Sharing Cloud Services: User Authentication for Social Enhancement of Home Networking

Slawomir Grzonkowski and Peter M. Corcoran, *Fellow,* IEEE

Abstract —*A user centric approach to authentication for home networks is proposed. A zero-knowledge-proof (ZKP) authentication is used to leverage the emerging cloud infrastructure allowing users to temporarily transfer their service and content rights within a trusted environment such as a friend's home. This approach enables the sharing of personalized content and more sophisticated network-based services over a conventional TCP/IP infrastructure. Experimental results derived from a reference prototype are presented. These demonstrate the practicality of the underlying approach. The potential to develop new cloud services for "social" home networks is also discussed* [1].

Index Terms — About four key words or phrases in order of importance, separated by commas.

I. INTRODUCTION

Historically research into home networking technologies has focused on the authentication of devices rather than their users. It is generally accepted that the home environment is relatively secure and services are typically tied to a fixed set-top-box (STB) or cable modem and thus there has been little motivation to implement user authentication for consumer electronic devices within the home.

Some consideration has been given by researchers to the use of Biometrics to enable user authentication [10]-[18]. Other researchers have looked at the use of RFID [26], trusted third party [29], or smart-card [32] technologies. However, the lack of a common interface mechanism to the home network implies that either additional components such as a biometric reader or RFID card would be required and the marginal benefits of *user-authentication*, over *device-authentication* have conspired to reinforce the status quo.

On the other hand, mobile computing applications and services have grown at an enormous rate in the last few years, fueled by a combination of emerging smart-phone technology, and the increasing bandwidth and ease of use of wireless mobile networks. The development of the "apps" market for smart-phones has served to accelerate the pace of innovation both in the capabilities of these devices and the range of services offered. Even more recently the development of the "tablet" market has added an additional dimension and a new mode of access to mobile services.

As users have grown more familiar with these mobile devices and services they have driven increasing demand for specialized content and improved services most of which are accessed directly from the Internet. Naturally it is possible to configure these new devices to function with a local network server and thus to employ them within the context of a home networking environment. In fact a state-of-art tablet device is arguably the "missing link" in terms of a UI device for the home networking environment. A similar interface device was envisaged nearly 20 years ago [33] but sadly never made it to commercial production.

A further development over the past 5 years or so has been the emergence of social networking on the Internet as witnessed by the success of iconic new Web services such as *Facebook*. Increased social interactivity on the Web has led users to expect to be able to customize and manage their own personalized environment and social networks. And a key element of such a personalized environment is the sharing of the online experience with friends, colleagues, community and family.

Given these varied developments it may be time to revisit the concept of a home networking environment and examine if some radical changes in our thinking on such environments is needed. While industry has struggled for many years to develop and implement a practical home networking environment the truth is that very little practical progress has been made since the early 1990's. At the same time many households have effectively established their own non-proprietary home networking environments, constructed around open Internet technologies, wireless access points and general-purpose broadband Internet connections. If we take the view that, in the absence of a viable and practical alternative, the Internet has effectively become the "home network" then perhaps the traditional home networking model of device authentication is already obsolete?

In any event the purpose of this paper is to examine how we can move beyond the traditional model of device authentication for home networks, and begin to implement a more user-centric approach. Simply put, how can I bring my *personal environment* with me when I visit a friend? How can I share my favorite online content, activities and experiences with other people *on their network* when I visit? In short, the home network experience must become mobile and the key to achieving this is to authenticate people, rather than devices.

We begin by considering the requirements of a user-centric authentication service that is linked to the user, rather than the device. A first step is a review of the literature and a range of

[1]The work presented in this paper was supported (in part) by the Lion project supported by Science Foundation Ireland under Grant No. RSF0840 and Enterprise Ireland under Grant No. REI 1005.

Peter Corcoran is with the College of Engineering & Informatics, National University of Ireland Galway (e-mail: peter.corcoran@nuigalway.ie).

Slawomir Grzonkowski is with the DERI research institute, National University of Ireland Galway (e-mail: slawomir.grzonkowski@deri.org).

Contributed Paper
Manuscript received 07/06/11
Current version published 09/19/11
Electronic version published 09/19/11.

related work in biometric authentication, wireless security, rights management and network sharing of digital content, peer-to-peer technologies, home networking middleware and home gateway systems. Following this review some usage modes are considered and key UI criteria are determined for a general-purpose home networking authentication mechanism. A prototype infrastructure is proposed and implemented, leveraging earlier work [34]-[36]. Finally, we present the results of some operational tests of our authentication system, with the client UI implemented on a state-of-art smart-phone.

II. RELATED WORK

A. Wireless & Mobile Authentication & Security

The authors of [25] describe a typical roaming scenario involving three parties: a roaming user, a foreign/visited server and a home server. The roaming user, who is a subscriber of the home server, is now in a network administered by the foreign server. In such situations it is desirable to enable the visitor to authenticate but to preserve anonymity. These authors identify five key properties that should be realized by the authentication process: (i) server authentication; (ii) subscription validation; (iii) key establishment with intermediary server; (iv) user anonymity; (v) user un-traceability. For our purposes properties (iv) and (v) are not generally required. The security protocol presented by these authors illustrates the potential complexity that may be required in such "third-party" systems. Fortunately we can simplify the protocol by using Zero Knowledge Proof (ZKP) techniques, as we shall see shortly.

In a later paper [31] these authors extend their work to provide protocols for two-party secure roaming system. This may provide either weak or strong anonymity, becoming more complex if strong anonymity is required. Revocation and billing schemes are included within the scope of this protocol. Note, however, that this is essentially device-level authentication and a user cannot establish and authenticate their credentials on a separate device. A similar problem for mobile networks is tackled in [27] but in this work the focus is primarily on use of efficient key exchanges to ensure that a mobile terminal is not exposed to eavesdropper or DoS attacks. The resulting protocol is also more efficient and some of the techniques employed in this work are closely related to our own, however this research is again directed to device authentication, rather than user-level authentication.

