromise router settings in homes. They evaluate the security of management interfaces for ten routers that are commonly used in homes, and compromised most of them. They conclude with recommendations to improve home router security: randomization of default login data, minimal information leakage, use of SSL/TLS, input validation, use of X-Frame-Options, setting the window name object to a random value, and using cookie flags: httpOnly and secure.

Similarly, Karamanos [18] evaluates the security of routers used in homes against different attacks. The attacks include authentication bypass, password guessing and brute force attacks, cross site request forgery, and UPnP exploitation. The researcher managed to conduct the attacks on the selected devices, and recommended: user awareness on account security, and for manufacturers to provide systems with well-implemented security that is transparent to the end user. Other recommendations to manufacturers of devices include use of secure kernels, applying software upgrades to the router, packet inspection, and use of lightweight versions of intrusion detection and intrusion prevention systems.

Additional research has been conducted to improve home network security on the basis of targeting the lack of expertise of the home user. We review some of these in section II-B.

B. Proposed Home Network Security Approaches

Xu et al. [36] propose a traffic profiling system for home networks that automatically collects and analyses home network traffic. The system is designed to leverage programmable home routers. The main aim is to analyse and report the behaviour of network devices, and also to detect anomalous behaviour. Researchers in [34] put forward an infrastructure that collects data from heterogeneous sources: home network traffic, intrusion detection logs from distributed firewalls, active open DNS resolver scanning, continuous snapshots of Internet routing tables, and geographic databases of Internet end hosts. Their approach integrates all the data and performs traffic analysis to detect attacks.

In a similar way, researchers in [35] propose a bloom-filter based analytics framework to capture persistent threats towards home routers, and identify correlated attacks towards distributed home networks. This is achieved by collecting and analysing inbound & outbound traffic, and traffic within the home. Martin et al. [23] propose a solution to prevent the exploitation of bugs in outdated software and weak passwords on a home network. Their solution aims at raising an attacker's uncertainty about devices, and enable the home network to monitor traffic, detect anomalies, and filter malicious packets. The proposed infrastructure makes use of a chain of honeypots and deep packet inspection that collects suspicious packet traces, acquires attack signatures, and installs filtering rules at a home router in a timely manner.

Taylor et al. [33] take a different approach to solving the problem of home security. The researchers put forward a cloud-driven infrastructure, which combines software-defined networking (SDN) & proxies with commodity residential Internet routers. They propose that security management be outsourced from expert service providers. At the centre of the solution is a modification to residential routers to allow them to export management to a remote controller using OpenFlow protocol, and a series of device proxies. In the same line, Hafeez et al. [15] propose a cloud-driven, Software as a Service (SaaS) solution that applies SDN to improve network monitoring, security, and management. The proposition utilises a modified gateway running an SDN controller and OpenVswitch to enable remote management of the home network through Cloud Security Service (CSS). Feamster [11] also proposes outsourcing security management of home networks to a third party with expertise. The solution harnesses programmable network switches and distributed network monitoring and inference algorithms.

Lastly, Cruz et al. [8] discuss a cooperative security management infrastructure between ISPs and home users. The researchers propose adoption of a Distributed Intrusion Detection System (DIDS) architecture. This is to achieve distributed monitoring of service activity and network traffic by specialised components at the remote gateway, and distributed inference and correlation at ISP level to process information from remote gateways. All operation is to be centrally orchestrated on the ISP's infrastructure.

Most of these proposals to improve network security in the home operate from the presumption that home users do not have the expertise or ability to perform security work in the home, and aim to take this responsibility away from home users. Our view is that this is in contrast with our observations of actual security work in the home, where social relationships are leveraged to provide tailored and trusted security work. Instead of removing the burden of work from the home user, another option would be to leverage existing practices and provide a solution that ties into existing arrangements.

We adopt a practice-based approach to ground our understanding of the problem domain, and from this gain insights into how appropriate technology and other forms of intervention could be developed. While the home faces many challenges, the enterprise security domain is a useful domain to draw inspiration from, as also noted by [33]. Accordingly, we review some of the core enterprise security practices and recommended network security practices in III.

III. Recommended Security Practices

In this section, we first discuss recommended practices in corporate security, and follow with a review of recommended home network security practices.

A. Enterprise Network Security

While Enterprise Network Security is a significant area of research and industry practice, our review draws on acknowledged best practice, in particular the ISO/IEC 27033 network security standard, NIST SP 800-27 Rev A standard, CERT System and Network Security Practices, and key textbooks and publications.

1) Security Principles: Corporate environments have a wide range of standards and guiding principles to ensure the security of their systems and data. Standards such as the NIST SP 800-27 and ISO/IEC 27033 provide corporate security practitioners with principles that should be followed when designing and managing the security of their infrastructure.

One such principle is the *use of layered security* to increase resilience. The goal is to ensure there is no single point of vulnerability or failure. Sub-principles under this include the "security trinity" [6]: Protection, Detection, and Response; and also "defense in depth" by having controls in multiple places of the system, such as on endpoints, but also on network devices. Measures are taken to identify and then secure the weakest link in the security chain, e.g. the gateway may need hardening as it is commonly targeted.

Compartmentalization of information is another core principle in enterprise security. Security measures are formulated to address multiple overlapping information domains. Based on sensitivity levels of information, different security zones can be created. Examples of security-related technologies utilised to achieve this would be network segmentation, classification schemes, and network Demilitarised Zones (DMZ).

In concert with the above, the *principle of least privilege* aims to ensure that users are granted the minimal privileges necessary to perform their roles within the different information compartments described above. This is achieved through a need-to-know basis in some environments, careful reasoning about permission assignments, and also requires the *use of unique identities to ensure accountability*.

2) Security as a Process: In addition to the principles discussed above, the guidelines in ISO/IEC 27033-1, the principles in SP 800-27 Rev A, and the CERT system and network security practices emphasize that security is a continuous process involving several phases. SP 800-27 categorises security principles in terms of a project management life cycle: initiation, development/acquisition, implementation, operation/maintenance, and disposal. ISO/IEC 27033-1 outlines network security planning and management guidelines, which follow a cycle pattern similar to the SP 800-27. The CERT system and network security practices [1] define five top-level steps: harden/secure, prepare, detect, respond, and improve.

