Constructing Secure Localization Systems with Adjustable Granularity Using Commodity Hardware

Patrick Traynor
Georgia Institute of Technology

Joshua Schiffman, Thomas La Porta, Patrick McDaniel
Pennsylvania State University

Abhrajit Ghosh
Telcordia Technologies

Abstract— **Proof of a user's identity is not always a sufficient means for making an authorization decision. In an increasing set of circumstances, knowledge of physical location provides additional and necessary context for making decisions about resource access. For example, sensitive information stored on a laptop (e.g. customer records, social security numbers, etc), may require additional protections if a user operates outside of an approved area. However, current localization techniques based on signal strength reporting or specialized hardware fail to achieve this goal. In this paper, we design, develop, deploy and measure a system which securely determines the location of a user to within one meter through using** *only off-the-shelf* **802.11 and Bluetooth equipment. We apply this equipment in a two-phased challenge-response protocol: first determining the general area of the client in the Regionalization phase and then pinpointing it in the Localization phase. Using nearly 32,000 data points collected over 75 days, we argue that the stability of wireless networks over time creates easily distinguishable location profiles by which a client can be positioned. Additionally, we demonstrate the inherent ability of a two-phased protocol to discern a client's location information at a level of granularity no finer than is necessitated by policy. After discussing a number of applications, we build a location-based access control framework that automatically protects a white-listed set of resources through encryption when the user leaves specified areas. Our analyses show that this system provides a realistic and efficient means of incorporating unforgeable location information at the appropriate level of granularity into many authorization decisions.**

Keywords: Localization, Security, Secure Network Protocols

I. Introduction

Access to data and services is often dependent on a simple tuple: *Subject, Object, Privilege*. In particular, a user attempting to perform an action on a specific resource is permitted to do so if their identity and operation conform to policy. While this model has served static computing scenarios well, it fails to consider critical contextual information for such decisions in a mobile environment. As recent history has repeatedly demonstrated [4], such mechanisms alone are not capable of protecting sensitive information including credit card numbers and personal information in lost and stolen laptops. If unforgeable knowledge of a mobile device's location could be incorporated into resource authorization decisions, individuals and organizations would be significantly better protected from such information losses.

Unfortunately, current approaches for localization fail to provide an adequate foundation for making such decisions for one of two reasons: reliance upon signal strength measurements or the requirement of dedicated hardware. In the case of the former, a localizing client or receiver can indicate the signal strength of a message exchanged between the two parties. Because signal strength for a particular location can easily be calculated even in the presence of temporary fluctuations [16], an adversary can easily create a detailed signal strength map of an area. Accordingly, signal strength is not an adequate proof of location from a security perspective. While dedicated hardware solutions relying on natural constants (e.g., the speed of light) to bound location have shown great promise, *the purchase of expensive dedicated hardware for this task is likely to be difficult to justify, especially in difficult economic times.*

In this paper, we introduce a secure localization scheme built to model a traditional challenge-response protocol. This two phase protocol begins with a Regionalization phase, which uses multiple standard 802.11 access points to broadcast unique tokens at multiple distinct power levels. The overlapping transmission radii of these access points makes the tokens received by any client unique to particular areas. Having reduced the search area, the protocol then enters the Localization phase. Using standard Bluetooth radios, the infrastructure then transmits a new set of tokens that are used to more accurately determine a device's location. By splitting our protocol into two distinct phases, we allow the system preserve some location privacy for clients by performing localization only to a level necessary to satisfy a specific policy.

We argue that this approach is more robust than instantaneous sampling as it leverages the stability of communications in wireless networks within a confidence interval over time. Moreover, because a client can not forge the value of tokens it can not hear, it is not possible to create a mapping of expected responses as is the case in localization systems built on signal strength reporting. Finally, because this system is composed of common components, much of this infrastructure is likely already deployed in an average office environment. We support our claims of *stable* and *distinct* location profiles with an extensive implementation, deployment and measurement of such a system.

We then present a number of applications enabled by our secure location infrastructure. To characterize the usefulness of such applications, we design and implement a location-based access-control overlay. This links verified location information with a user-space daemon using eCryptfs to manage encrypted filesystems. As a user enters and leaves a specific location, these filesystems are automatically mounted (unencrypted) and unmounted (encrypted) to provide and restrict access to sensitive resources as dictated by policy. Because our framework is an access control overlay, location policies are applied to resource access *in addition* to the requirements of the traditional subject, object, privilege model.

We note that secure localization is an attempt to augment authorization decisions with additional context and not a replacement for the traditional *Subject, Object, Privilege* tuple. Like other forms of weak authentication (e.g., IP callback, distance bounding [5], [7], etc), such systems are susceptible to attacks by dedicated adversaries. However, our scheme not only increases the effort required by such an adversary over widely proposed signal strength schemes, but also accomplishes this goal using only COTS technology that is already deployed in most settings. Accordingly, the challenge in implementing such an approach comes in using infrastructure that is currently in service and not augmenting it further with expensive, specialized and limited-use equipment.

The remainder of this paper is organized as follows: Section II examines related research; Section III presents the architecture, algorithms and models used as the basis of our secure localization system; Section IV presents a localization study of our system; Section V evaluates the effectiveness and speed of localization our algorithm; Section VI introduces a number of sample applications, including the design, implementation and measurement of a location-based file access control framework; Section VII offers concluding remarks.