B. Other modes of Authentication for Home Networks

Building control networks are particularly vulnerable from a security perspective as, in contrast to mobile networks, they are designed for a closed community [28]. Similar arguments have applied to home networks, but as such networks link into cloud services more attention needs to be paid to enhanced authentication of users. Some researchers have looked at the use of RFID [26], trusted third party [29], or smart-card [32], [37] technologies. In [26] an RFID tag is used to identify and authenticate users to access a personalized and interactive IPTV service. This concept is very much in the spirit of how we feel home networks must evolve to meet emerging user needs. However it suffers the drawback of linking the user with a physical RFID card and in its present form requires the user to move within a relatively close distance of the TV in order to authenticate. In [30] the authors implement a mutual authentication protocol using nested one-time secret mechanisms. Such an approach could have value in the context of certain pre-paid network services, but again we find a relatively complex protocol making it less attractive for CE applications.

C. Biometric Authentication on Home Networks

A key drawback of the authentication protocols described in the previous section is that they all rely on the use of cryptographic keys generated within a specific device. Thus they represent device-level authentication. For mobile wireless services where each user is linked to the network via a unique device this is quite acceptable and even a desirable approach. However access to a home network could be over a range of devices, viz: smart-phone, tablet, laptop computer, remote control or wall-panel. But following today's rapid evolution in mobile and cloud services users now expect to gain access to their personal environment in a uniform manner and thus we need to authenticate the user rather than the device. One natural approach has been to use a biometric to perform authentication and a range of approaches can be found in the literature.

The concept of biometric access to a computer dates back to the 1960's had has periodically come back into fashion. In CE networks it was not considered cost-effective until the early 2000's and Rahman *et al* [38] were one of the first groups of researchers to envisage the use of biometric authentication within the home environment. Lin and Lai [12] described a flexible authentication scheme using a biometric smart-card to read fingerprints combined with a changeable user password. Khan and Zhang [17] subsequently refined this work. Hwang *et al* [11] considered issues relating to a portable, low-power biometric authenticator and how to partition the authentication between device and server. Today, with embedded facial analysis algorithms in our camera-phones and more sophisticated system-on-chip (SoC) technologies it is clear that device-level biometric authentication is feasible. Nevertheless other authors have remarked on the unreliable nature of acquiring a raw biometric [14], [15].

Several researchers have remarked on the potential to use biometrics for content or service encoding in addition to basic authentication [13], [14], [15] and [19]. In Corcoran *et al* [13] all digital media streams are encoded using keys derived from unique fingerprint features. Without the presence of an authenticated user the A/V content within a media stream will be corrupted, although the structure of the underlying MPEG stream remains intact. Face recognition is used to determine if the authenticated user continues to view the content and the display will eventually time-out if they leave the room. or turn away from the display.

D. State-of-Art in Home Networking

Integration of home networks with the Internet has been a topic of interest in Consumer Electronics since the mid-1990's [39]-[42]. In recent research Internet connectivity is assumed and the focus tends to be on home networking middleware which provides a range of local device-oriented services while also managing connectivity with the Internet [4], [6]-[8]. Some authors have also focused on the concept of an integrated UI that can combine the functionality of multiple devices into a single *metadevice* [5], [43], [44]. Such concepts were originally presented in [41]. Other authors have developed gateway devices that are extensible using a modular software framework such as OSGi [3], [20].

More recently the focus has shifted to consider how digital content can be managed within the home network and how sharing of digital assets and content, both within [13], [15], [16] and beyond the local network might be achieved [9], [10]. Recent trends indicate that consumers want improved access and availability of content. The success of centralized services such as iTunes™ suggests that each consumer will eventually "own" a personalized repository of content and Home Networking middleware should evolve with this in mind.

The authors of [45] point out the security challenges for home networks that typically rely on a shared physical medium (e.g. wireless 802.11, or AC power lines). This exposes the home user to significant security risks, and the use of link-level, network-level and peer-to-peer security mechanisms becomes even more important to prevent the exploitation of these vulnerabilities. These authors also present a de-centralized architecture, built on 802.11, Ethernet and TCP/IP networking that enables local and remote access to home networks using mobile devices such as smart-phones.

E. Peer-to-Peer and other emerging Technologies

Another important emerging field of technology is that of peer-to-peer and social networking. One aspect of such networks is their ability to share and distribute content across a distributed group of clients using specialized protocols such as *bittorrent*. This enables new approaches to the sharing and distribution of multimedia content between home networks [22], [23] and can be modified to provide a novel method of managing "long-tail" content as a *virtual IPTV* service, where there is no centralized repository [21].

Peer-to-peer networking creates a relational framework on top of the existing TCP/IP infrastructure of the Internet. In addition to the ability to exchange raw data, it is also possible to build higher-level functionality on top of such networks. Most people are now aware of the rapid development of peer-to-peer social networks and popular applications based on these networks such as Facebook™. Interestingly the concept of social networks extends back before their introduction on the Internet [1]. Mirroring the characteristics of *human* social networks the concepts of *reputation* and *trust* have been rediscovered in online communities [24] and form the basis for many emerging *social-networking* technologies and next-generation computer applications. An example of these technologies is D-FOAF [57], [58]. It provided a distributed trust component for using social networks as data sources.

III. User Authentication and Social Home Network

The typical use case envisaged is when someone visits the household of a friend or neighbor. The visitor may have personalized content or be subscribed to network services, which they wish to share in a social context. For example, a user might wish to share some family videos or perhaps they own a premium subscription to a "new release" movie service that allows temporary sharing of content when visiting friends or family (see Figure 1).

