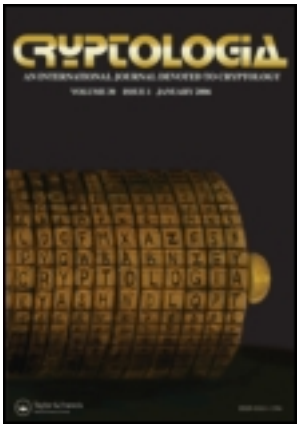

Cryptologia
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ucry20

Location Authentication, Tracking, and Emergency Signaling through Power Line Communication: Designs and Protocols for New Out-of-Band Strategies

Alan T. Sherman, Dhananjay Phatak, Vivek G. Relan & Bhushan Sonawane

Available online: 12 Apr 2012

To cite this article: Alan T. Sherman, Dhananjay Phatak, Vivek G. Relan & Bhushan Sonawane (2012): Location Authentication, Tracking, and Emergency Signaling through Power Line Communication: Designs and Protocols for New Out-of-Band Strategies, Cryptologia, 36:2, 129-148

To link to this article: http://dx.doi.org/10.1080/01611194.2012.660370

Cryptologia, 36:129–148, 2012

ISSN: 0161-1194 print
DOI: 10.1080/01611194.2012.660370

Taylor & Francis
Taylor & Francis Group

Location Authentication, Tracking, and Emergency Signaling through Power Line Communication: Designs and Protocols for New Out-of-Band Strategies

ALAN T. SHERMAN, DHANANJAY PHATAK, VIVEK G. RELAN, AND BHUSHAN SONAWANE

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 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 meter permanently attached to the building, our system offers fine-grain location authentication. The user authorizes certificate requests by reading the HAD's display including transaction details and pushing a button, thus mitigating the 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, including banking and SCADA systems. We present our architecture and protocols in sufficient detail to permit further implementation and analysis. We also outline applications for anti-theft and emergency signaling.

Keywords applied cryptography, anti-theft mechanism, human authorization detector (HAD), location authentication, man-in-the-middle attack, network security, out-of-band authentication, power line communication (PLC), security engineering

1. 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 [4] sells an authentication service using telephone callback. For many applications, such a strategy meaningfully enhances authentication

Address correspondence to Alan T. Sherman, Cyber Defense Lab, Department of CSEE, University of Maryland, Baltimore County (UMBC), 1000 Hilltop Circle, Baltimore, MD 21250, USA. E-mail: sherman@umbc.edu

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 marginal cost when added as part of changes to meters and other power grid components coming for the emerging smart grid.

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. Our system offers cryptographic evidence that the user has access to his home meter (but not necessarily that he is at home). 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. 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 system assumes the user has a secure electric meter at a known and fixed physical location. Although the meter plays a crucial role, it is less important how the PG communicates with the meter. In this sense, our system primarily exploits the "last hop" of PLC.

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 accept button on the HAD to authorize any request for, and receipt of, any location certificate generated by our protocol. Unlike competing approaches, the HAD displays transaction details and these details are cryptographically bound to the location certificate. 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, (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, and (4) related applications of PLC location authentication (not involving the HAD) for anti-theft mechanisms and emergency signaling.

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 useful applications 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 (for additional details, see Appendix). Section 5 discusses our threat model and security properties of PLAP. Section 6 discusses important design choices. Section 7 describes our demonstration implementation. Section 8 outlines two additional applications: anti-theft and emergency signaling mechanisms. Finally, Section 9 summarizes our conclusions. We assume the reader is familiar with the basics of applied cryptography, as presented by Anderson [3] for example.

2. Background and Related Work

This paper expands our related conference paper [36] by adding protocol details and anti-theft and emergency signaling applications. Phatak [29] filed patent applications on this invention.

We now 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. We also note recent work on the HAD and related technology.

Using a clock synchronized with the application server, the RSA SecurID hardware token generates a new one-time password every 60 sec. to be entered by the user [35]. Dongles, such as ID2P Technologies' SafeIDKey and Yubico's YubiKey [45], 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

[1]Private correspondence with David Chaum.

randomly generated string sent to the user's email account. The companies Authentify [4], StrikeForce [39], and PhoneFactor [31] 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. In another option, after the string is sent to the user via the Internet, Authentify calls the user who must speak the number into his phone. 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 [13] 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 [17]. Kindberg, Zhang, and Shankar [23] offered a different distance-bounding protocol, based on token broadcast, but their approach is subject to a token-forging proxy attack [17]. Capkun and Hubaux [12] combine distance-bounding and triangulation strategies. For additional methods, see Gonzales-Tablas et al. [17]. Our approach provides fine-grain location authentication without depending on GPS reception.

First demonstrated in 1940 [10], communications over power lines are now used in many countries for Automatic Meter Reading (AMR), SCADA system control, and Internet service [28]. Applications that use PLC must deal with a variety of challenges, including low network bandwidth [11], high signal attenuation and interference on low-voltage lines [11, 2], silent nodes [44], transformers which obstruct signals, and a hierarchical structure [26] comprising low-, medium-, and high-voltage lines. The REMPLI project [42] 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 [21]. Treytl and Novak [41] 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, and HFC.