We summarise this as a security process with four core stages: Assessment, Protection, Monitoring, Response. A wide range of tools are available in the corporate environment to ease the management of each of these phases. These include configuration management tools, vulnerability scanners, intrusion detection and intrusion prevention tools, and several tools for incident management and reporting among others.

B. Home Network Security

After looking at network security practice in a corporate environment, we now review the recommendations for home network security. We consider the ITU-T X.1111 recommendation: framework of security technologies for home network, and US-CERT guidelines on home network security (https://www.us-cert.gov/ncas/tips/ST15-002).

ITU-T X.1111 takes a technology-centred approach to home network security. The standard provides a general home

network model for security, and describes threats and security requirements to the home network. In addition, X.1111 categorizes security technologies by security functions that satisfy the security requirements. The security threats presented in the recommendation include eavesdropping/disclosure/interception, interruption/communication jamming, injection and modification of data, unauthorized access, repudiation, shoulder surfing, lost remote terminal, and stolen remote terminal among others. Suffice to say that the threats might be targeted or non-targeted, and they might directly or indirectly target an individual or a community (such as a family, friends, colleagues, neighbours, and/or a household).

The recommendation presents the following as security requirements in the home: data confidentiality, data integrity, authentication, access control or authorization, non-repudiation, communication flow security, privacy security, and availability. And finally the security functions to satisfy these requirements are outlined as encipherment (or encryption), digital signatures, access control, data integrity, authentication, notarization, message authentication codes, and key management.

US-CERT provides a range of recommendations for securing the home network (https://www.us-cert.gov/Home-Network-Security), most of which are for endpoints. These include use of antivirus, data backup, patching, and mindfulness among others. Another security tip for "securing your home network" (ST15-002) outlines countermeasures to prevent unauthorized access to the home network. These include changing the default username and password, changing default SSID, logging out of the router management interface, configuring WPA2, disabling UPnP when not needed, upgrading firmware, disabling remote management, and monitoring for unknown device connections through the router's management website.

In the next section we discuss the methodology we adopted to investigate the security practices in the home and how enterprise principles of network security can be applied to home networks.

IV. Methodology

Our research aim is to investigate home network security practices in order to understand how home users and ISPs secure home networks and also to identify other security-related practices in the home that could be leveraged in improving home network security. Our approach is qualitative, exploratory and sense-making, and we focus in the first instance on how home users perceive their own security practices by collecting data from semi-structured interviews with selected home users. We acknowledge that more research will need to be done to identify whether home user perceptions of security practices match their actual and observable behaviour, but we believe that it is reasonable to scope our research accordingly to inform our initial understanding.

Our choice of semi-structured interviews to collect our data allows us to cover a common number of topics in home data security practices while retaining the flexibility to explore interesting responses in more detail. A set of guiding questions was developed based on our understanding of typical security management processes. These questions controlled the flow and consistency of the interview, while keeping the interview open for both depth and breadth topic exploration as the interview progressed.

The study was ethically reviewed and approved by the Social Sciences and Humanities Inter-divisional Research Ethics Committee at our institution.

A. Participant Recruitment

We recruited home users for the interviews by advertising through community centres, newspapers (in print and online), and other social groupings, and by putting up posters at the National Museum of Computing. The recruitment was conducted in different locations in the UK. Each participant was compensated with a £10 Amazon voucher for an approximately one-hour interview session.

In addition to home users, we recruited ISPs through emails, and at a conference where representatives from most of the ISPs operating in the UK were in attendance.

B. Semi-structured Interviews

Prior to the interview, the 50 participants were asked to complete a demographic form, which included questions regarding the devices and services they use. During the interview, we asked the participants questions in the following categories: (1) *Protection:* we asked about the participants' data security concerns and what they did to keep the concerns in check; (2) *Response:* we sought to know if the participants have experienced a security incident before (successful or not), and what they did in such a scenario. We also asked the participants where they (would) seek help in case of a security incident; (3) *Monitoring:* we asked the participants how they knew about any security incident they had experienced, and what they use to know of any incident. We also wanted to know any other security-related changes they have made to any device or service in the home, and what prompted them to do so. (4) *Assessment:* we also asked the participants for instances where they had security concerns or had heard of some possible security measures, but they did not follow recommended action, and why they did that; for each security-related action carried out, we asked for the reasons motivating it. In addition to these questions, we asked the participants for any challenges they had faced in making security decisions; rules and guidelines they followed in making security decisions; sources of such rules or guidelines; sources of security information, advice, and technical support; examples of what they considered to be good security practices/measures/controls; and whose responsibility it was for implementing good security practices. All these topics were grounded in specific scenarios that home users would have encountered at least once before. The researcher was careful to avoid specifically discussing *network security* as this could lead to ambiguity and may have been confusing to the participants. Finally, the researcher asked for an enumeration of the security measures on all devices in the home, including endpoints and network devices. The interview duration varied between 30 and 60 minutes.

For ISP interviews, we adopted a project management life cycle approach, asking security questions pertaining to each phase - an approach ideal for understanding business processes. The aim was to understand the different activities that ISPs undertake to secure homes and the extent of such

activities. Prior to delving into details of each phase of the life cycle, we asked the participant questions regarding the services and devices sold and/or rented to customers; and the threats from which the ISP protects customers. Moving forward, questions were categorised as follows: (1) *Installation/Commissioning:* we sought to know the categories of security settings/considerations done during installation of a service or device, whether home customers are allowed to use their own modems and/or routers, additional things the ISP does to protect home customers apart from settings in services and devices, and the level of involvement (if any) of home customers when making security configurations. (2) *Operation and Maintenance:* we asked the participant about (a) routine maintenance - if they perform any and examples, and whose responsibility it is to maintain and secure ISP-provided devices when they are in operation in the home; (b) expectations - the expectations of the ISP of what home customers should do on their end to secure their systems, how the ISP communicates such expectations, and how the ISP ensures that customers are meeting the expectations; (c) troubleshooting - measures the ISP has in place for identifying problems/issues affecting customers, how the ISP deals with customer problems, and whether there is any coordination with other stakeholders in dealing with customer incidents; (d) support - kinds of support the ISP offers to home customers, channels through which support is offered, and costs associated with support. (3) *Decommissioning:* we asked the participant how they deal with obsolete devices from homes after an upgrade, and what happens to customer devices and data when they cease to use the ISP's services. We concluded the interviews with questions regarding what the ISP wishes they would do more to protect home customers, where they draw the line between protecting the ISP's internal infrastructure and protecting home customers, and the challenges the ISP faces in securing home customers. The interviews lasted between 60 and 120 minutes.

