Location Authentication through Power Line Communication:

Design, Protocol, and Analysis of a New Out-of-Band Strategy

Alan T. Sherman, Dhananjay Phatak, Bhushan Sonawane, Vivek G. Relan
Cyber Defense Lab, Department of CSEE
University of Maryland, Baltimore County (UMBC)
1000 Hilltop Circle, Baltimore, MD 21250
{ sherman, phatak, bhushan1, relan1 }@umbc.edu

***Abstract*—We propose using *Power Line Communication (PLC)* as a second channel for data origin authentication, and we present a system architecture and protocol for doing so taking advantage of existing infrastructure for communicating over power lines. Our system connects a user's computer to a secure electric meter in his building via a secure *Human Authorization Detector (HAD)*. The electric meter, which has a unique secret identifier and encryption key, communicates securely with the trusted *Power Grid Server (PG)* through PLC. Upon request from an Internet *Application Server (AS)*, the user sends a location certificate to the AS, obtained via PLC from the PG and signed by the PG. Because PLC requires physical access to the electric meter, our system offers fine-grain location authentication. Unlike movable modems and dongles, the meter is permanently attached to the user's building. The user authorizes or denies certificate requests and deliveries by reading the HAD's display and pushing a button on the HAD, thus protecting against the possible threat of malware on the user's computer maliciously requesting or forwarding location certificates unauthorized by the user. Our system provides strong location authentication useful to many on-line applications, such as banking and SCADA systems. PLC offers finer-grain location authentication than do cellular telephones. Furthermore, the power grid is deployed widely and is highly reliable, even in many places where cellular telephone and GPS signals are obstructed or unavailable. We present our architecture and *Power line Location Authentication Protocol (PLAP)* in sufficient detail to permit further implementation and analysis.**

Keywords-Applied cryptography, location authentication, man-in-the-middle attack, network security, out-of-band authentication, Power Line Communication (PLC), security engineering.

I. INTRODUCTION

To authenticate users of applications accessed over the Internet, strong strategies often require each user to pass multiple independent authentication challenges. Such challenges might involve knowledge of passwords, possession of physical tokens, biometrics, control of second channels, and proofs of physical location. For example, Authentify [1] sells an authentication service using telephone callback. For many applications, such a strategy meaningfully enhances authentication assurance by forcing the adversary to corrupt multiple independent systems. We propose using *Power Line Communication (PLC)* as a second channel, for location authentication.

As a bidirectional out-of-band authentication channel, PLC is attractive for several reasons. The power grid is highly reliable and widely available, including in many locations (*e.g.*, inside a building, in an underground or underwater facility, or in a remote area) where wireless communications or GPS signals are obstructed or unavailable. PLC can provide fine-grain location authentication, at the resolution of electric circuits serviced by a particular stationary meter. Such resolution is typically more accurate than that provided by cellular telephones. Although GPS signals can often yield highly accurate locations, when inside a tall building PLC can sometimes determine locations more accurately than can GPS. For some users, PLC is more convenient than communication over landline or cellular telephone: a user might not have a cellular telephone, and cellular telephones can be lost or stolen. Finally, PLC has relatively low cost for environments that already have power service, including both the fixed costs of adding PLC to a power grid and the marginal costs of adding additional users.

For many applications, location authentication meaningfully enhances security by providing evidence that the user is physically present within an authorized area. For example, an on-line banking service might require the user to be at home, or a SCADA or corporate system might require the user to be within the physical boundary of an enterprise. Attacking our system requires physical access to the electric meter for the user's building.

We propose a system architecture and protocol for using PLC as a second channel to authenticate users of Internet applications. The main components of our system comprise the *Application Server (AS), Power Grid Server (PG),* Power Grid Substation, user, user's computer, electric meter, and *Human Authorization Detector (HAD)*—with display and physical button—located in between the client's workstation and meter. The user obtains a location certificate from PG via PLC, which the user forwards to AS over the Internet. The HAD plays a crucial role in mitigating the threat of possible compromise of the user computer or home network: the user must push the button on the HAD to authorize any request for, and receipt of, any location certificate generated by our

Sherman is supported in part by the Department of Defense under IASP Grant H98230-09-1-0404.