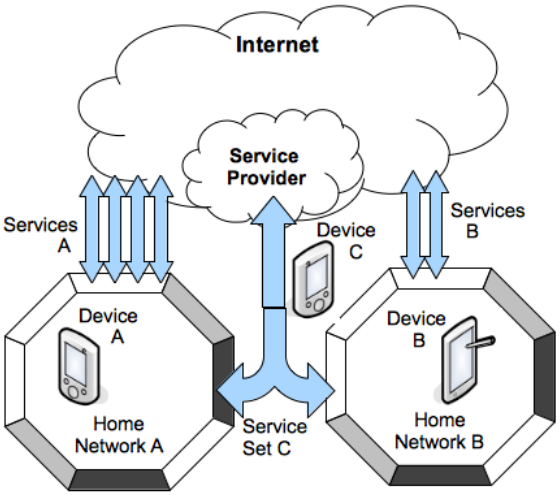

Figure 1: Device based authentication

As we identified in Section II, there are numerous limitations in the state of the art solutions that prevents us from building a secure and socially enhanced home networking infrastructure (see Figure 2). We list requirements for a protocol that would provide a solution applicable for home networks:

- Provide support for personalized environment
- Provide secure authentication
- Avoid overly complex protocols
- Facilitate both user-level and device-level authentication
- Avoid physical tokens
- Provide improved access and availability of the content

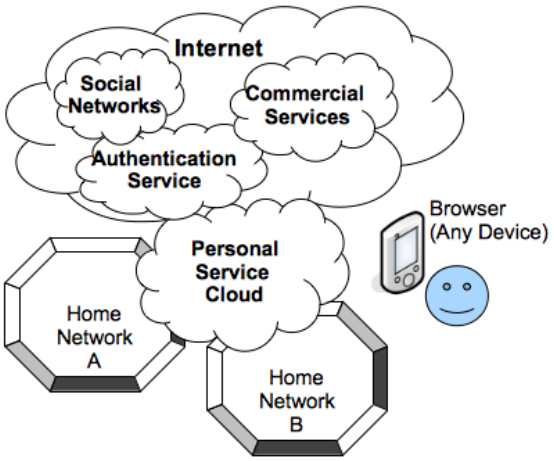

Figure 2: Device independent authentication

In addition to this list, we propose the following requirements that are derived from our previous work:

- Decentralized ad-hoc architecture: users should be able to create secure home networks of devices in a convenient manner
- The protocol should use existing infrastructure, such as the Internet, to take the full advantage of user's data
- High usability for the users, such as the support of memorable passwords and a convenient way of creating home networks
- The presence of any third parties should not influence the user's privacy

IV. User-Authentication Approach

Our previous work includes design and implementation of an efficient and secure infrastructure for micropayments in Massively Multiplayer Online Role-playing Games (MMORPG) [36]. That infrastructure was especially suitable for mobile devices. Taking into account this experience and our work in the area of Zero Knowledge Proof (ZKP) protocols [34], we designed a solution that addresses the requirements listed in Section III. Our proposal belongs to the family of trusted third-party protocols

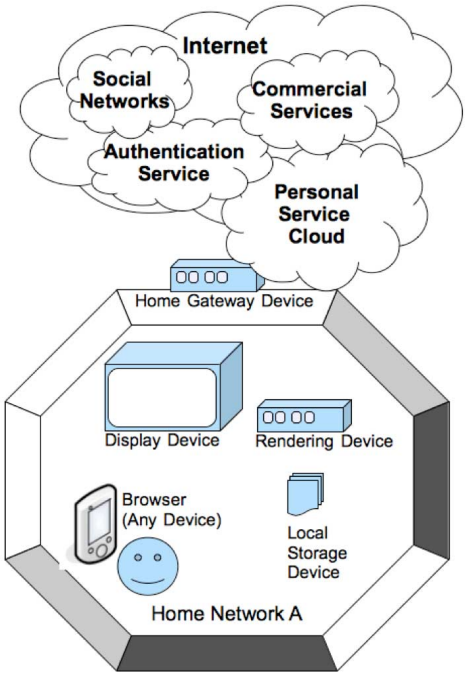

Figure 3: Home network and its component devices; ideally a smart-gateway will understand device capabilities [43], [44].

The proposed protocol has the following participants (see Figure 3):

- **Users:** they are the owners of personalized content and services, typically kept in the cloud. In a home network environment, their content & services can be accessed from the home network they successfully authenticate.
- **Home Gateway Devices:** they act as network gateways that a home network is equipped with. They provide access to user-owned services present in the cloud.
- **User's Services:** A number of services deployed in the user's personal cloud. These include authentication; social networks; commercial services such as IPTV, 3D-TV, VOD; and other personalized services.
- **Other devices:** these devices enable a user to take advantage of cloud services. Typically they will be a combination of display, storage, and rendering capabilities. A simple example is a modern smartphone.

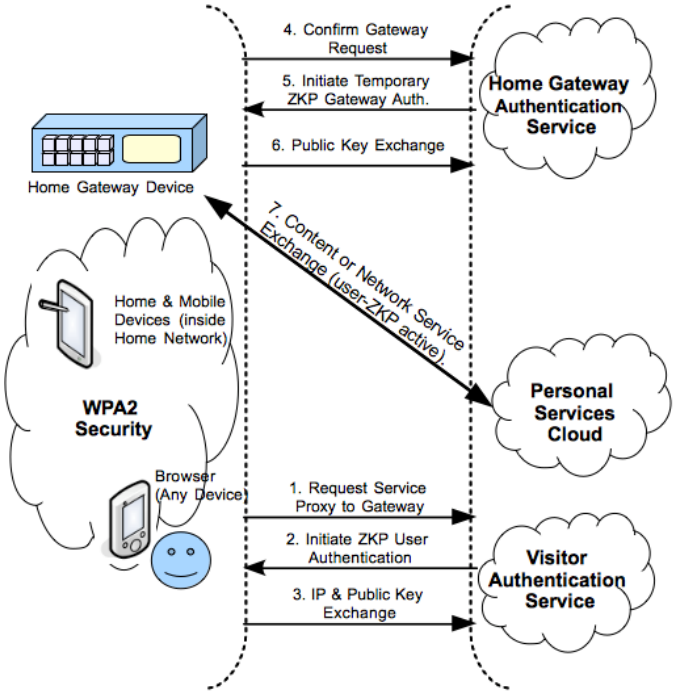

Figure 4: Authentication infrastructure

The generic protocol in which a user, say *Alice*, visits her friend *Bob* consists of five steps:

- **Request Service Proxy to Gateway:** *Alice* who is outside her home network, requests access to her personalized cloud services. Thus, she connects to Bob*'s* home gateway device to authenticate to her cloud services.
- **Initialize ZKP User Authentication:** *Alice* is requested to authenticate. For the requirement of increased security, the process is conduced using zero-knowledge proof-based protocols. Thus the service requires her public key and a proof that she has the knowledge of the corresponding private key.
- **IP and Public Key Exchange:** To proceed, the authentication service requires her login and her cloud address to regenerate her public key and profile. After this procedure, her home gateway authentication service locates her IP address within Bob's home network. Then, after successful authentication it is possible for the gateway to classify *Bob's* home gateway device and its associated local network as trusted.