C. Grounded Theory

While this data was being collected, we conducted a qualitative analysis using Grounded Theory [7]. Grounded Theory is aimed at developing a well integrated set of concepts that provide a thorough theoretical explanation of social phenomena under study. It is best utilised where little is already known and makes use of constant comparison to generate the concepts, and explain the relationships between them. This makes it ideal to study the network security and decision-making practices in the home in order to come up with a coherent understanding of all issues surrounding the topic.

The analysis involved three researchers. The primary researcher conducted the initial open coding of the interview transcripts. To ensure credibility of the codes, a second researcher cross-checked all the codes against the interview transcripts. At the same time, the third researcher reviewed the initial codes and all quotes supporting each code. Any differences and/or issues arising from the initial coding were discussed and resolved among the three researchers. A codebook consisting of 130 codes emerged from the initial coding. These codes were then applied across other interviews through constant comparison, while new codes were added as they emerged and were deemed necessary. In further analysis, the three researchers discussed and grouped the codes into themes (axial coding) and categories (selective coding), based on the properties and dimensions of each theme. Regular coding meetings were held to discuss any emerging codes and to group the codes into families.

D. Limitations

Our study has some limitations. First, all are participants are residents of the UK. This might raise questions regarding generalisability of our results. However, we have documented the procedure we followed in this study, which makes it possible for other researchers to replicate elsewhere.

Second, common to all qualitative studies, researcher bias is a concern. A single researcher, trained to conduct research interviews, conducted all the 52 interviews. The researcher avoided leading questions, and ensured participants felt comfortable to respond to questions. The researcher avoided interrupting participants, and probed for more information when required. To further mitigate bias, two other researchers reviewed and were part of the data analysis to enhance consistency in data coding.

V. Results

In this section, we discuss the results from our study. We present the participant demographics, security practices in the home, assessment of risk in the home, detection of incidents and attempts, and security incident response.

A. Participants

A sample of 60 home users was selected for interview, 50 of which attended the interview. We made sure to keep a balance between male and female participants, as well as a diversity of age, ethnicity, education, and employment status. Demographics for our 50 participants are shown in Figure 1. Two participants indicated being both students and employed, while one indicated being both employed and self-employed.

Fifty two percent of our participants were male, while forty eight percent were female. Forty four percent belonged to the 18-34 age group, while forty eight percent belonged to the 35-64 age bracket. During the interviews, these two age groups were noted to be the ones responsible for making most of the security decisions in the home environment. The other two age groups, 12-17 and 65+, made up four percent of the participants each. Thirty two percent of the participants held postgraduate degrees, twenty four percent had graduate degrees, sixteen percent completed undergraduate studies, four percent completed trade/technical/vocational training, twenty two percent completed high school, and two percent did not complete any school level. Apart from the finding that those below the age of 18 depended on their guardians for the security of the devices and services they use, our analysis showed no differences in our studied security practices in the home caused by the other demographics shown in Figure 1.

8 ISPs were contacted, but only 2 accepted to take part in the study. We interviewed 2 participants from the 2 ISPs, both responsible for managing security interventions for home customers for each respective ISP. The ISPs operate throughout the UK, and have a user base of over 15 million combined. They both offer a range of services, including broadband, TV, and communication (phone services).

Demographic	Category	Number of Participants
Age		
	12-17	2
	18-34	22
	35-64	24
	65+	2
Gender		
	Male	26
	Female	24
Highest educational level		
	No schooling completed	1
	High School	11
	Trade/technical/vocational training	2
	Undergraduate	8
	Graduate	12
	Postgraduate	16
Ethnicity		
	White	39
	Hispanic/Latino	1
	Black/African/Caribbean	5
	Asian/Pacific Islander	5
Marital Status		
	Single	28
	Married	18
	Divorced	3
	Separated	1
Employment status		
	Employed	28
	Retired	3
	Self-employed	8
	Not working	2
	Student	12

Fig. 1. Interview participant demographics

Assessment	Protection	Monitoring	Response
Antivirus			
	Firewall	Inbound and Outbound Traffic Monitoring for Malware	Adware remover
	Harden browser settings		Report
	Data backup		Network disconnection
	Encryption		
	Adblocker		
	Authentication (password, biometric, 2FA)		
	Password manager		
	VPN		
	Delete unused software and apps, cookies, browser history		
	Patching/Updating		
	Parental controls		
	Router firmware upgrade		
	Mindfulness		

- Security that ISPs can provide is highlighted in grey

Fig. 2. Security Practices in the Home

B. Securing the Home Network

To contextualise the interview questions, the researcher started by eliciting data regarding the devices and services that each participant used in their home. Common devices (owned and/or used by at least 3 participants) in the home included computer, laptop, tablet, smartphone, modem, router, switch, game console, security camera, digital camera, TV, set-top-box, and smart devices (e.g. fit bit). Most of the routers, modems, and set-top-boxes in the participants' homes were sold by or rented from an ISP. Common services include banking, shopping, entertainment (gaming; watching/streaming/downloading video/TV, music, etc.), work, education, home security, health management.