978-1-4244-5010-7/10/$26.00 ©2010 IEEE 279

protocol. Our design takes into consideration the special characteristics of PLC, including low bandwidth and the hierarchical structure of the power line network involving meters, substations, and power grid server**.**

Our solution satisfies the following problem requirements. An active network adversary intercepting all Internet and power line communications, and even corrupting the user's computer, must not be able to forge, modify, or replay certificates without detection. Also, the adversary must be unable to learn any of the secrets stored on the meter, HAD, or power grid components.

To the best of our knowledge, we are the first to propose using PLC as an out-of-band channel for location authentication. Contributions of this paper include: (1) a system architecture for using PLC for location authentication, (2) a protocol—which we call *Power line Location Authentication Protocol (PLAP)*—for generating location certificates signed by the power grid server, and (3) a system design incorporating a HAD for protecting against possible *Man-in-the-Middle (MitM) attacks* between the meter and AS launched from a compromised user computer. Although we are not the first to design an out-of-band or location authentication system, we are the first to provide engineering details for doing so using PLC. Similarly, although the value (even necessity) of a HAD is known by some in the cryptographic folklore,[1] we are not aware of any publication providing design details, and we are not aware of any current authentication product that protects against such MitM attacks. Applying standard security engineering techniques to a new authentication channel, our system illustrates a useful application for the PLC network.

To demonstrate system feasibility, we provide architectural details specific to PLC. Our protocol, however, can be used with other authentication channels. Also, our design could be implemented (albeit less securely) without the HAD.

The rest of this paper is organized as follows. Section 2 reviews selected background and related work. Section 3 presents our system architecture, assumptions, and key management strategy. Section 4 explains Protocol PLAP. Section 5 discusses our threat model and security properties of PLAP. Section 6 discusses important design choices. Section 7 describes our demonstration implementation. Finally, Section 8 summarizes our conclusions. We assume the reader is familiar with the basics of applied cryptography, as presented by Anderson [2], for example.

II. Background and Related work

We briefly review selected previous work in multi-factor authentication and in PLC. To begin, we explain how our system relates to previous multi-factor authentication systems based on physical tokens, second channels, and location.

Using a clock synchronized with the application server, the RSA SecurID hardware token generates a new one-time password every 60 secs. to be entered by the user [3]. Dongles, such as ID2P Technologies' SafeIDKey and Yubico's YubiKey [4], generate cryptographic tokens to be sent by the user's computer to an Internet application. Unlike these three authentication systems, ours protects against compromise of the user computer with a human-in-the-loop strategy enforced by the HAD that binds transaction details to a location certificate. Also, unlike dongles, the electric meter is tied to a fixed location, which supports location authentication but works against mobile users.

Many Internet applications use email as a simple out-of-band authentication channel: after entering a username and password, the user also enters a use-once randomly generated string sent to the user's email account. The companies Authentify [1], StrikeForce [5], and PhoneFactor [6] perform a similar authentication service using telephony as the second channel. A variety of architectural choices are possible. With Authentify, one option is for the application to send the user's telephone number to the Authentify authentication service, which generates a random string and sends it both to the application and via telephone to the user, who then enters the string into the application. These products are vulnerable to a MitM attack carried out on a compromised user computer, and they do not bind a user to a location.

Several location authentication methods have been suggested using GPS, wireless, infrared, timing, or triangulation strategies. In 1998, Dennings and MacDoran [7] proposed using a trusted GPS receiver to sign a location certificate. In 1993, Brands and Chaum [8] described distance-bounding protocols based on roundtrip time between prover and verifier, though this approach is vulnerable to collaborative attacks [9]**.** Kindberg, Zhang, and Shankar [10] offered a different distance-bounding protocol, based on token broadcast, but their approach is subject to a token-forging proxy attack [9]. Capkun and Hubaux [11] combine distance-bounding and triangulation strategies. For additional methods, see Ferreres *et al.* [9]. Our approach provides fine-grain location authentication without depending on GPS reception.