The city of Manassas, Virginia demonstrated the feasibility of broadband PLC—also known as Broadband over the Power Line (BPL). Although the Manassas experiment was discontinued in 2010 largely due to income deficits,[2] other interesting PLC projects are underway, including in Brazil and China. Because our applications use low bandwidths, they will work both with broadband over powerline and with narrow band PLC technologies.

In 2010–2011, David Burns, Christopher Buswell, Matthew Duerr, and Christopher Watt designed, implemented, and tested a HAD for their capstone computer engineering project at UMBC.

Parno [27] addresses the MitM threat on commodity computers with a different approach from the HAD. In his approach, the user attests the environment of the user's computer with a trusted hand-held device. This device interrogates a Trusted Platform Module (TPM) on the computer to check that the correct software was loaded. This approach, however, does not bind transaction details to the human authorization and it does not provide location authentication. Given the imperfect

[2]http://www.eham.net/articles/23668.

nature of TPMs and trustworthy computing, we feel that our HAD offers a higher level of assurance against MitM attacks.

3. 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 5,000 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, located adjacent to the computer (perhaps attached to the monitor). It might be connected to the computer via a USB cable. Using the button, the user accepts or denies requests for and deliveries of displayed location

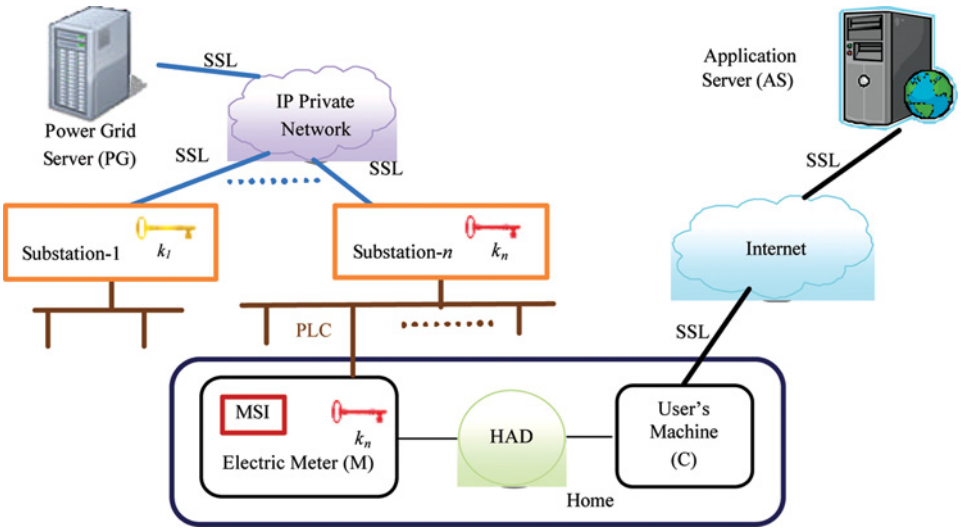

Figure 1. System architecture. Upon request of an Application Server (AS), the user sends a location certificate to the AS, obtained via Power Line Communication (PLC) from the trusted Power Grid Server (PG). The user authorizes or denies certificate requests and deliveries by pushing a button on a trusted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

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 HAD differs from existing authentication dongle products because it displays transaction details bound to the certificate. See the Appendix for more details.

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 meter is a vital element of the system that cannot be eliminated.

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.

4. 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),

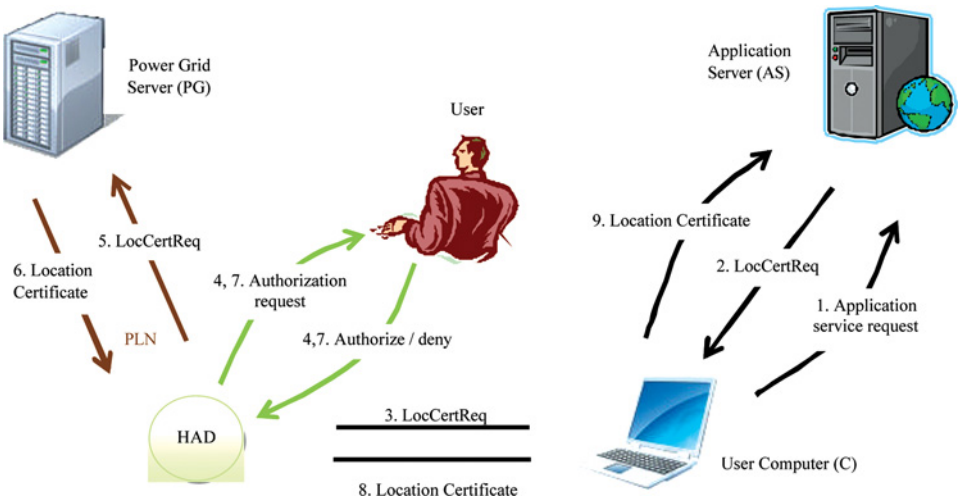

Figure 2. The nine steps of the Power line Location Authentication Protocol (PLAP). Upon a Location Certificate Request (LocCertReq) from the Application Server (AS), the user obtains and submits a location certificate signed by the Power Grid Server (PG). The user authorizes or denies certificate requests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

the user obtains and submits a location certificate signed by the Power Grid Server (PG). To mitigate the threat of a possible MitM attack 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 the Appendix for additional technical 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:

$$\text{LocCert} = (\text{LocInfo}, \text{UID}, \text{ASID}, h(D), \text{TS}, \text{S}_{PG}(h(\text{LocInfo}, \text{UID}, \text{ASID}, h(D), \text{TS}))), \tag{1}$$

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 (1) in the expression $h(D)$, 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 and 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 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.