We gathered data on security practices aimed at securing data and systems in the home. This included use of security-related technologies and mindful behaviours available in the home. Data was gathered from both home users and ISPs. Figure 2 summarises the security practices from our analysis of the interviews. While this is not a comprehensive list of all security practices in the home, we believe that it gives an indication of a typical home security posture. *Assessment* in this case refers to vulnerability assessment, and risk assessment; *Protection* encompasses practices for hardening the security of a system; *Monitoring* refers to practices for detecting security threats; and *Response* includes practices for managing and reporting security incidents.

1) Interventions by Home Users: 'Mindfulness' in the figure comprises deleting or not opening email attachments from unknown sources, shopping from secure websites (check availability of padlock or https), looking out for phishing emails, making online payments through PayPal, stream legal content only, avoid sharing passwords, and minimising amount of information shared especially online.

With the exception of the firewall, all other security practices are for endpoints, mainly computers, laptops, tablets, and smartphones. The researcher asked the home users of any security measures taken to secure the network devices, including switches, modems, and routers. Of the fifty participants, only two had implemented a firewall on a router.

Our analysis revealed two main reasons our home user participants did not apply security measures to network devices. 1) They assume the router is secured by the ISP who provided it - *implicit delegation of security responsibility*. One participant said *"The router comes with everything set properly. We just connect and start using it. Our Internet Service Provider does everything for us. If there is anything to change for security, I think they do all that"* - P25. 2) Home users assume that network devices are already secure when they are purchased, whether from an ISP or elsewhere - plug and play: *"I bought my router from Amazon, and I think everything is configured in the best way possible - all firewalls are already there. I just connected it and somebody helped me setup our Internet connection"* - P47. 8 of the 50 participants use routers purchased elsewhere, other than from an ISP.

We did not ask our participants to assess and report on their technical or security expertise. However, 5 participants reported that they are employed in a security role in their organisation. 10 other participants have technical jobs (including software developer, database engineer, IT support technician) that involve some security tasks. These 15 participants reported learning from their jobs and applying some of their organisational security controls and practices in their homes, and in the homes of those they help. One participant said, *"It's normally the kind of stuff I do at work, except for some of things which use expensive and complicated software"* - P19.

Overall, 36 participants reported offering security help to their family, friends, and colleagues. 19 of these have offered one-off help, while the other 17 have taken on the responsibility of managing the security of their families or friends. *"I always visit my parents' home to check their devices if they are secure. I just scan them to see if there is a virus.*

When I see something I don't know, I take the computer to a colleague in our IT Support." - P1. The kinds of security measures that our participants reported to have implemented in their homes, and the homes of those they help are listed under *protection* in Figure 2.

The mode of offering support is either *in-person* or *remotely* via a phone. We identified in-person help where the helpers visited the homes of those who need help, and/or devices such as laptops, phones, and tablets were brought to the helpers for their assistance. Remote help on the other hand was reportedly offered where the helpers had no physical access to the devices of those being helped. Most of the 36 participants who had offered help reported having used one or the other, or both means at some point. For instance, *"I call my parents to check if there are any issues affecting their computers. If they complain and I don't understand what they say, I try to make time to go and see what the problem is"* - P49.

2) Interventions by ISPs: On the other hand, our analysis revealed that ISPs approach the security of their home customers in two ways:

Duty of Care: The participants indicated that the ISPs understand their duty to provide cyber care to their customers. In this regard, they provide a generic basic-level of security which includes free antivirus, firmware-upgrade (for customers using ISP-provided devices such as modem/router, and set-top-boxes), parental controls, and traffic analysis for suspicious behaviour on traffic going to or exiting a home network (highlighted in grey in Figure 2). If suspicious traffic patterns are detected, the originating customer's home is disconnected and the customer alerted. Customers are informed of the reasons behind the disconnection, and are advised to take necessary actions before they are reconnected.

While both participants indicated the ISPs' wish to do more, they indicated that their involvement in home network security is limited by two main factors: 1) *cost*: it is expensive to implement and maintain an infrastructure that takes care of the security of all customers; and 2) the router marks the edge of the ISP's *responsibility boundary*—according to regulations and also context (the ISP does not know the needs of the home user). One of the two ISPs engaged does not allow customers to use routers purchased elsewhere for their connection, only the ISP's own. The other ISP on the contrary gives customers the freedom to connect their own routers.

Business Need: The limitations on how much ISPs could offer as a duty of care have provided a business opportunity to ISPs who now offer Security as a Service, in addition to the generic interventions offered under the duty of care. Unlike the duty of care, this offering is targeted, and comes with specialised support. Aside from offering security as a service, the need for ISPs to maintain their *reputation* in a competitive market forces ISPs to offer some level of security, such as that mentioned under the duty of care.

Both participants indicated that they strive to implement solutions (either as a duty of care or as a service) that can *scale well* with growing numbers of their customers. One participant said: *"We need to make sure that whatever we are introducing will be sustainable for our growing number of customers for the next few years"* - I2.

C. Evaluating Security in the Home

We sought to find out how our participants arrive at the decisions to implement the security controls presented in Figure 2. Our aim was to understand how they identify risks in their context, and how they evaluate them.

Our analysis revealed two main ways through which our participants identify risks. First, through personal or vicarious negative experience. The participants reported learning from what other people using similar technology have experienced, and applying that experience to evaluate their home context: *"I have not lost data on my laptop, but one of my friends lost everything because he had a virus. So I installed an antivirus on all computers in our home"* - P35. For others, the experience was personal.

Second, participants reported hearing of risks from the media. Sources include news about attacks, awareness campaigns, and online fora. Some participants reported: *"You always hear on the news that someone has lost money, or their data has been exposed. I don't want that to happen to me"* - P41, and *"We just use most of these devices and software. We don't know whether they are good or they are bad. But I am a member of an online forum where people discuss these issues. Some are experts in security, and they provide useful feedback when you ask. I find it very useful"* - P6.

Our analysis revealed two main ways through which our participants evaluate security risks in their context to decide on the appropriate course of action: *perceived value of impact of a successful attack* and *perceived gain of the attacker*.