First demonstrated in 1940 [12], communications over power lines are now used in many countries for *Automatic Meter Reading (AMR)*, SCADA system control, and Internet service [13]. Applications that use PLC must deal with a variety of challenges, including low network bandwidth [14], high signal attenuation and interference on low-voltage lines [14, 15], silent nodes [16], transformers which obstruct signals, and a hierarchical structure [17] comprising low-, medium-, and high-voltage lines. The REMPLI project [18] proposes a generic architecture for distributed data acquisition and remote control, which can support applications including AMR and SCADA. Broadband services follow a similar approach [19]. Treytl and Novak [20] designed a key management architecture for REMPLI. In these architectures, each home meter communicates over power lines with its substation, which communicates with the power grid server using a separate private network such as GPRS, 3G, WiMax, WiFi, HFC.

[1] Private correspondence with David Chaum.

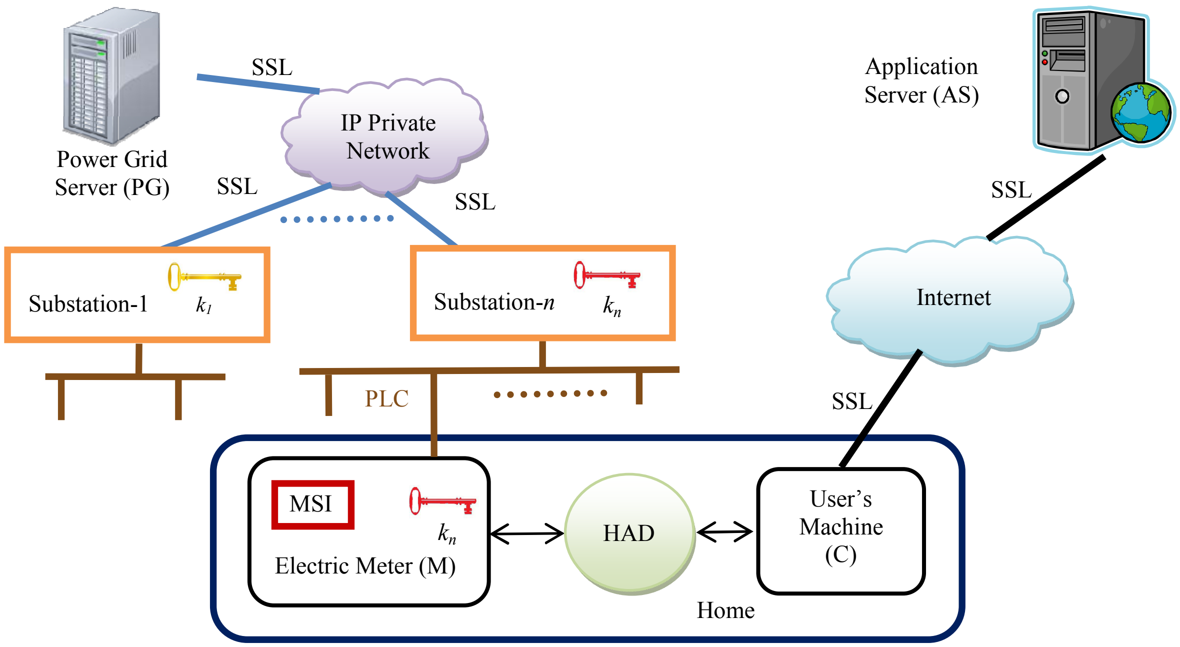

Figure 1: System architecture. Upon request of an *Application Server (AS)*, the user sends a location certificate to the AS, obtained via *Power Line Communication (PLC)* from the trusted *Power Grid Server (PG)*. The user authorizes or denies certificate requests and deliveries by pushing a button on a trusted *Human Authorization Detector (HAD)* residing between the user's computer and electric meter. Each meter has a secret *Meter Secret Identifier (MSI),* also known by its substation and the PG. Each meter shares a working key *k* with its substation.