Also, standard communications strategies are employed to address the harsh and noisy characteristics of PLC.

Protocol MAP works in three rounds:

1. M $\rightarrow$ (SS: Mname, TS1, R1, HMAC(MSI, (Mname, TS1, R1))
2. SS $\rightarrow$ (M: Mname, TS2, HMAC(SSSI, (Mname, MSI, TS2, R1 + 1))
3. M $\rightarrow$ (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 offers greater security against appending data attacks [6].

5. 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 the 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.

A corrupt user could transport one of his location certificates to another location and use it to complete the same authorized transaction from the new location, but we see no advantage to the user in doing so. Similarly, a corrupt user could network from a different location to his home meter, to pretend that he is home when he is not. Our system does not protect against this threat but rather provides evidence that the user has physical access to his electric meter. Thus, for example, our system can provide strong cryptographic evidence to a bank that a transaction is linked to the electric meter of an authorized customer, but this evidence should not be used by law enforcement to collaborate an alibi that the user was at home at a certain time.

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.

Any attacker who physically meddles with the meter or PLN must deal with the technology and dangers of power transmission. Although this fact does not constitute a strong security barrier, it does add to any such attack a special challenge not present in many digital systems.

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. A registration process collects initial information and establishes policies. The LocInfo in the certificate might be a hash of certain 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.

6. 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 HAD concept is most useful for transactions with short summary details, such as many banking transactions or SCADA commands. It is unlikely that most humans would be able to check lengthy transaction details accurately.

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. Alternatively, the PG could send two copies of the certificate: one to the user, and the other directly to the AS (the AS would check that they match). 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 users. 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) The PLC network must overcome any existing obstructions caused by transformers. (4) 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). (5) The power company must be assured that the system does not unreasonably expose their meters to new potential vulnerabilities that could affect billing. (6) 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.

7. Demonstration Software

To demonstrate our design, we implemented two simple applications using the HomePlug power line adapter [19] 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 [7]. In these toy demonstrations, power line communication took place over existing electrical wiring within our office building over a distance of a few dozen meters. We estimate our implementation of PLAP requires network bandwidth of about 0.35 Mbps, which is practical for PLC.

8. Additional Applications

Using similar models and techniques, we outline how PLC can also be used to locate stolen devices and to enhance emergency signaling. To the best of our knowledge, we are the first to propose anti-theft mechanisms based on PLC.

Locating Stolen Devices via Power Line Communication

We propose a new anti-theft mechanism for locating a stolen device by forcing the device to report its location whenever it is plugged into the power grid. A variation of this technology can disable the device whenever it fails to receive periodic status updates sent over PLC only to an authorized location, thus deterring theft. Our approach improves upon existing similar Internet-based anti-theft technologies by harnessing the fine-grain location authentication capability of PLC, while balancing legitimate privacy concerns.

Customers contract with a Device-Tracking Service, which operates a trusted Device Tracking Server (DT) that communicates with the trusted Power Grid Server (PG). Customers can report stolen devices to the DT. Each protected device includes special hardware to facilitate PLC over the hierarchical PLN. Each device has a Device Secret Identifier (DSI) protected in tamper resistant hardware (e.g., TPM). Whenever the device is plugged into the power grid, the special hardware initiates a PLC exchange with the PG, which creates, signs, and sends a location certificate to the DT showing the location and identity of the device. Based on this information,

the device status as reported by the customer, and prearranged policies, the DT takes appropriate actions, which might include notifying the customer and sending a command to the device to shut down.

Advantages of this approach include the fine-grain location authentication (at level of electric meter) made possible through PLC. Also, the PLN is widely available, and electronic devices need a source of power. Challenges include dealing with thieves who recharge batteries without plugging the device into the PLN (the aforementioned variation is one approach to this challenge).

Existing anti-theft mechanisms suffer from various limitations. Intel's anti-theft hardware approach [33] uses the Internet to locate stolen devices and Intel's DAR technology [38] to protect the confidentiality of data stored on the device. But Internet WiFi does not locate devices very precisely, and anonymous proxies and Tor [14] can hide IP addresses. Although GPS can provide precise locations, not all devices are GPS-enabled, and GPS signals are not always available (e.g., inside buildings).

Power Line Anti-Theft Mechanism (PATM)

Our Power Line Anti-Theft Mechanism (PATM) helps to locate stolen devices and to protect sensitive information on stolen devices. In this section, we describe our Power Line Anti-Theft Protocol (PATP), which helps locate and optionally disable stolen devices. To protect sensitive information on these devices, we use Intel's DAR technology [38].