1) Perceived Value of Impact: 46 out of 50 participants reported evaluating the severity of an attack by assessing the value of its perceived impact. Our analysis revealed that the value is highly contextual and is evaluated on the basis of 1) security concerns for the particular home user - according to 46 participants, and 2) personal or vicarious experience - reported by 8 participants .

For the security concerns, our findings are similar to [27], where three clusters of concerns were identified: loss, nuisance, and uncertainty. Loss includes loss of privacy, money, data, and control among others: *"I don't want to lose my documents - they are my life"* - P27, *"I don't share my laptop and phone with anyone else. They are private and I would not allow anyone to look at what I keep or do"* - P49. Nuisance comprises things the participants find annoying, such as ads, and spam emails: *"I have had ads pop up on my browser now and again, so I bought an adware remover so that I could not be disturbed again"*- P2. Uncertainty on the other hand consists of unclear security-related issues, such as *"I don't know what the app does, whether it steals my data. But I just chose to accept the risk"* - P15.

The participants reported making trade-offs in their security decisions. *"I don't mind exposing my pictures, but my bank details are the most important. I can lose money."* - P31. In addition, the concerns are contextual, and reactions depend on the estimated value of loss resulting from an attack. A previous personal or vicarious experience plays an important role in risk assessment. A common scenario was *"there are always lots of security warnings and pop-ups when I'm on the internet saying this is not secure. I always ignore the warnings because I know*

the resources and I have used them before. Some are academic websites and even well known online retail websites that I always shop from like Decathlon. I don't know who sends those warnings, but they are boring" - P8. *"I once had a browser pop-up which said that my computer was infected with a virus, and that Apple had detected it so they wanted to help. They requested for my Apple ID and password. Since I was having a lot of ads, I thought they would help with that so I provided my credentials. I waited for minutes and nothing happened, no feedback. So I just shutdown my computer and changed my password later"* - P15. Examples regarding security warnings were shared by a number of our participants.

2) Perceived Gain of the Attacker: Our analysis revealed that 26 of the participants evaluate the value of gain for the attacker as a basis for taking security action. The participants reported that *"Well, I am not an important person, why would someone target me? If I were like the Prime Minister, then I would hire someone like you to take care of my security. But I do not see the need for doing much security-wise. An antivirus is enough"* - P45; and *"I don't think I have anything interesting in my home that someone would be interested in. My life is boring"* - P34.

D. Identifying Security Problems in the Home

The quest to understand how our participants identify security problems affecting them in the home revealed three ways used by our participants: *visibility of harm, alerts and warnings*, and *intuition*.

1) Visibility of Harm: Given the typical absence of vulnerability assessment tools in the home, and also limited monitoring, the presence of harm is seen as one way of detecting an attack according to responses from 33 individuals. The evidence of harm that our participants reported seeking is either to them or to their friends and relatives. *"I have not had any harm in my home network, so I think everything is fine, bullet-proof"* - P38. Such evidence is sought in different ways; *"I have not lost money in my account yet, so all should be well"* - P6, *"I don't think there is anyone who managed to see the photos in my phone"* - P44, *"I lost very important documents some years back, so since then I decided to always use and update an antivirus"* - P13, *"I don't think there is anything I do that can harm anyone. None of my friends has ever told me they suffered because of what I did"* - P17.

2) Alerts and Warnings: 11 participants gave positive reviews and satisfaction with security alerts as an important tool for them to know of any incidents. Examples of this included online accounts, Google and Facebook. *"I was once alerted that someone logged into my Gmail account in Brazil. I have never been to Brazil. So I followed what Google recommended and changed my password"* - P2. *"Facebook always tells me when I login to my account from any device. It tells me the device and location. So I know if someone hacks my account, I will know and change the password"* - P43.

On the other hand, 38 interviewees reported mixed views regarding security warnings. While some reported following security warnings and others not, some did both: *"When it says it is not a secure website, sometimes I don't visit. Even though other times I just ignore the warning and go ahead."* - P11; *"At work, malicious websites are blocked and we cannot access them. But when I am home, the browser just gives some warnings without blocking me which is good. So I think the risk here [at home] is not that serious compared to the risks at the work place because they have a lot of information and can be hacked. But sometimes I do follow some warnings at home that look a bit serious"* - P22.

3) Intuition: The analysis also pointed out that intuition is one of the ways through which 17 of our participants detect security incidents in the home. Without any evidence, the participants reported the ability to identify security incidents as they happen. *"We both had quick flash screens on our laptops. Since my husband and I were both involved in some political movement at that time, we were very confident that someone was capturing what we were doing on our laptops."* - P15. Similarly, *"I had a quick capture screen for like seconds. At that time I was involved in some political campaign for our area. So I knew that someone, especially the secret service were tracking me. I immediately shutdown my computer. And I later deactivated the email account I was using the time I had the screen captured."* - P10.

E. Managing Security Incidents in the Home

Three ways through which the participants manage security incidents emerged from the data. Of the 50 participants, 22 of our interviewees in the home reported having experienced security incidents before. The incidents included ransomware, loss of data, data corruption, loss of money from a bank account through unrecognised transactions, and unauthorised access to email/social networking/STEAM accounts among others. Incidents are managed in the following ways.

1) Act on Recommendation(s): Our participants reported acting on *recommendations from the technology* they use. For instance, to quarantine malware detected by an antivirus - the action itself recommended by the antivirus software. Another example is about the recommendation from a Google alert presented in section V-D2. Similarly, some participants reported being taking action(s) *recommended by individuals within a particular community (such as online fora) or a blog*. One participant reported: (*"I saw this problem for some time and I searched online for a good solution. Someone recommended a commercial adware remover, which I bought and it worked"* - P23). Overall 20 of the 22 victims acted on recommendations from different sources.