- **Confirm Gateway Request:** In this step, *Bob's* home gateway is already recognized as trusted by *Alice's* service cloud. Thus it can make direct requests to her services.
- **Initiate Temporary ZKP Gateway Authentication:** *Bob's* home gateway begins the process of establishing a temporary ZKP public key. Thus *Alice's* services can be accessed from *Bob's* network in a secure manner.
- **Public Key Exchange:** *Bob's* home gateway registers its temporary public key in *Alice's* service cloud.
- **Content or Network Service Exchange (user-ZKP active):** Once the trusted ZKP link between the gateway and service cloud is established, *Alice's* content and network services are accessible from *Bob's* home network.

Our approach is depicted in Figure 4. Further details are given in Section V. Note that our authentication is based on techniques which deliver an efficient infrastructure for a Zero-Knowledge Proof-based protocol [34].

A. Zero Knowledge Proof Authentication

Zero-knowledge proof (ZKP) protocols have been formalized by Goldwasser, Micali, and Rackoff [49] in 1985. They provide a challenge-response authentication, in which parties are required to prove the correctness of their secrets, without revealing these secrets. Such protocols can be constructed for any NP-set, provided that one-way functions exist [4]. The use of zero-knowledge proofs as a mean of proving identity was first proposed by Fiege et al. [50]. There are many modifications of ZKP protocols. For example Guillou and Quisquater [51] proposed how to lower the bandwidth and memory requirements; Schnorr [52] described an alternative that uses the discrete logarithm problem. Our implementation uses a protocol based on isomorphic graphs [35].

B. Authentication Protocol in a Home Network

In the presented home networking scenario, the users of a home gateway are located in a close proximity. Thus, they can physically see or hear each other. They can also immediately interrupt the ongoing communication; even if it is already approved and in progress.

We note that such a physical presence can be considered as a second authentication factor [59] that additionally strengthens the overall security of the proposed protocol. Thus from the security perspective, the main threat is the possibility of eavesdropping the actual device-to-device communication.

C. Limitations and Comparison with Other Approaches

The main limitation of our protocol is that both devices must be connected to the Internet and have external IP addresses. This requirement is, however, satisfied if 3G technology is used. We also note that our protocol does not require users to expose their privacy to any third parties or services. Our protocol uses the *home gateway authentication service*. It does not provide any data routing between two communicating parties as it has been proposed in other solutions [54].

Since commercially deployed applications often work in hostile environments, malicious users may try to perform some side-channels attacks such as timing attacks. To protect from them, implementers and designers should, for example, provide a secure cryptographic random numbers generator. We did not use such a generator in our prototype as we were working in a friendly environment. It is also necessary to ensure that the responses for both successful and unsuccessful authentication take exactly the same time. We provided this functionality in our reference implementation.

D. Testing & Verification

Our protocol is based on the graph isomorphism problem. Thus there is a need to store and generate graphs. Our prototype implementation (see Section 5) performs graph operations on matrices. To store a graph of size 32 we need 32 x 32 bits. Thus the number of possible distinct graphs is 2^{1024}. This number is important from the perspective of attacks based on the birthday paradox: if in a graph isomorphism-based protocol the prover sends the same graph twice, the verifier can recover the private key.

For RSA-based protocols the security of 1024 bits is still considered to be secure. However, it does not imply that a graph isomorphism-based protocol using 32 vertices also offer 1024 bits security in the meaning introduced by RSA. These are two fundamentally different approaches to the problem of authentication. In addition, there are solutions for finding graph isomorphism for some known graphs types, such as planar graphs [46], graphs of bounded genus [47], trees [48], strongly regular graphs [2] and others.

Some authors suggested that, for a similar problem of the subgraph isomorphism, a graph of 81 or more vertices cannot be mapped faster than in 100000 years with a software-based solution [53]. There are also claims that "*256 nodes provide security for more than 70000 years with current technology*" [56]. To protect from graphs of known types we recommend the use of cryptographically secure random numbers generators, e.g. embedded in hardware. To avoid other security risks, we suggest using larger graphs.

For home network applications it is clear that the level of security provided by ZKP techniques is more than adequate and can be easily scaled to provide additional levels of security, for example for financial transactions, if required.

V. Details of the Protocol

As we described in Section 3, the proposed protocol requires several steps to merge a user's, say *Alice*, personalized content into her friend's, say *Bob's*, home network:

- Alice is connected to Bob's *home gateway*. The gateway has access to the Internet. She wants to access her personalized content and services that are hosted in the cloud.
- She requests access to her cloud by sending an HTTP POST request to her *authentication service* that is accessible from *Bob's* home network. The message body contains her username and the location of her home network. This is sufficient for Bob's authentication service to obtain her public key and profile.

- Once the gateway has her public key, the proper authentication process begins in which Alice located at Bob's network authenticates to her home gateway. The protocol extends the HTTP specification [55] in a way that our ZKP protocol is used instead of HTTP Basic or Digest protocols [55]. However, the response codes are preserved: if her browser does not send credentials, the response code "*401 Unauthorized*" is returned. If the credentials are correct, the service responds with "*200 OK*" value. Otherwise, it responds with "*403 Forbidden*".
- Bob's home gateway expects "200 OK" response code to continue the process. After successful authentication, Bob's home gateway can locate her home network and proceed with the procedure of enabling her personalized content and services within his network.
- Bob's device generates its temporary ZKP public and private key pair. The public key is registered at Alice's authentication service. The credentials expire on the agreed terms, which can be defined as concurrent use, specified date, or the number of accesses, etc.
- Device to service authentication, which follows the initial registration, is based on our previous work in the context of ZKP authentication for mobile devices [34], [36].
- Alice's personalized content and services exchange starts after the successful device to device authentication. During this phase the devices starts the actual data exchange. The presence of the user-authentication service is no longer necessary for the transaction.