Figure 3 depicts Protocol PATP in terms of its architecture and seven main steps. The main entities are the DT, PG, and protected Device (Dev). Each DT has a unique pubic Device Tracking Server Identifier (DTID). Each device has a

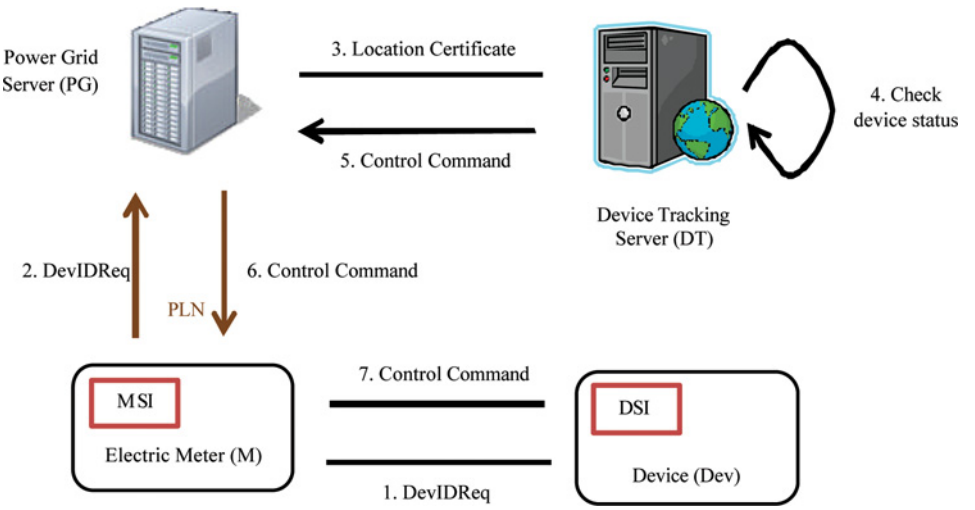

Figure 3. The seven steps of our Power line Anti-Theft Protocol (PATP) for locating and optionally disabling stolen devices. The Device (Dev) periodically sends a Device Identification Request (DevIDReq) to the Device Tracking Server (DT) through the PLN via the Power Grid Server (PG). For each DevIDReq, PG signs and sends a location certificate to DT. Based on the current status of Dev (e.g., is it reported stolen?) and established policies, DT sends a control command to Dev. (Color figure available online.).

unique Public Device ID (DevID) and DSI, issued by the PG during registration. A PLC power adaptor [22] enables the device to communicate over the PLN while it is plugged in (e.g., during recharging).

Although many policy variations are possible, PATP is built on the seven main steps shown in Figure 3. Using PLC, periodically the device sends a device identification request to DT through PLN via PG. As part of this communication, the electric meter executes the Meter Authentication Protocol (MAP) with its substation. PG creates, signs, and sends a location certificate to DT. This certificate contains the meter location, DevID, DTID, and current timestamp. DT keeps track of location certificates for registered devices. Based on current information and agreed upon anti-theft policies, DT sends an appropriate control command to the device through PLC. See the Appendix for protocol details.

We envision two primary policy choices. (1) The device operates normally *except* after receiving an authenticated disable command from DT. For example, after the owner reports to the DT that her device was stolen, the DT could issue a disable command upon receipt of an identity request from the device. A limitation of this policy is that a thief might be able to block the device from sending or receiving PLC signals. (2) The device operates normally *only when* it receives periodic status signals from the DT over PLC. Thus, if a thief blocks PLC signals, or connects the device to an unauthorized power source, the device could disable itself. A disadvantage of this policy is the possibility that a device shuts down even though it is not stolen due to a disruption of the PLN.

For either policy, the owner would have a way to reset the device after passing additional authentication challenges (e.g., based on keys and biometric information stored on a trusted platform module)—similarly to that of Intel's anti-theft approach [33].

Discussion of Anti-Theft Mechanism

Our anti-theft mechanism illustrates a way power companies could enhance the value of their services through the capabilities of the smart grid.

Costs of this solution include administrative costs (which amortize well over many customers) and required hardware and software support for PLC and key storage on each protected device.

Our mechanism can be used both for mobile devices (e.g., laptops) and fixed devices (e.g., flat screen televisions). Electric cars could be tracked as soon as they are plugged in for recharging, and expensive electronic devices could be disabled when they are unplugged from their authorized locations. The system can ensure that an electronic voting machine is turned on only at its designated precinct. The system can also create verifiable chains of custody of electrical equipment.

As with many secure applications, there is a tension between accountability and anonymity. In particular, the device owner would like to track her stolen device, but PATM should not reveal her location to untrustworthy entities. As noted by the Electronic Privacy Information Center [40], the smart grid creates many potential vulnerabilities to privacy. Pseudonyms (including the concept of spread identity [30]) can be used to hide the association between a device and its owner. And this association can be protected by a cryptographic key split among several DT trustees.

Previous Work on Anti-Theft Mechanisms

We now briefly review selected related anti-theft technologies, which aim to locate stolen devices and/or protect sensitive information on them. These goals are especially challenging to achieve when the adversary has physical possession of the device.

Lojack [24], GPS tracking [9], and Enfotrace [18] provide GPS-based anti-theft mechanisms in which a radio transceiver is secretly installed inside the device. If the thief can locate the transceiver, the thief can remove or disable it.