2) Report: We sought to know if the participants do report security incidents anywhere or to anyone, and for what purpose they do this. Our analysis revealed that reporting of security incidents was a common phenomenon in the home for two main reasons: 1) *to seek help* - according to 18 of the 22 victims, and 2) *to warn others* of the threat - according to 12 of the 22. In 6 cases were money was lost in a bank account or unrecognised transactions were charged to a credit card, reporting was done to a service provider seeking a refund. Interestingly, in the other 16 cases, reporting was done to family, friends, and work colleagues. Reasons for the choice of who to report to include trust, competence of the other stakeholder, availability, and cost when they are reporting to be helped, *"I have a friend who is good with computer, and I always go to him when I have a problem. He always helps."* - P5; and duty of care for others when reporting is done to warn

others of the threat, *"When I have a bad experience, I always try to advise my family and friends to avoid what I did"* - P3.

3) Do Nothing: Lastly, 2 participants felt helpless when they were faced with security incidents, and they did nothing. One participant said: *"All my pictures [on my laptop] could not open. There was a message saying my files were corrupt. I had hundreds of pictures, and they were all gone. I did not know what to do."* - P14; and the other reported: *"My computer shows a lot of ads when I want to browse the Internet. I have had them for some months now. I don't know how to remove them... I just have to live with them I guess."* - P17.

VI. Discussion

A. Security Technology

We have seen that most of the security-related technology in the home is for securing the endpoint. While technical endpoint protection measures are important, they do not provide comprehensive security on their own as evidenced by the proliferation of network attacks (e.g. [2], [4], [10], [22], [28], [30]). The home would also benefit from the approaches discussed in section III-A, if supported by appropriate technology.

The lack of—and need for—network monitoring tools in the home has long been recognised. As discussed in section II-B, most of the network security proposals are aimed at performing network monitoring. Similarly, US-CERT states in ST15-002 that: *"**Monitor for unknown device connections:** Use your router's management website to determine if any unauthorized devices have joined or attempted to join your network. If an unknown device is identified, a firewall or media access control (MAC) filtering rule can be applied on the router. For further information on how to apply these rules, see the literature provided by the manufacturer or the manufacturer's website."* As reported in section V-B2, ISPs perform traffic monitoring on inbound and outbound traffic for malware. This is a significant intervention, and would be well complemented with approaches that perform internal network monitoring for malware and other kinds of threats such as unauthorised access to devices and systems in the home.

Monitoring and managing a secure network is a cumbersome task to carry out. Organisations have automated tools that monitor and flag out incidents - successful or attempted. The lack of such solutions in the home has forced home users to depend on what they perceive to work best for them in detecting incidents. Relying on harm as a way of detecting incidents may have detrimental consequences. First, they might not be able to detect an attempted attack and so cannot take appropriate actions that could prevent its success. Another aspect to the lack of timely detection is the inability to mitigate an ongoing impact as it is happening. Second, they might not be able to detect incidents which are only visibly harming others: the December 2014 Lizard Squad attack on XBox Live and PlayStation networks, for instance, used home devices to attack third parties. Provision of tools that detect and communicate attempted or successful incidents would provide an early warning to home users, and would also provide evidence that regardless of their assessment of themselves as lacking in value (as discussed in section V-C2), they are still targets of attacks.

The reliance on intuition to detect incidents and attempts does not give an accurate representation of the issues, as reported in section V-D. Wrong assumptions might a) lead a home user to abandon a secure service or application for an insecure one, and/or b) cause stress on the stakeholder involved - as reported in section V-D for instance. The two security-related technologies that have some ground in detecting incidents and attempts are warnings and alerts. The success of security warnings, however, is very limited mostly due to a large number of false positives and the frequency of their use; as reported in our study and also extensively studied in [20].

Alerts on the other hand seem to perform better, as reported in section V-D2. We postulate that this might be due to their limited and occasional use, as applied in the cited scenarios of Facebook and Gmail. We believe such an approach could be leveraged in detecting and communicating network security incidents. Such a technology could work better if complemented with recommended actions (as reported in section V-E1 about the Gmail alerts), that are simple to perform for the home users, or are tailored to include the individuals who typically assist the home users (user-centric). Detecting administrative access and modifications to a network router, for instance, might help prevent potential serious threats. It could allow home users to act in time, either stopping an ongoing attack, or hardening their system so that an attempt could not materialise. In the case where an incident is successful, the ability to easily roll back any changes made to the configuration could help home users manage the incident in a timely and cost-effective way. However, more empirical work needs to be conducted to identify and understand the attributes that lead to success of the alerts, as in the cited scenarios.

B. Responsibility and Competence

Our findings highlight another issue: responsibility for home network security (e.g. in section V-B2 regarding ISP duty of care). Home users, ISPs, device manufacturers—and maybe even more—all share in the responsibility of securing the infrastructure in the home. The lack of a clear definition of responsibility boundaries creates ambiguity and leads to diffusion of responsibility, especially for the home user as reported in section V-B1. Attached to this problem is the issue of competence and security effectiveness. By its very nature, good network security requires competence and expertise, and a key problem is that this is not readily available to homes. The current situation is that ISPs that are technically competent to provide network security in the home are unwilling to take on the responsibility, device manufacturers and service providers generally constrain their efforts to their own devices and services and not the wider home network, and home users that do take responsibility face significant issues in competently resolving their network security needs (see section V-B).

This is a hard challenge to solve, and we propose three possible options that target the need for clear responsibility that is complemented by competence for securing home networks.

The first option is for ISPs and device manufacturers to slowly and appropriately transfer control of the network to home users. The proliferation of mobile apps, for example, has seen a lot of service providers offer a number of services and controls through apps (as reported in [19]). Embedding

security functionalities such as configuration management, network monitoring, and incident response tools within the other services could give home users more control over their environments and, with time, take on the responsibility of managing their security. While this might address the issue of responsibility, the question of competence and expertise of home users remains, but might be addressed through improvements in digital assistants, AI agents, and machine learning algorithms.

The second option is to build an infrastructure to offer security support to home users. While this could address both issues of responsibility and competence, it is a costly solution. Much of the success of such an approach might depend on economic factors, as it is not clear how much home users might be willing to pay (given that cost is a significant factor in security decision-making in the home), and whether other stakeholders could be willing to finance an infrastructure they do not directly benefit from (the main benefit of increasing the security of home networks is in the reduction of threats leveraging home networks to attack others—it is doubtful whether this is sufficient to attract investment from stakeholders who could benefit from this threat reduction).