VI. Implementation and Evaluation

To enable portability between various devices, we built our prototype implementation in java. Our implementation was tested on one of the state of the art 3G devices.

Since the main bottleneck of this protocol is the device-to-device authentication that is based on a ZKP protocol, we focus our evaluation on this aspect. It is the most challenging part both in terms of computation and bandwidth. The applied ZKP protocol is based on graph isomorphism that we described in our earlier work [34], [36]. It requires two parties: a client and a server. In our protocol, devices act as both clients and servers for the device-to-device authentication. From the perspective of computations and data generations, the client application, which is in our case a browser executed at a user's device, is responsible for the following operations:

- Generating a private key, Pk, from the user password
- Generating a public key, Puk, from the private key
- Generating random data of size $(Pk)^2$ for the ZKP authentication
- Responding Server's challenge vector
- Checking server timeout
- Delaying responses to provide a correct implementation for concurrent environments

The server, which is in our case a home network gateway, is responsible for the following operations:

- Looking-up the user's public key
- Storing user's random data
- Generating a random vector of size (Pk) to match the user's random data
- Verifying the user's response
- Checking its clients timeouts

In comparison with classical authentication approaches, such as HTTP Basic and Digest, there is a requirement of additional computations for both parties. Table I depicts how the ratio of the computations that are conducted by the server and the client depends on the number of authentication challenges and the graph size. We observe that once we increase one of these parameters, the server needs proportionally more time to respond the client's request. However, as we see in Figure 5, the amount of data sent by the server, which is equal to data received by the client, is much smaller than the data sent by client.

TABLE I
Data Measurements

Graph size	Challenges	Sent [KB]	Received [KB]	Total [KB]
32	10	3.7	1.3	5.0
32	20	7.2	2.3	9.5
32	30	10.7	3.2	14.0
64	10	12.3	3.0	15.4
64	20	24.5	5.0	29.5
64	30	36.7	6.9	43.5
128	10	45.0	8.0	53.0
128	20	89.8	11.9	101.7
128	30	134.6	15.7	150.3
256	10	171.7	24.2	195.9
256	20	343.2	31.8	375.1
256	30	514.7	39.5	554.3

The number of bytes exchanged for various authentication parameters.

Figure 5 depicts the impact of the graph size and the number of challenges on the authentication times. It shows that together with the increase of the number of challenges, the time required for computations grows linearly. However, the increase of the size of the graph causes quadratic time increase for the same number of challenges (see Fig. 6).

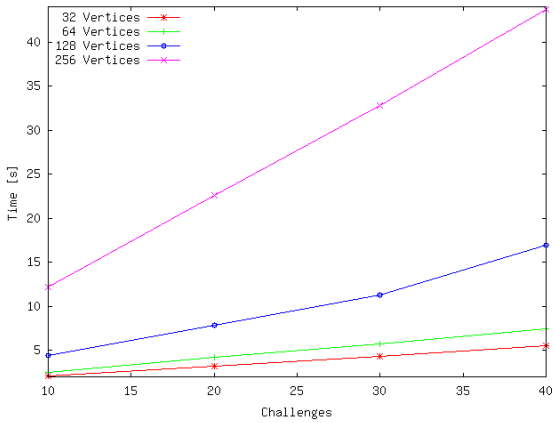

Figure 5: The authentication time for various parameters

We note that our previous work [36] demonstrated that the optimal number of challenges in terms of security and usability is in the range of 20-40. Thus we focus our analyses on this range.

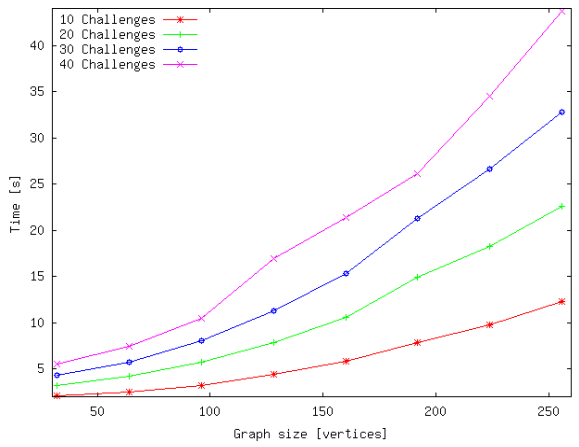

Figure 6: Relation between graph size and time in function of the number of challenges

Figure 7 summarizes the data exchange details. We observe that the amount of data exchanged between the client and the server grows linearly for a fixed graph size and the increasing number of challenges. Increasing the graph size has, however, polynomial impact on the number of data exchanged. This dependency is best described by $O(n^2)$. The quadratic dependency relates to the fact that the graphs are kept in matrices whose sizes are square function of their number of vertices. This property is important when customers of a given system are required to pay for bandwidth usage. In such a situation, the selection of this parameter would influence not only the system security properties but also the price of the service.

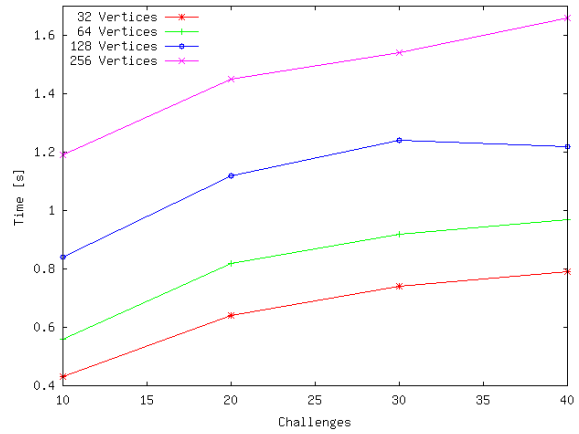

Figure 7: The distribution of computations between server and client; The data is calculated as the server computation time / client computation time.