Prey [32], BackStopp [5], FailSafe [15], and GadgetTrak [16] provide device-tracking software to locate stolen devices based on IP address. The device periodically contacts a central inventory server (through Internet, WiFi, and/or GSM). Unfortunately, IP addresses can be obscured using anonymous proxies or Tor [14], and the thief can disable these products by reinstalling the operating system. The BIOS-based Computrace Lojack [1] is similar to these products but more difficult (yet not impossible [20]) to remove.

Remote Laptop Security (RLS) [34], Bitlocker [43], and Intel Centrino 2 with vPro [33, 38] use encryption and authentication to protect files on stolen computers. Unfortunately, the software-based RLS scheme and its authentication mechanisms can be bypassed through reinstalling the operating system and using password recovery software such as Ophcrack [25]. The hardware-grounded Bitlocker and Intel full disk encryption systems offer stronger protection. In RLS, the owner can issue disable commands remotely when the stolen device is connected to a central server. In the Intel system, a hardware system periodically checks in with a central monitoring server which can issue disable commands.

Power Line Monitoring and Emergency Signaling (PMES)

Exploiting the bidirectional nature of PLC, the smart grid can be used as platform for advanced services [37] including power monitoring, remote management of major appliances, and emergency signaling. Elements of Protocol PLAP can be used to authenticate the communications and to determine the building location assuredly. For example, the owner or a sensor could issue an emergency message to authorities over multiple communication channels including PLC. Conversely, officials could broadcast authenticated emergency warnings over the PLN, as the British did during World War II (without authentication by lowering the current frequency) for air raid warnings. Sending an emergency call over multiple channels increases assurance that the message will get through.

9. Conclusion

We have shown how to perform location authentication using the Power Line Communication (PLC) network and demonstrated our design with applications for banking and SCADA control. We also describe applications for a LoJack-like anti-theft device, home monitoring, and emergency signaling. 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 that binds transaction details to the confirmation. We enforce this confirmation via our Human Authorization Detector (HAD), which is of independent interest and could be combined with personal assistants and GPS location authentication devices.

Our system could be introduced with low marginal cost as part of the next generation of substations and electric meters. These changes are coming as part of the emerging smart grid, which will increase energy efficiency and support local microgeneration of power. This paper explores one class of useful security applications for the emerging PLC network, whose intriguing potential remains largely untapped.

Appendix

In this appendix we provide additional technical details for our out-of-band Power line Location Authentication Protocol (PLAP), our Human Authorization Detector (HAD), and our Power line Anti-Theft Protocol (PATP). In addition, we list acronyms and abbreviations used in the body of the paper.

For brevity and clarity we focus on the special elements of protocols PLAP and PATP, omitting certain standard details, such as mechanisms for preventing protocol interaction attacks and dealing with noisy channels. All communications between meter (M), substation (SS), and Power Grid Server (PG) are encrypted. We suggest that SS and PG maintain encrypted logs.

I. Protocol PLAP

We present Protocol PLAP in four parts: (i) communication between the user's Computer (C) and the Application Server (AS) over Internet, (ii) communication between C and PG over PLN to obtain a location certificate, (iii) human-in-the-loop authorization using HAD, and (iv) C relays location certificate to AS over Internet.

Communication between C and AS over Internet

1. C → AS: Request service
   User requests service from AS. The request is sent through a SSL tunnel, which is established between user's computer and application server for secure communication.
2. AS → C: Ask for location certificate
   If the situation requires it, AS asks user to authenticate his location.

Communication Between C and PG over PLN to Obtain Location Certificate

1. C → HAD: LocCertReq(UID, ASID, D)
   User requests a location certificate from PG via HAD for transaction data *D* with AS.
2. Human-in-loop test using HAD
   HAD displays transaction data *D* on the HAD and asks user to accept or deny the associated location certificate request by pressing the accept or deny button on the HAD. If user accepts, HAD saves data *D* for some time period for later display.

3. HAD → M: LocCertReq(UID, ASID, $h(D)$)
   If user accepts the location certificate request, HAD relays it to the electric meter, replacing the transaction data D with its hash $h(D)$. Sending $h(D)$ rather than D protects user privacy from PG and reduces the number of bits needed to be transmitted over the low bandwidth PLN.
4. M → SS: Mname, TS1, R1, HMAC(MSI, (Mname, TS1, R1))
   SS → M: Mname, TS2, HMAC(SSSI, (Mname, MSI, TS2, R1 + 1))
   M → SS: Mname, UID, ASID, $h(D)$, TS3, R2,
   HMAC(MSI, (Mname, UID, ASID, $h(D)$, TS3, R2))
   These three messages between meter and substation compose the Meter Authentication Protocol (MAP) explained in Section IV. All communications between M and SS are encrypted with symmetric encryption under the working key. It would be possible to augment MAP with additional mutual authentication checks by SS and PG of their power signatures.
5. SS → PG: Mname, UID, ASID, $h(D)$, TS4, R3,
   HMAC(MSI, (UID, ASID, $h(D)$, TS4, R3))
   After successful mutual authentication between meter and substation, substation establishes SSL tunnel with power grid server and relays the location certificate request from meter to PG.
6. PG processes location certificate request
   From Mname, PG looks up MSI and uses it to verify the HMAC construction. PG also verifies the timeliness of the time stamp. If these verifications succeed, then PG constructs the appropriate detail of LocInfo of user to include in the location certificate being created for AS.
7. PG → SS: LocInfo, UID, ASID, $h(D)$, TS5,
   S_{PG} (h(LocInfo, UID, ASID, $h(D)$, TS5))
   PG signs a location certificate, and PG sends it to substation through existing SSL tunnel. Here, S_{PG} denotes asymmetric encryption under PG's secret key.
8. SS → M: LocInfo, UID, ASID, $h(D)$, TS5, TS6,
   S_{PG} (h(LocInfo, UID, ASID, $h(D)$, TS5))
   Substation forwards location certificate to meter through PLN. All communications between SS and M are encrypted using the working key.
9. M → HAD: LocInfo, UID, ASID, $h(D)$, TS5, TS7,
   S_{PG} (h(LocInfo, UID, ASID, $h(D)$, TS5))
   Meter relays a location certificate to HAD.