III. System Architecture

Figure 1 summarizes our system architecture in terms of the players and hardware components. Upon request of an *Application Server (AS)*, via the Internet the user sends a location certificate to the AS. The user obtains the certificate via PLC from the trusted *Power Grid Server (PG)*, which signs the certificate. To enforce human authorization of certificate requests and deliveries, a trusted *Human Authorization Detector (HAD)* resides between the user's computer and the user's electric meter, securely connected by Ethernet, USB cables, and/or HomePlug communication.

We assume a hierarchical model for PLC in which a meter in each home communicates with its substation over low and/or medium voltage power lines. Each substation communicates with its meters on a shared bus, and each meter has a unique secret identifier. Typically, there are approximately 5000 meters per substation. Each substation performs asymmetric encryption and is connected to the PG perhaps through a private IP network, such as WiMax or GPRS. Each substation has a unique *SubStation Secret Identifier (SSSI)* known to all meters it controls.

The physically separate HAD has a digital display and physical button. It is a trusted bridge between the user's computer and meter. Using the button, the user accepts or denies requests for and deliveries of displayed location certificates. Transaction data are bound to the certificate, and these data are shown on the HAD display. The HAD also limits denial-of-service attacks from user computer to meter.

The electric meter is a trusted physically-secure device with limited computing resources. It has a unique public name and a private *Meter Secret Identifier (MSI)* also known by the substation and PG. Tamper-resistant hardware, such as a TPM, protects its MSI and cryptographic keys.

The PG is a trusted party which controls the PLAP subsystem, and the power company is a trusted party which controls all of the substations.

Following the REMPLI model, keys are managed primarily by the PG in three levels. Each meter shares a unique long-term *Key Management Key (KMK)* with PG. Similarly, each substation shares a unique long-term KMK with PG. These KMKs are provisioned at the factory. For each meter, PG establishes a unique *Management Key (MK),* which it shares with the substation and meter by encrypting it with the KMKs. Using the MK, a unique *working key* is established for each meter and shared with the substation and PG.

The PG communicates with the substations using SSL. The PG and each substation has its own public/private key pair, managed by a *Public Key Infrastructure (PKI)*. We assume the AS knows the public key of the PG.

IV. Protocol

Figure 2 summarizes the nine steps of our out-of-band *Power line Location Authentication Protocol (PLAP).* Upon request from the *Application Server (AS),* the user obtains and submits a location certificate signed by the *Power Grid Server (PG).* To mitigate the threat of a possible MitM attack