VII. Conclusion and Future Work

An authentication framework for home networks is presented. A design for the essential authentication protocols using zero-knowledge proof (ZKP) techniques is given, allowing the use of a simple user/password authentication. Because the user/password never leaves the authenticating device this keeps a very high level of security and the risk of "cracking" the service is restricted to the "trusted" home environment.

Despite additional bandwidth and computational requirements it is shown that such an approach is feasible with acceptable authentication delays and using a range of today's CE smartphone devices. The proposed system provides user-centric authentication as any device with a Web browser can generate a login screen and implement the user/password hashing to regenerate the required key private/public keypair.

An additional advantage is that this service can be adjusted dynamically by increasing the number of authentication challenges generated from the server. In normal use it is sufficient to generate a smaller set of challenges every few minutes. For higher levels of authentication the response time for up to 30 consecutive challenges and using a graph of 128 vertices is still less than 15 seconds but provides a superior level of security to today's ecommerce solutions. For 10 consecutive challenges it is of the order of 4 seconds (Figure 5). Smaller graph sizes can be significantly faster (Figure 6).

One exciting aspect of such a security-architecture is the ability of users to share their services and content with others when making a social visit. This offers service providers scope to create new interactive services and applications that leverage the potential viral effect of "sharing" such services. In effect new services can self-market. If they are interesting and captivating enough to share with your friends and colleagues in the course of social and family visits then there is a strong likelihood they will consider registering for the full service.

For service providers there is no longer a need to create a restricted or limited-time trial service. And existing customers become your marketing team and greatest advocates. As "social sharing" only requires a user/password combination and a Web browser connected to the "cloud", you can effectively share anywhere and with anyone, assuming that their home network offers support for the appropriate display or rendering devices.

Naturally the greatest risk to any such system is at the human level. It has been assumed that high levels of trust exist when services are shared. But there are risks that a friend or neighbor may decide to abuse the trust shown to them and effectively hi-jack a user's services and personalized content. In this paper we have not directly considered the potential for such service hi-jacking and associated preventative measures. From the perspective of a service provider there are straightforward session management mechanisms for ensuring that only a single real-time access to a cloud service is available to a registered user and these could be readily adapted to address such issues [60]. However this lies outside the scope of the current work and we prefer to leave a detailed consideration of such issues for now.

Again we recall that the purpose of this paper is to examine how we can move beyond the traditional model of device authentication for home networks, and begin to implement a more user-centric approach in line with current trends in mobile network services. It is shown that ZKP techniques combined with cloud computing services can offer a suitable and practical approach to this problem.

REFERENCES

[1] S. Milgram. The small world problem. Psychology Today, pages 60-67, May 1967.

[2] D. A. Spielman. Faster isomorphism testing of strongly regular graphs. In STOC'96: Proceedings of the twenty-eighth annual ACM symposium on Theory of computing, pages 576-584, New York, NY, USA, 1996. ACM Press.

[3] D. O. Kang, K. Kang, S. Choi, J. Lee. 2005. UPnP AV architectural multimedia system with a home gateway powered by the OSGi platform. IEEE Transactions on Consumer Electronics, Vol. 51, No. 1, pp. 87-93, February 2005.

[4] Dong-Sung Kim; Jae-Min Lee; Wook Hyun Kwon; In Kwan Yuh; , "Design and implementation of home network systems using UPnP middleware for networked appliances," *IEEE Trans. Consumer Electron.,* vol. 48, no.4, pp. 963- 972, Nov 2002.

[5] P.M. Corcoran, J. Desbonnet, P. Bigioi, I. Lupu, "Home network infrastructure for handheld/wearable appliances," *Consumer Electronics, IEEE Transactions on* , vol.48, no.3, pp. 490- 495, Aug 2002.

[6] P. Dobrev, D. Famolari, C. Kurzke, B.A. Miller, "Device and service discovery in home networks with OSGi," *Communications Magazine, IEEE* , vol.40, no.8, pp. 86- 92, Aug 2002.

[7] Dong-Oh Kang; Kyuchang Kang; Sung-Gi Choi; Jeunwoo Lee, "UPnP AV architectural multimedia system with a home gateway powered by the OSGi platform," *Consumer Electronics, 2005. ICCE. 2005 Digest of Technical Papers. International Conference on* , vol., no., pp. 405- 406, 8-12 Jan. 2005.

[8] J. Wu, L. Huang, D. Wang, and F. Shen, "R-OSGi-based architecture of distributed smart home system." *IEEE Transactions on Consumer Electronics*, vol. *54*, no.3, pp.1166-1172, Aug 2008.

[9] Hyun Yong Lee; Jong Won Kim; , "An approach for content sharing among UPnP devices in different home networks," *IEEE Trans. Consumer Electron.,* vol. 53, no.4, pp.1419-1426, Nov. 2007

[10] E. Kawamoto, K. Kadowaki, T. Koita, K. Sato, "Content sharing among UPnP gateways on unstructured p2p network using dynamic overlay topology optimization," *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE* , vol., no., pp.1-5, 10-13 Jan. 2009.

[11] D.D. Hwang, I. Verbauwhede, "Design of portable biometric authenticators - energy, performance, and security tradeoffs," *Consumer Electronics, IEEE Transactions on* , vol.50, no.4, pp. 1222- 1231, Nov. 2004

[12] Chu-Hsing Lin, Yi-Yi Lai, "A flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, pp. 19-23, Volume 27, Issue 1, November 2004.

[13] P. Corcoran, C. Iancu, F. Callaly, A. Cucos," Biometric access control for digital media streams in home networks", *IEEE Trans. Consumer Electron.,* vol. 53, No. 3, pp. 917-925, August 2007.