Second Human-In-the-Loop Authorization Using HAD

Before displaying transaction details, HAD verifies consistency of $h(D)$ with its buffered data D; HAD verifies the location certificate using P_{PG}; and HAD verifies the freshness of the time stamps. If verification is successful, HAD displays D. If user accepts, HAD forwards the certificate to C.

C Relays Location Certificate to AS over Internet

1. C → AS: LocInfo, UID, ASID, $h(D)$, TS5,
   S_{PG} (h(LocInfo, UID, ASID, $h(D)$, TS5))
2. C relays the location certificate to AS through the pre-established SSL tunnel. Upon receipt, AS verifies the certificate using P_{PG}, the freshness of the timestamp, and all hashed values.

II. Protocol PATP

In Protocol PATP, a protected Device (Dev) periodically contacts its Device Tracking Server (DT) via the Power Grid Server (PG) through the PLN. PG creates and signs a location certificate containing the current location of device and its Device Secret Identifier (DSI). The PG sends this location certificate to DT. Based on the current status of the device and preconfigured policies, DT sends a response (possibly with a control command) to the device via PG through PLN.

1. Dev → M: DevIDReq
   Device sends a device identification request to the electric meter (M), where

$$\text{DevIDReq} = \text{DevName}, \text{SID}, \text{DTID}, \text{TS1}, \text{R1},$$
$$\text{HMAC}(\text{DSI}, (\text{DevName}, \text{DTID}, \text{TS1}, \text{R1}))$$

   and SID is the session identifier.
2. M → PG: Mname, DevIDReq, TS2, R2,
   HMAC(MSI, (Mname, DevIDReq, TS2, R2))
   Initially, M and substation mutually authenticate each other using Protocol MAP. Upon success, the meter forwards DevIDReq to PG.
3. PG → DT: LocInfo, DevIDReq, TS3, S_{PG} (h(LocInfo, DevIDReq, TS3))
   PG verifies the HMAC and infers the current device location from MSI. PG signs a location certificate consisting of LocInfo, DevIDReq, and TS3. The PG sends the signed location certificate to DT through a SSL tunnel.
4. DT processes device identification request
   DT verifies the DevIDReq and location certificate. Based on the current status of the device (e.g., reported stolen) and established policies, DT decides an appropriate response (possibly including a control command).
5. DT → PG: DevIDResp
   The DT signs its response as follows

$$\text{DevIDResp} = \text{Action}, \text{SID}, \text{TS4}, \text{R4}, S_{DT}(h(\text{Action}, \text{SID}, \text{TS4}, \text{R4}))$$

   where

$$\text{Action} = \text{DevName}, \text{DTID}, \text{Control-Command},$$
$$\text{HMAC}(\text{DSI}(\text{DevName}, \text{DTID}, \text{Control-Command}, \text{TS4}, \text{R4})).$$

6. PG → M: DevIDResp
   PG forwards the DT's response to the meter via PLN.
7. M → Dev: DevIDResp
   The meter forwards the DT's response to the device. The device verifies the DT's signature, HMAC in the Action, freshness of timestamp, and consistency of nonces. The device takes the specified action, which might block access to the device and its stored data.

III. List of Acronyms and Abbreviations

AMR	Automatic Meter Reading
AS	Application Server
ASID	Application Server Identifier
BPL	Broadband over the Power Line
C	User's Computer
D	Transaction Details
Dev	Mobile Device
DevName	Device name
DSI	Device Secret Identifier
DT	Device Tracking Server
DTID	Device Tracking Server Identifier
GPS	Global Positioning System
HAD	Human Authorization Detector
HMAC	Hash-based Message Authentication Code
IP	Internet Protocol
M	Electric Meter
MAP	Meter Authentication Protocol
MitM	Man-in-the-Middle
Mname	Meter Name
MSI	Meter Secret Identifier
PATM	Power line Anti-Theft Mechanism
PATP	Power line Anti-Theft Protocol
PG	Power Grid Server
PLAP	Power line Location Authentication Protocol
PLC	Power Line Communication
PLN	Power Line Network
R	Random nonce
SCADA	Supervisory Control And Data Acquisition
SID	Session Identifier
SS	Substation
SSL	Secure Sockets Layer
SSSI	Substation Secret Identifier
TPM	Trusted Platform Module
TS	Time Stamp
UID	User Identifier

About the Authors

Alan T. Sherman earned the PhD degree in computer science at MIT in 1987 studying under Ronald L. Rivest, the SM degree in electrical engineering and computer science from MIT, and the ScB degree in mathematics, magna cum laude, from Brown University. He is an associate professor of computer science at the University of Maryland, Baltimore County (UMBC) in the CSEE Dept. and Director of UMBC's Center for Information Security and Assurance. His main research interest is high-security voting systems. Sherman has carried out research in election systems,

algorithm design, cryptanalysis, theoretical foundations for cryptography, and applications of cryptography. Dr. Sherman is also a private consultant performing security analyses, an editor for *Cryptologia*, and a member of Phi Beta Kappa and Sigma Xi.