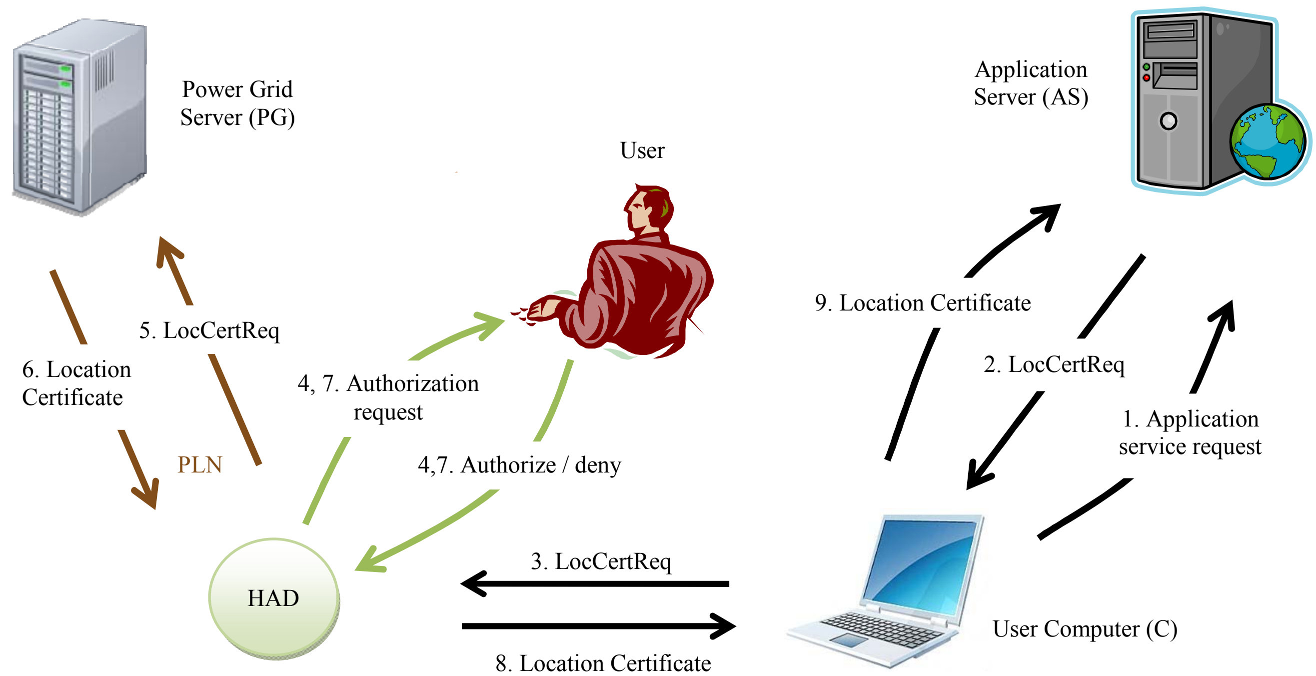

Figure 2: The nine steps of the *Power line Location Authentication Protocol (PLAP)*. Upon a *Location Certificate Request (LocCertReq)* from the *Application Server (AS),* the user obtains and submits a location certificate signed by the *Power Grid Server (PG)*. The user authorizes or denies certificate requests and deliveries by pushing a button on the *Human Authorization Detector (HAD)*. Messages 5 and 6 flow through the hierarchical *Power Line Network (PLN)***.**

emanating from a compromised user computer, the user authorizes or denies certificate requests and deliveries by pushing a button on the *Human Authorization Detector (HAD).* Messages between the HAD and PG flow through the hierarchical *Power Line Network (PLN*), which includes the user's meter and substation.

We now explain the main elements of PLAP, including its nine steps, the structure of the location certificate, and selected details. See our full paper for more details.

Our protocol uses a cryptographic hash function h, a *Hash-based Message Authentication Code (HMAC),* and an asymmetric cryptosystem. Let P_{PG} and S_{PG} denote, respectively, the public and secret keys of PG. Lifting this notation, for any string x, let $P_{PG}(x)$ and $S_{PG}(x)$ denote, respectively, the encryption of x under keys P_{PG} and S_{PG}.

Signed by the PG, a *Location Certificate (LocCert)* is constructed for a particular transaction between the user and the AS. It is given by

$$LocCert = (LocInfo, UID, ASID, h(D), TS, S_{PG}(h(LocInfo, UID, ASID, h(D), TS))), \qquad (1)$$

where LocInfo is the user location, UID is the user ID; ASID is the ID of AS; *D* is the transaction data (which also contains a unique identifier); and TS is the current time. Known as "limited civic location information," LocInfo is provided by PG for AS (from registration information), after PG verifies that the user's request originated from the user's meter. In the first line of (1), the hash function protects the privacy of *D*.

To verify a location certificate, AS checks the signature and recomputes the hashed values. In addition, AS verifies freshness of the timestamp and the appropriateness of LocInfo for the user. Assuming *h* is collision resistant, the certificate cannot be modified without detection.

To illustrate how PLAP works, we give selected details for an important part of Steps 5–6 in which the user *Meter (M)* and *SubStation (SS)* authenticate themselves to each other. We call this part the *Meter Authentication Protocol (MAP)*.