[14] P. Corcoran, A. Cucos, T. Grossman, "Biometrically auditable public key infrastructure technology for secure multimedia content," *Consumer Electronics, ICCE. 2005 Digest of Technical Papers. International Conference on* , vol., no., pp. 33- 34, 8-12 Jan. 2005

[15] P. Corcoran, A. Cucos, "Techniques for securing multimedia content in consumer electronic appliances using biometric signatures", IEEE Transactions on Consumer Electronics, Vol. 51, No. 2, pp. 545-551, May 2005.

[16] F. Callaly, C. Cucu, A. Cucos, M. Leyden, P. Corcoran, "Real-time fingerprint analysis & authentication for embedded appliances". Paper presented at the Consumer Electronics, 2007. ICCE 2007. Digest of Technical Papers. International Conference on.

[17] Muhammad Khurram Khan, Jiashu Zhang, "Improving the security of `a flexible biometrics remote user authentication scheme", Computer Standards & Interfaces, Volume 29, Issue 1, ADC Modelling and Testing, January 2007, Pages 82-85

[18] C. Cucu, A. Cucos, P. Corcoran, "Determining unique fingerprint features for biometric encoding of data," *Consumer Electronics, 2008. ICCE 2008. Digest of Technical Papers. International Conference on* , vol., no., pp.1-2, 9-13 Jan. 2008

[19] Pei-Chen Tseng; Jing-Wein Wang; Wen-Shyang Hwang; , "Securing traffic at QoS-aware residential gateway using biometric signatures," *Consumer Electronics, IEEE Transactions on* , vol.54, no.3, pp.1148-1156, August 2008

[20] W.K. Edwards, M.W. Newman, T.F. Smith, J. Sedivy, S. Izadi, "An extensible set-top box platform for home media applications," *IEEE Trans. Consumer Electron.,* vol. 51, no.4, pp. 1175- 1181, Nov. 2005.

[21] F. Callaly, P. Corcoran, "Architecture of a PVR appliance with 'long-tail' Internet-TV capabilities," *IEEE Trans. Consumer Electron.,* vol. 52, no.2, pp. 454- 459, May 2006.

[22] Jung-Tae Kim, Yeon-Joo Oh, Hoon-Ki Lee, Eui-Hyun Paik, Kwang-Roh Park, "Implementation of the DLNA proxy system for sharing home media contents", *IEEE Trans. Consumer Electron.,* vol. 53, No. 1, pp. 139-144, Feb 2007.

[23] Chin-Feng Lai; Yueh-Min Huang; Han-Chieh Chao, "DLNA-based multimedia sharing system for OSGI framework with extension to p2p network," *IEEE Systems Journal*, vol.4, no.2, pp.262-270, June 2010.

[24] Li Xiong; Ling Liu; , "PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. on Knowledge and Data Engineering*, vol.16, no.7, pp. 843- 857, July 2004

[25] Guomin Yang, Duncan S. Wong, Xiaotie Deng: Anonymous and authenticated key exchange for roaming networks. *IEEE Transactions on Wireless Communications* Vol 6 no.9: 3461-3472, September 2007

[26] H. Jabbar, Jeong Taikyeong; Hwang Jun; Park Gyungleen, "Viewer identification and authentication in IPTV using RFID technique," *Consumer Electronics, IEEE Transactions on* , vol.54, no.1, pp.105-109, February 2008

[27] C. Tang, " An efficient mobile authentication scheme for wireless networks" *IEEE Transactions on Wireless Communications*, vol.7, no.4, pp.1408-1416, April 2008

[28] W. Granzer, F. Praus, W. Kastner, "Security in building automation systems," *Industrial Electronics, IEEE Transactions on* , vol.57, no.11, pp.3622-3630, Nov. 2010

[29] Jung-Shian Li; Chuan-Kai Kao; Shiou-Jing Lin; , "A Kerberos-based single sign-on system for VoIP SIP servers and clients with a terminal mobility capability,"*Computer Communication Control and Automation (3CA), 2010 International Symposium on* , vol.2, no., pp.75-80, 5-7 May 2010

[30] Chun-I Fan; Pei-Hsiu Ho; Ruei-Hau Hsu, "Provably secure nested one-time secret mechanisms for fast mutual Authentication and key exchange in mobile communications," *Networking, IEEE/ACM Transactions on* , vol.18, no.3, pp.996-1009, June 2010

[31] Guomin Yang; Qiong Huang; Duncan Wong; Xiaotie Deng, "Universal authentication protocols for anonymous wireless communications," *IEEE Transactions on Wireless Communications*, vol.9, no.1, pp.168-174, January 2010

[32] Binod Vaidya, Jong Hyuk Park, Sang-Soo Yeo, and Joel J. P. C. Rodrigues, "Robust one-time password authentication scheme using smart card for home network environment." *Comput. Commun.* 34, pp.326-336 3, March 2011.

[33] Y. Fujita, "Remote controller For cebus home system," Consumer Electronics, 1993. Digest of Technical Papers. ICCE, IEEE 1993 International Conference on , vol., no., pp.152-153, 8-10 Jun 1993

[34] S. Grzonkowski, "A privacy-enhanced usage control model", Ph.D. dissertation, Digital Enterprise Research Institute, National University of Ireland, Galway, 2010.

[35] S. Grzonkowski, W. Zaremba, M. Zaremba, B. McDaniel, "Extending web applications with a lightweight zero knowledge proof authentication". In CSTST'08: Proceedings of the 5th international conference on Softcomputing as transdisciplinary science and technology, pages 65-70, New York, NY, USA, 2008. ACM.

[36] S. Grzonkowski, P.M. Corcoran. A secure and efficient micropayment solution for online gaming. In Proceedings of the International IEEE Consumer Electronics Society's Games Innovations Conference 2009 (ICE-GIC 09), 2009.

[37] Li, C-T; Hwang, M-S; "An efficient biometrics-based remote user authentication scheme using smart cards.", *Journal of Network and Computer Applications* Vol 33 pp 1–5, 2010.

[38] M. Rahman, P. Bhattacharya, "Remote access and networked appliance control using biometrics features," *Consumer Electronics, IEEE Transactions on* , vol.49, no.2, pp. 348- 353, May 2003

[39] P.M. Corcoran, J. Desbonnet, K. Lusted, "CEBus network access via the world-wide-web," *Consumer Electronics, 1996. Digest of Technical Papers., International Conference on* , vol., no., pp.236, 5-7 Jun 1996.