Dhananjay Phatak earned the PhD degree in computer engineering at University of Massachusetts, Amherst (UMASS) in 1994, the MSEE degree in microwave engineering at UMASS in 1990, and the B. Tech degree in Electrical Engineering from the IIT, Bombay. He is an associate professor of computer science at the University of Maryland, Baltimore County (UMBC) in the CSEE Department, and member of UMBC's Center for Information Security and Assurance. His main research interests are computer and network security, number theory, computer arithmetic algorithms and their VLSI realizations, mobile and high performance computing. Dr. Phatak has been a member of the technical program committee of the IEEE Biannual symposium on Computer Arithmetic from 1999 through 2009. He also served a three-year term as an Associate Editor of the IEEE Transactions on Computers, January 2002 through December 2005. He was a recipient of the National Science Foundation's (NSF) Career award in FY'99.

Vivek Relan earned the MS in computer science at UMBC in 2010 studying under Dhananjay S. Phatak and Alan T. Sherman. He earned the B.E. computer engineering from PICT, Pune, India in 2006. His primary interests are computer networking, information security and cryptography. He is a software development engineer at Amazon; previously, he worked as Member of Technical Staff, Jul'06–Jun'08, at GS Lab, Pune.

Bhushan Sonawane earned the MS in computer science at UMBC in 2010 studying under Dhananjay S. Phatak and Alan T. Sherman. He earned the B.E. computer engineering from PICT, Pune, India in 2006. His primary interests are computer networking, information security and cryptography. He is a software development engineer at Microsoft; previously he worked as a Member of Technical Staff, Jul'06-Jun'08, at Airtight Networks, Pune.

Acknowledgments

Phatak suggested the idea of using PLC for location authentication. We are grateful to Rick Carback, Russ Fink, Yordan Kostov, Tim Leschke, Chintan Patel, John Pinkston, and the reviewers for helpful comments. Sherman is supported in part by the Department of Defense under IASP Grants H98230-09-1-0404 and H98230-10-1-0359.

References

1. Absolute Software, Computrace, [Online]. http://www.absolute.com/ (accessed November 14, 2009).
2. Anatory, J., N. H. Mvungi, and 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.
3. Anderson, R. J. 2008. *Security Engineering—A Guide to Building Dependable Distributed Systems*, 2nd ed. New York: Wiley.
4. Authentify Inc. "Out of Band Authentication Employing Existing Infrastructure" [Online]. http://www.authentify.com/collateral/OOBAwhitepaper.pdf (accessed November 14, 2009).

5. BackStopp Laptop and Data Theft Protection, [Online]. http://www.backstopp.com/ (accessed November 14, 2009).
6. Bellare, M., R. Canetti, and H. Krawczyk. 1996. "Keying Hash Functions for Message Authentication." In: *Advances in Cryptology–CRYPTO '96*, Neal Koblitz, Ed., Volume 1109 of Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1–15.
7. Bouncy Castle Crypto APIs, [Online]. http://www.bouncycastle.org/java.html (accessed November 14, 2009).
8. Brands, S. and D. Chaum. 1994. "Distance-Bounding Protocols." In: *Advances in Cryptology—Eurocrypt '93*, T. Helleseth, Ed. Berlin: Springer-Verlag, 344–359.
9. BrickHouse Security, GPS Tracking—Live Tracking Devices from the Worldwide Leader in Real-Time GPS, [Online]. http://www.brickhousesecurity.com/info.html (accessed November 14, 2009).
10. Broadbridge, R. 1989. "Power Line Modems and Networks." In: *2nd IEEE National Conference on Telecommunications*, April 1989.
11. Bumiller, G., T. Sauter, G. Pratl, and A. Treytl. 2005. "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.
12. Capkun, S. and J.-P. Hubaux. 2004. "Securing Position and Distance Verification in Wireless Networks." Swiss Federal Institute of Technology Lausanne, Lausanne, Switzerland, Technical Report EPFL/IC/200443, February 3, 2004.
13. Denning, D. and P. MacDoran. 1996. "Location-Based Authentication: Grounding Cyberspace for Better Security." In: *Computer Fraud and Security*. Elsevier.
14. Dingledine, R., N. Mathewson, and P. Syverson. 2004. "Tor: The Second-Generation Onion Router." In: *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, USA, August 9–13, 2004.
15. FailSafe by Phoenix Technologies, [Online]. http://www.failsafe.com/ (accessed November 14, 2009).
16. GadgetTrak Laptop Security, [Online]. http://www.gadgettrak.com/ (accessed March 10, 2012).
17. Gonzales-Tablas, A. I., K. Kursawe, B. Ramos, and A. Ribagorda. 2005. "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, 797–806.
18. GPS Anti-Theft Systems, Enfotrace's GPS Anti-Theft Systems, [Online]. http://www.gpsantitheftsystems.com/ (accessed March 10, 2012).
19. HomePlug Powerline Alliance. "HomePlug AV White Paper," [Online]. http://www.homeplug.org/products/whitepapers/HPAV-White-Paper_050818.pdf (accessed November 14, 2009).
20. How to Remove Computrace Lojack, [Online]. http://www.freakyacres.com/remove_computrace_lojack?page=2 (accessed March 10, 2012).
21. "IEEE Standard for Broadband over Power Line Hardware." 2009. IEEE STD 1675–2008.
22. Integrated PLC Power Adapter, [Online]. http://www.upaplc.org/_files/ph2510_integrated_plc_power_adapter2.pdf (accessed November 14, 2009).
23. Kindberg, T., 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.
24. Lojack for Laptops, [Online]. http://www.lojack.com (accessed November 14, 2009).
25. Ophcrack, Windows Password Cracker, [Online]. http://ophcrack.sourceforge.net/ (accessed November 14, 2009).