Mutual authentication between M and SS is accomplished through their mutual knowledge of the secrets MSI and SSSI. Our construction ensures that, without knowledge of MSI and SSSI, an adversary cannot forge, modify, or replay messages without detection.

We assume that at all elements of PLAP are implemented using standard best practices for cryptographic protocols, including mechanisms to prevent splicing and protocol interaction attacks. Also, all messages between M and SS are encrypted with the working key.

Protocol MAP works in three rounds:

(1) *M→SS: Mname, TS1, R1, HMAC(MSI, (Mname, TS1, R1))*

(2) *SS→M: Mname, TS2,*
HMAC(SSSI, (Mname, MSI, TS2, R1+1))

(3) *M→SS: Mname, Data, TS3, R2,*
HMAC(MSI, (Mname, Data, TS3, R2)),

where Mname is the public meter name, TS1, TS2, TS3 are current times, and R1 and R2 are random nonces. `Data' represents the location certificate request. At each round, the recipient verifies the correct computation of the HMAC'd values, the freshness of the time stamp, and the uniqueness and consistency of the nonce. The HMAC protects the privacy of MSI and SSSI, and it prevents undetected modification of the transmitted values. The HMAC functions like a hash function, but offer greater security against appending data attacks [21].

V. Security Arguments

The goals of an attacker include forging, modifying, or replaying certificates without detection; learning private information including the MSI and user application transactions details; and gaining unauthorized control of meter or substation.

We assume an active network adversary who can intercept all communications from the Internet and PLN, and who can gain complete control of the user's computer. The adversary might also control a neighbor's meter.

We assume the PG, substation, meter, and HAD are trustworthy, and in particular, they have sufficient physical protection. We also assume all of the standard cryptographic functions used are secure, including the hash function, HMAC, and symmetric and asymmetric encryption systems.

Modification of certificates or protocol messages would be detected because of the hash constructions. Timestamps and random nonces protect against replay attacks. In addition, all communications between meter and substation are encrypted with symmetric encryption. Communications between substation and PG, and between AS and the user's computer are protected by SSL. The user must manually authorize all certificate requests and deliveries via the HAD, which displays associated transaction and certificate data. The adversary cannot forge certificates, nor impersonate the meter or substation, without the MSI.

The MSI is physically protected on the meter, and it never appears as plaintext in any message. Whenever it does appear, it is hashed together with a random nonce and timestamp. Our design permits the substation and PG to impersonate meters. This limitation could be avoided with more powerful meters capable of asymmetric encryption.

Privacy of transaction details D are hidden from PG because the location certificate includes the hash of D rather than D.

We envision a flexible policy-driven system in which it is possible to release various forms of location information to the AS, depending in part on the type of transaction. The initial information is collected, and the policies are established, at registration. The LocInfo in the certificate might be a hash of plaintext location information.

Targets include the PG, substation, meters, and user computers. In particular, the security of the system depends critically on the secrecy of the MSI, which is known by the meter, substation, and PG.

VI. Discussion

The main advantages of our system are second-factor authentication by a separate channel, and location authentication tied to a stationary physically secure meter.

Importantly, our design includes a human-in-the-loop authorization, enforced by the HAD, and enabled by a location certificate structure that includes application transaction data. With traditional second-factor authentication (including typical dongles), malware on the user computer could execute a MitM attack in which the malware changes critical transaction data (*e.g.,* the destination account of a bank transfer). By contrast, in our system, the user would have an opportunity to notice such changes on the HAD's display, and the AS would notice any modified certificate. Although we are not aware of any product that incorporates a HAD, the idea has been well known in the electronic commerce folklore since the 1980s. It is an essential feature for authenticating transactions securely.

The location granularity of our approach is at the resolution of an electric meter. How this resolution compares with those of competing approaches depends on context. For many applications (*e.g.,* home banking), it is significant to know that a signal came from the user's home meter. By contrast, a GPS system might be unable to distinguish between signals emanating from within a house versus from immediately outside the house. Individual units in apartment buildings typically have separate meters. Although some meters might service large areas within large buildings, often it is significant to know that the signal emanated from within a corporate building.