Another way can be proposed inspired from a common theme in our data which can be categorised under the idea of *social cure*, where informal support workers play a key role in the digital well-being of their communities. Our findings are consistent with other work in this area, such as Dourish et al. [9], Besmer et al. [5], and Lipford et al. [21] who all point to the key role that *social navigation* and communities play in privacy and security work. Our data shows that some participants regularly rely on a trusted individual to treat their security problems (delegated security responsibility within the home environment), while others seek ad hoc help from wherever they can get it from within their social communities. This is an existing and available source of support, however the issue of competence and ability is less clear: informal support workers have 1) an uneven level of security expertise and ability to diagnose security problems; 2) difficulty in providing remote support, usually requiring them to be physically present when helping others; and 3) a genuine problem in procuring, configuring, and deploying security technologies that are tailored to protecting home networks beyond the traditional antivirus offering. On that note, it is interesting to note that a number of enterprise network security tools are made available to home users for free, but i) they are typically not tailored to home networks, and ii) the expertise needed to use them competently is typically lacking in homes, and iii) using them is not seen as necessary by home users (see Section V-B1).

Based on this assessment, our third proposal is therefore to leverage, provide additional resources to, and build competence in these existing informal support networks to target the gaps we have seen in Section V-B1. This might entail providing informal security workers with 1) tailored reference material to help them achieve good network security practice in the home (to help remediate the perception that network devices do not need security and provide a common baseline of good network security design), 2) appropriate and tailored tools to help apply good enterprise network security practices to the home (increasing the provision of assessment, monitoring, and response options), and 3) practical remote support options to help them perform their tasks conveniently, securely, and in a timely fashion (over and above the reported use of telephones). Because these networks of support are already in use, we believe that these steps will help the existing support workforce to bring about improvements in the quantity, quality, and timeliness of their security work. The end result could have a direct and pragmatic impact on the practical security posture of homes while remaining acceptable to the home user population and fitting in with their existing practices.

VII. Conclusions

Our work has revealed gaps between home network security and enterprise security best practice: *a focus on technical endpoint security in the home*, *a lack of tools for assessment, monitoring, and incident response in the home*, and *a fractured structure of security responsibility in the home*. We have also pointed to two potentially useful security-related practices in the home: *careful use of security alerts* and *advances in cheap, open source, and portable security technology.* Based on these findings, we put forward the following recommendations:

A. Prioritise security efforts and develop appropriate tools

While outsourcing security management for home networks may seem ideal (as proposed by a number of approaches in II-B), it comes with its own challenges: privacy concerns to the home user; scalability of such services ([11] discusses privacy and scalability challenges); cost to the service provider (as reported in section V-B2) and the home user (cost concerns regarding security for home users were reported by [27]); and the issue of false positives blocking a home user from accessing a legitimate service. We believe that prioritising efforts on critical points in the home network infrastructure, and developing appropriate tools to help home users with assessment, protection, monitoring, and incident response is a viable option.

B. Leverage the informal security support infrastructure

Providing targeted security support to home users is costly and complex (as reported in section V-B2), and informal support networks which already exist in the home environment could be targeted to empower them with appropriate resources to perform their tasks effectively and competently. Such networks would benefit from tools to diagnose vulnerabilities, monitor for incidents and attempts, and manage incidents network-wide. Such tools would also enable the support workers to remotely offer support.

As a means of improving the competence of informal support workers, an interesting idea would be to identify key members of social groups, target them with particular security interventions, and let the new behaviours cascade through the social networks organically.

Given the intrinsic and complex social aspects of these existing networks of support, we foresee significant challenges, e.g. better understanding the motivations behind giving and receiving support; mapping out the type and extent of different kinds of security work that individuals are willing to offer to others; or exploring the kind and extent of access individuals are willing to allow to people who they know socially, rather than professionals who are performing a contracted service.

ACKNOWLEDGMENT

This work was supported by the Research Institute in Science of Cyber Security (RISCS) under grant No. BLR01330, and grant No. BLR01790. Recruitment of participants was done in collaboration with the National Museum of Computing, and Community Centres in Oxford. Norbert is funded by the Rhodes Scholarship (Malawi & Linacre, 2015). We also thank the anonymous reviewers for their useful comments on this publication.

REFERENCES

[1] J. Allen, "Cert system and network security practices," in *Proceedings of the Fifth National Colloquium for Information Systems Security Education (NCISSE'01), George Mason University, Fairfax, VA USA*, 2001, pp. 22–24.

[2] F. Assolini. (2012) The tale of one thousand and one dsl modems. https://securelist.com/the-tale-of-one-thousand-and-one-dsl-modems/57776/. Kaspersky Lab. Online; accessed on 19-November-2017. [Online]. Available: https://securelist.com/the-tale-of-one-thousand-and-one-dsl-modems/57776/

[3] K. Aytes and T. Connolly, "Computer security and risky computing practices: A rational choice perspective," *Journal of Organizational and End User Computing (JOEUC)*, vol. 16, no. 3, pp. 22–40, 2004.

[4] BBC. (2016) Smart home devices used as weapons in website attack. BBC. Online; accessed on 03-April-2017. [Online]. Available: http://www.bbc.co.uk/news/technology-37738823

[5] A. Besmer, J. Watson, and H. R. Lipford, "The impact of social navigation on privacy policy configuration," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, ser. SOUPS '10. New York, NY, USA: ACM, 2010, pp. 7:1–7:10. [Online]. Available: http://doi.acm.org/10.1145/1837110.1837120

[6] J. E. Canavan, *Fundamentals of network security*. Artech House, 2001.

[7] J. M. Corbin and A. Strauss, "Grounded theory research: Procedures, canons, and evaluative criteria," *Qualitative sociology*, vol. 13, no. 1, pp. 3–21, 1990.