26. Pacheco, F., M. Lobashov, M. Pinho, and G. Pratl. 2005. "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.
27. Parno, B. J. 2010. "Trust Extension as a Mechanism for Secure Code Execution on Commodity Computers." ' Ph.D. Dissertation, Dept. of Electrical and Computer Engineering, Carnegie Mellon University, Pittsburgh, PA.
28. Pavlidou, N., H. Vinck, J. Yazdani, and B. Honary. 2003. "Power Line Communications: State of the Art and Future Trends," *IEEE Communications Magazine*, 41(4):34–40.
29. Phatak, D. S. 2010. US and International Patent Application, "System, Method and Apparata for Secure Communication Using an Electric Grid Network," filed May 28, 2010.
30. Phatak, D. S., A. T. Sherman, B. Sonawane, and V. Relan. 2010. "Spread Identity: A New Dynamic Address Remapping Mechanism for Anonymity and DDoS Defense," Unpublished manuscript, Department of CSEE, University of Maryland, Baltimore County, 24 pages.
31. Phonefactor Inc. "Tokenless Two-Factor Authentication: It Finally Adds Up," [Online]. http://www.phonefactor.com/wp-content/pdfs/PhoneFactor-WhitePaper.pdf (accessed November 14, 2009).
32. Prey, Open-Source, Multi-Platform (Windows, Mac, Linux), Remote Tracking, [Online]. http://preyproject.com/ (accessed November 14, 2009).
33. Protect Notebooks and Data with Intel Anti-Theft Technology, [Online]. http://www.intel.com/technology/anti-theft/anti-theft-tech-brief.pdf (accessed November 14, 2009).
34. Remote Laptop Security, [Online]. http://en.wikipedia.org/wiki/Remote_Laptop_Security (accessed November 14, 2009).
35. RSA Security Inc. "The Power Behind RSA SecureID: Two-Factor User Authentication: RSA ACE/Server," [Online]. http://www.opsec.com/solutions/partners/downloads/rsa_securid_whitepaper.pdf (accessed November 14, 2009).
36. Sherman, A. T., D. Phatak, B. Sonawane, and V. G. Relan. "Location Authentication through Power Line Communication: Design, Protocol, and Analysis of a New Out-of-Band Strategy." In: *On-Line Proceedings of the IEEE ISPLC 2010: International Conference on Powerline Communications and Its Applications*, Rio de Janeiro, Brazil, March 21–28, 279–284. Available through IEEE Explore.
37. Smart Grid, [Online]. http://en.wikipedia.org/wiki/Smart_grid (accessed November 14, 2009).
38. Storage Protection with Intel Anti-Theft Technology—Data Protection (Intel AT-d), [Online]. http://www.intel.com/technology/itj/2008/v12i4/7-paper/1-abstract.htm (accessed November 14, 2009).
39. Strikeforce Inc. "Specializing in Preventing Identity Theft," [Online]. http://www.sftnj.com/news/pdf/Phishing_malware_spyware_prevention_by_StrikeForce.pdf (accessed November 14, 2009).
40. The Smart Grid and Privacy, Electronic Privacy Information Center (EPIC) statement, [Online]. http://epic.org/privacy/smartgrid/smartgrid.html/#intro (accessed June 7, 2010).
41. Treytl, A. and T. Novak. 2005. "Practical Issues on Key Distribution in Power Line Networks." In: *10th IEEE Conference on Emerging Technologies and Factory Automation*, September 2005.
42. Treytl, A., T. Sauter, and G. Bumiller. 2004. "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.
43. Windows BitLocker Drive Encryption [Online]. http://technet.microsoft.com/en-us/library/cc766200%28WS.10%29.aspx (accessed June 7, 2010).
44. Yu, J., P. Chong, P. So, and E. Gunawan. 2005. "Solutions for the 'silent node' problem in automatic meter reading system using powerline communications." In: *7th International Power Engineering Conference*, December 2005.
45. Yubico Inc. "YubiKey Security Evaluation," [Online]. http://yubico.com/files/Security_Evaluation_2009_09-09.pdf (accessed November 14, 2009).