A variety of communication paths are possible among the AS, user, and PG. For example, the AS could contact the PG directly. We chose our design to force all certificate requests and deliveries to pass through the HAD, to mitigate the threat of possible MitM malware on the user computer.

As with any strong security feature, there is a risk that the strong feature might deny service to intended uses. For example, the PLN might not be available after a hurricane. AS authentication policies must be carefully chosen.

Although we provide a design that is consistent with the constraints of power line networks, our architecture and protocol (including the HAD) are independent from the power line channel. Thus, in our protocol, the power line channel could be replaced with other second channels.

Challenges to implementation and adoption include the following. (1) The power company must be able to earn a profit (*e.g.,* through extra fees) for enabling this service. (2) New meters and substation upgrades will have to be installed. (3) Key management issues will have to be worked out, including the public-key infrastructure (perhaps provided by existing companies like Verisign). This situation is complicated by the existence of numerous different power companies (one approach would be to add a PG entity above many power companies). (4) The power company must be assured that the system does not unreasonably expose their meters to new potential vulnerabilities that could affect billing. (5) In buildings where many separate meters are located together (*e.g.,* in the basement), care must be taken to ensure a trusted communication path between the meter and HAD.

VII. Demonstration Software

To demonstrate our design, we implemented two simple applications using the HomePlug power line adapter [22] and software simulations of the meter, HAD, substation, and PG. In one application, banking customers negotiate and test authentication policies with a simulated bank, such as requiring power line authentication from home for any remote transaction over a specified limit. In another application, access to a simulated SCADA system requires location authentication from within an authorized area. Our software uses the SHA-256, RSA-2048, and AES-128 cryptographic algorithms, and an X.509-style format for location certificates, as supported by the Bouncy Castle cryptographic package [23]. We estimate our implementation of PLAP requires network bandwidth of about 0.35 Mbps, which is practical for PLC.

VIII. Conclusion

We have shown how to perform location authentication using the *Power Line Communication (PLC)* network and demonstrated our design with simple applications for banking and SCADA control. Other possible applications are a LoJack-like anti-theft device, home monitoring, and outgoing emergency calls. Our system enhances authentication assurance by forcing the adversary to compromise a separate channel, and doing so would require physical access to the user's electric meter. PLC is widely available and provides fine-grain location authentication tied to an electric meter physically secured to a known location, even in many places where cellular telephone and GPS signals are unavailable. Unlike many competing multi-factor authentication services, our approach protects against a compromised user computer through a human-in-the-loop confirmation. Our system could be introduced inexpensively as part of the next generation of substations and electric meters. This paper explores one useful security application for the emerging PLC network, whose intriguing potential remains largely untapped.

Acknowledgments

Phatak suggested the idea of using PLC for location authentication. We are grateful to Russ Fink, Yordan Kostov, and John Pinkston for helpful comments.

References

[1] Authentify Inc, "Out of band authentication employing existing infrastructure," [Online].
Available: http://www.authentify.com/collateral/OOBAwhitepaper.pdf, Last accessed Nov. 14, 2009.

[2] R.J. Anderson, *Security Engineering—A Guide to Building Dependable Distributed Systems*, Second Edition, New York : Wiley, 2001.

[3] RSA Security Inc, "The power behind RSA SecurID: Two-Factor user authentication: RSA ACE/Server,"
[Online] Available: http://www.opsec .com/solutions/partners/
downloads/rsa_securid_whitepaper.pdf, Last accessed Nov. 14, 2009.

[4] Yubico Inc, "YubiKey security evaluation," [Online] Available: http://yubico.com/files/Security_Evaluation_2009-09-09.pdf, Last accessed Nov. 14, 2009.

[5] Strikeforce Inc, "Specializing in preventing identity theft,"
[Online]. Available: http://www.sftnj.com/news/pdf/Phishing_malware_
spyware_prevention_by_StrikeForce.pdf, Last accessed Nov. 14, 2009.