[40] J. Desbonnet, P.M. Corcoran, "System architecture and implementation of a CEBus/Internet gateway ," *Consumer Electronics, IEEE Transactions on* , vol.43, no.4, pp.1057-1062, Nov 1997

[41] P.M. Corcoran, J. Desbonnet, "Browser-style interfaces to a home automation network," *Consumer Electronics, IEEE Transactions on* , vol.43, no.4, pp.1063-1069, Nov 1997.

[42] P.M. Corcoran, "Mapping home-network appliances to TCP/IP sockets using a three-tiered home gateway architecture," *Consumer Electronics, IEEE Transactions on* , vol.44, no.3, pp.729-736, Aug 1998

[43] P. Corcoran, A. Cucos, F. Callaly, "Home networking middleware infrastructure for improved audio/video appliance functionality and interoperability," *Computer as a Tool, 2005. EUROCON 2005.The International Conference on* , vol.2, no., pp.1316-1319, 21-24 Nov. 2005

[44] P. Corcoran, F. Callaly, "Rapid prototyping of networked A/V CE appliances," *Computer as a Tool, 2005. EUROCON 2005.The International Conference on* , vol.2, no., pp.1312-1315, 21-24 Nov. 2005

[45] M.J. Saaranen, D.N. Kalofonos, "Mobile device connectivity in home networks", Proceedings of the 2005 International Symposium on Wireless Personal Multimedia Communications, pp.179-186 (2005)

[46] J. Gil and Y. Zibin. Efficient algorithms for isomorphisms of simple types. Mathematical. Structures in Comp. Sci., vol. 15, no. 5, pages 917-957, 2005.

[47] I.S. Filotti and J.N. Mayer. A polynomial-time algorithm for determining the isomorphism of graphs of fixed genus. In STOC'80: Proceedings of the twelfth annual ACM symposium on Theory of computing, pages 236-243, New York, NY, USA, 1980. ACM Press.

[48] A.V. Aho, J.E. Hopcroft, J.D. Ullman. The design and analysis of computer algorithms. Addison-Wesley, 1974.

[49] S. Goldwasser, S. Micali, C. Rackoff. The knowledge complexity of interactive proof-systems. In STOC'85: Proceedings of the seventeenth annual ACM symposium on Theory of computing, pages 291-304, New York, NY, USA, 1985. ACM Press.

[50] U. Feige, A. Fiat, A. Shamir. Zero-knowledge proofs of identity. J. Cryptology, vol. 1, no. 2, pages 77-94, 1988.

[51] L. C. Guillou and J.-J. Quisquater. A practical zero-knowledge protocol fitted to security microprocessor minimizing both transmission and memory. In Lecture Notes in Computer Science on Advances in Cryptology-EUROCRYPT'88,pages123-128, New York, NY, USA, 1988. Springer-Verlag New York, Inc.

[52] C.P. Schnorr. Efficient identification and signatures for smart cards. In CRYPTO, pages 239-252, 1989.

[53] S. Ichikawa and S. Yamamoto, ,Data dependent circuit for subgraph isomorphism problem, in field-programmable logic and applications: reconfigurable Computing Is Going Mainstream, 2002, vol. 2438, pp.203-210.

[54] S. Grzonkowski, P.M. Corcoran: A Privacy-enabled Solution for Sharing Social Data in Ad-hoc Mobile Networks. In 29th International Conference on Consumer Electronics (ICCE), 2011

[55] R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach and T. Berners-Lee. "Hypertext transfer protocol, HTTP/1.1 (RFC 2616)", 1999.

[56] L. Szollosi, T. Marosits, G. Feher, and A. Recski, Fast digital signature algorithm based on subgraph isomorphism, in Proceedings of the 6th international conference on Cryptology and network security, ser. CANS'07, 2007, pp. 34-46.

[57] S.R. Kruk, S. Grzonkowski, A. Gzella, T. Woroniecki and H.C. Choi. D-FOAF: distributed identity management with access rights delegation. In Procedings of Asian Semantic Web Conference 2006, September 2006

[58] S. Grzonkowski, A. Gzella, S.R. Kruk, J.G. Breslin, T. Woroniecki, J. Dobrzanski. Sharing information across community portals with FOAFRealm. Int. J. Web Based Communities, vol. 5, no. 3, pages 351-370, 2009.

[59] B. Schneier. Two-factor authentication: too little, too late. Commun. ACM, vol. 48, no. 4, page 136, 2005.

[60] M. Jensen, J. Schwenk, N. Gruschka, L.L. Iacono, "On technical security issues in cloud computing," Cloud Computing, 2009. CLOUD '09. IEEE International Conference on , vol., no., pp.109-116, 21-25 Sept. 2009

BIOGRAPHIES

Slawomir Grzonkowski received his MSc in Computer Science from Gdansk University of Technology (Faculty of Electronics, Telecommunications and Informatics), Poland in 2006. He continued his studies at National University of Ireland, Galway in Digital Enterprise Research Institute (DERI) where he was awarded a PhD in 2010 for his work on Privacy-enhanced Usage Control Models. Currently he is the founding member of the Security, Privacy and Trust group in DERI. He also works for CISCO to enable semantic web in its products. He is an author/co-author of over 20 scientific articles related to the mentioned topics.

Peter Corcoran received the BAI (Electronic Engineering) and BA (Math's) degrees from Trinity College Dublin in 1984. He continued his studies at TCD and was awarded a Ph.D. in Electronic Engineering for research work in the field of Dielectric Liquids. In 1986 he was appointed to a lectureship in Electronic Engineering at NUI, Galway. He is currently vice-dean in the College of Engineering & Informatics at NUI, Galway. His research interests include embedded systems applications, home networking, digital imaging, pattern recognition, face & fingerprint biometrics, smart grid and wired and wireless networking technologies. He is author of more than 200 technical publications and co-inventor on more than 100 granted US patents. He is a Fellow of the IEEE.