[8] T. Cruz, P. Simões, E. Monteiro, F. Bastos, and A. Laranjeira, "Co-operative security management for broadband network environments," *Security and Communication Networks*, vol. 8, no. 18, pp. 3953–3977, 2015.

[9] P. DiGioia and P. Dourish, "Social navigation as a model for usable security," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*, ser. SOUPS '05. New York, NY, USA: ACM, 2005, pp. 101–108. [Online]. Available: http://doi.acm.org/10.1145/1073001.1073011

[10] ENISA. (2016) "mirai" malware, attacks home routers. ENISA. Online; accessed on 03-April-2017. [Online]. Available: https://www.enisa.europa.eu/publications/info-notes/mirai-malware-attacks-home-routers

[11] N. Feamster, "Outsourcing home network security," in *Proceedings of the 2010 ACM SIGCOMM workshop on Home networks*. ACM, 2010, pp. 37–42.

[12] I. Flechais and M. A. Sasse, "Stakeholder involvement, motivation, responsibility, communication: How to design usable security in e-science," *International Journal of Human-Computer Studies*, vol. 67, no. 4, pp. 281–296, 2009.

[13] S. Furnell, P. Bryant, and A. D. Phippen, "Assessing the security perceptions of personal internet users," *Computers & Security*, vol. 26, no. 5, pp. 410–417, 2007.

[14] H. H. Gharakheili, J. Bass, L. Exton, and V. Sivaraman, "Personalizing the home network experience using cloud-based sdn," in *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on a*. IEEE, 2014, pp. 1–6.

[15] I. Hafeez, A. Y. Ding, L. Suomalainen, A. Kirichenko, and S. Tarkoma, "Securebox: Toward safer and smarter iot networks," in *Proceedings of the 2016 ACM Workshop on Cloud-Assisted Networking*. ACM, 2016, pp. 55–60.

[16] I. Hafeez, A. Y. Ding, and S. Tarkoma, "Securing edge networks with securebox," *arXiv preprint arXiv:1712.07740*, 2017.

[17] R. Kainda, I. Flechais, and A. Roscoe, "Security and usability: Analysis and evaluation," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on*. IEEE, 2010, pp. 275–282.

[18] E. Karamanos, "Investigation of home router security," 2010.

[19] E. Kim, J.-S. Lin, and Y. Sung, "To app or not to app: Engaging consumers via branded mobile apps," *Journal of Interactive Advertising*, vol. 13, no. 1, pp. 53–65, 2013.

[20] K. Krol, M. Moroz, and M. A. Sasse, "Don't work. can't work? why it's time to rethink security warnings," in *risk and security of internet and systems (CRiSIS), 2012 7th International conference on*. IEEE, 2012, pp. 1–8.

[21] H. R. Lipford and M. E. Zurko, "Someone to watch over me," in *Proceedings of the 2012 New Security Paradigms Workshop*, ser. NSPW '12. New York, NY, USA: ACM, 2012, pp. 67–76. [Online]. Available: http://doi.acm.org/10.1145/2413296.2413303

[22] P. Lunsford and M. C. Boahn, "How the lizard squad took down two of the biggest networks in the world," 2015.

[23] V. Martin, Q. Cao, and T. Benson, "Fending off iot-hunting attacks at home networks," in *Proceedings of the 2nd Workshop on Cloud-Assisted Networking*. ACM, 2017, pp. 67–72.

[24] M. S. Mendes, E. Furtado, G. Militao, and M. F. de Castro, "Hey, i have a problem in the system: Who can help me? an investigation of facebook users interaction when facing privacy problems," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2015, pp. 391–403.

[25] A. Müller, H. Kinkelin, S. K. Ghai, and G. Carle, "A secure service infrastructure for interconnecting future home networks based on dpws and xacml," in *Proceedings of the 2010 ACM SIGCOMM workshop on Home networks*. ACM, 2010, pp. 31–36.

[26] M. Niemietz and J. Schwenk, "Owning your home network: Router security revisited," *arXiv preprint arXiv:1506.04112*, 2015.

[27] N. Nthala and I. Flechais, ""if it's urgent or it is stopping me from doing something, then i might just go straight at it": A study into home data security decisions," in *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 2017, pp. 123–142.

[28] K. on Security. (2015) Lizard stresser runs on hacked home routers. Krebs on Security. Online; accessed on 19-November-2017. [Online]. Available: https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/

[29] B. P., F. S.M., and P. A.D., "Improving protection and security awareness among home users," *Advances in Networks, Computing and Communications 4*, 2008.

[30] M.-A. Russon. (2014) Two london ip addresses hijack over 300,000 home routers. Krebs on Security. Online; accessed on 19-November-2017. [Online]. Available: http://www.ibtimes.co.uk/two-london-ip-addresses-hijack-over-300000-computers-1438719

[31] I. L. Stats. (2017) Internet users. http://www.internetlivestats.com/internet-users/. Internet Live Stats. Online; accessed on 25-August-2017. [Online]. Available: http://www.internetlivestats.com/internet-users/

[32] M. Stawowski, "The principles of network security design," *ISSA Journal*, pp. 29–31, 2007.

[33] C. R. Taylor, C. A. Shue, and M. E. Najd, "Whole home proxies: Bringing enterprise-grade security to residential networks," in *Communications (ICC), 2016 IEEE International Conference on*. IEEE, 2016, pp. 1–6.

[34] K. Xu, F. Wang, R. Egli, A. Fives, R. Howell, and O. Mcintyre, "Object-oriented big data security analytics: A case study on home network traffic," in *International Conference on Wireless Algorithms, Systems, and Applications*. Springer, 2014, pp. 313–323.

[35] K. Xu, F. Wang, and X. Jia, "Secure the internet, one home at a time," *Security and Communication Networks*, vol. 9, no. 16, pp. 3821–3832, 2016.

[36] K. Xu, F. Wang, and M. Lee, "Hometps: Uncovering what is happening in home networks," in *Consumer Communications and Networking Conference (CCNC), 2012 IEEE*. IEEE, 2012, pp. 40–41.