[6] Phonefactor Inc, "Tokenless two-factor authentication: It finally adds up," [Online]. Available: http://www.phonefactor.com/wp-content/pdfs
/PhoneFactor-WhitePaper.pdf, Last accessed Nov. 14, 2009.

[7] D. Denning and P. MacDoran, "Location-Based authentication: Grounding cyberspace for better security," *Computer Fraud and Security. Elsevier*, February 1996.

[8] S. Brands and D. Chaum. 1994. "Distance-Bounding protocols," in *Advances in Cryptology—Eurocrypt '93*, T. Helleseth, Ed., Springer-Verlag, Berlin, 344–359.

[9] Gonzales-Tablas, Ana Isabel, Klaus Kursawe, Benjamin Ramos, and Arturo Ribagorda, "Survey on location authentication protocols and spatial-temporal attestation services," in *Embedded and Ubiquitous Computing: Proceedings of the EUC 2005 Workshops: UISW, NCUS, SecUbiq, USN, and TAUES, Nagasaki, Japan,* December 6–9, 2005. Berlin, Heidelberg, New York: Springer, 2005. 797–806.

[10] T. Kindberg, K. Zhang, and N. Shankar. 2002. "Context authentication Using Constrained Channels," in *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications*, June 2002.

[11] S. Capkun and J.-P. Hubaux, "Securing position and distance verification in wireless networks," *Swiss Federal Institute of Technology Lausanne*, Lausanne, Switzerland, Technical Report EPFL/IC/200443, May 2004.

[12] R. Broadbridge, "Power line modems and networks," in *2nd IEEE National Conference on Telecommunications*, April 1989.

[13] N. Pavlidou, Han Vinck, J. Yazdani, B. Honary, "Power line communications: State of the art and future trends," *IEEE Communications Magazine*, vol.41, no.4, pp. 34–40, April 2003.

[14] G. Bumiller, T. Sauter, G. Pratl, and A. Treytl, "Secure and reliable wide-area power-line communication for soft-real-time applications within REMPLI," in *9th International Symposium on Power Line Communications and Its Applications*, April 2005.

[15] J. Anatory, N.H. Mvungi, M.M Kissaka, "Trends in telecommunication services provision: Powerline network can provide alternative for access in developing countries," in *7th AFRICON Conference in Africa*, September 2004.

[16] J. Yu, P. Chong, P. So, and E. Gunawan, "Solutions for the 'silent node' problem in automatic meter reading system using powerline communications," in *7th International Power Engineering Conference*, Decmber 2005.

[17] F. Pacheco, M. Lobashov, M. Pinho, and G. Pratl, "A power line communication stack for metering, SCADA and large-scale domestic applications," in *9th International Symposium on Power Line Communications and Its Applications*, April 2005.

[18] A. Treytl, T. Sauter, G. Bumiller. "Real-time energy management over power-lines and Internet," in *Proceedings of the 8th International Symposium on Power-Line Communications and its Applications*, March 2004.

[19] "IEEE standard for broadband over power line hardware," in *IEEE STD 1675–2008*, Jan. 2009.

[20] A. Treytl and T. Novak, "Practical issues on key distribution in power line networks," in *10th IEEE Conference on Emerging Technologies and Factory Automation*, September 2005.

[21] Mihir Bellare, Ran Canetti, and Hugo Krawczyk, "Keying hash functions for message authentication," in *Advances in Cryptology – CRYPTO '96*, edited by Neal Koblitz, volume 1109 of Lecture Notes in Computer Science, pages 1–15. Springer-Verlag, Berlin, Germany, 1996.

[22] HomePlug Powerline Alliance, "HomePlug AV white paper," [Online]. Available: http://www.homeplug.org/products/whitepapers/HPAV-White-Paper_050818.pdf, Last accessed Nov. 14, 2009.

[23] Bouncy Castle Crypto APIs. [Online]. Available:
http://www.bouncycastle.org/java.html, Last accessed Nov. 14, 2009.