II. Related Work

Location-based services offer data and amenities specific to a user's geographic location. Used as a commercial application, a user's relative proximity to a store or restaurant may allow them to receive information about sales or discounts. In social networks, such services may instead be used to inform users when friends are within their vicinity [6], [18]. When used in industrial and corporate environments, location-based services offer the ability to maintain information on the whereabouts of both employees and valuable equipment. In order for all such services to be successful, they must be able to rely upon the accuracy and integrity of some underlying location determination mechanism. As traditional systems including GPS [9] are not effective indoors, researchers began investigating the use of other technologies to provide such assurances.

Many proposed localization systems rely on the presence of dedicated hardware [17], [20]–[22], [24], [27]. The difficulty with all such solutions, however, is that they employ non-standard and therefore potentially expensive dedicated hardware. The predominant means of providing indoor localization information using standard hardware is through the measurement of signal strength. First suggested by Bahl et al [3], this technique uses the triangulation of a client's received signal strength from multiple perspectives and compares them against a map of known signal strength readings to determine their location. Because such static maps fail to capture the dynamic nature of signal strength and are time-intensive to create, a number of modifications including statistical modeling [13] and the automatic generation [14], [15] and calibration of maps [16] were used to extend this basic technique. Faria et al [10] use overprovisioning and access-point specific handshakes to provide localization; however, this approach is not robust against a single direct antenna. Gwon et al [12] even build a system similar to the original RADAR based instead on a combination of 802.11 and Bluetooth receivers. Unfortunately, as signal strength is inherently and easily spoofable, all such systems fail against even basic adversaries. While a number of techniques have been designed to combat against location forgery [2], [19], [23], these mechanisms rely on signal strength, which can be spoofed by an adversary.

A handful of other techniques have also been built on commodity hardware. Analyzing roundtrip messaging times between access points and clients is proposed by Gunther et al [11]. Youssef et al [29] achieve asynchronous timing measurements through the use of modified hardware. Unfortunately, the accuracy of these methods suffers from ambient noise and competing traffic, hardware delay and non-line-of-sight transmissions. More relevant to this work, as these schemes involve interaction between a client and a single access point, they are more vulnerable to location spoofing than multi-observer systems.

While the above techniques fail to provide robust location determination against a determined adversary, they offer a number of useful building blocks. As described in our architecture in the following section, we use a number of the observations made in the previous work in concert with a two-phase, variable granularity protocol to accurately determine a client's physical location.

III. System Design

Proof of one's location should not be possible using a static response. Accordingly, characteristics of a location that can easily be approximated or learned within some tolerance (e.g., signal strength) are not sufficient as the basis of an unforgeable localization system. We instead find inspiration from traditional cryptographic protocols, in which only correct responses to unique challenge-response requests can be used to verify a user. Specifically, by requiring a user to overhear and return a set of random values unique to each iteration of the protocol, we bound knowledge of a location's characteristics temporally.

We present a two-phase protocol designed to provide location information only as specific as is required by policy. In the first, or *Regionalization* phase, commodity 802.11 access points transmit tokens containing random values at multiple power levels. The regions created by overlapping transmission radii can be distinguished by the specific tokens received and reported by a client. Should this phase of localization return a region with an area too large to assure compliance to a policy, our system then launches the *Localization* phase. Using Bluetooth radios surrounding the region discovered in the previous phase, we are able to more tightly bound a user to a physical location. The details of this architecture, our model and policy in our system are explained in this section.

A. Protocol Specification

Before presenting a more formal version of the localization protocol, we provide the following notation.

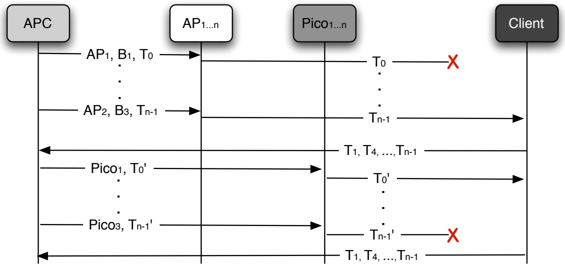

Fig. 1. A high-level overview of the two-phased protocol. After generating random tokens for the Regionalization phase, the APC compares the tokens reportedly heard by the client against known fingerprints. If the policy specified for this attempt requires a more accurate representation of a user's location, the APC then selects a group of Pico nodes for the Localization phase. The APC generates new tokens, evaluates the client's response and determines the client's location.

Notation:

- AP_i is the i^{th} access point.
- B_i is the power level at which a token is to be broadcast. $1 \leq i \leq 3$ for low, medium and high power, respectively.
- n is the number of tokens generated in a single round.
- T is the set of tokens generated by the APC for a round.

Localization can be initiated in one of two manners. A client may contact the *Access Point Controller* (APC) with a specific location policy to which it wishes to prove compliance. Alternatively, the APC can initiate localization. The APC then generates a unique set of tokens. Each token is randomly assigned an *Access Point* (AP) from which it is to be broadcast. Tokens are also assigned one of three transmission powers: low, medium or high. The power level (dB) associated with each of these three classifications bounds the distance over which a token is heard by clients. When such distance-bounded tokens are transmitted from multiple APs, localization becomes a problem of matching the received tokens to overlapping transmission radii.

Should the granularity of this first round not be sufficient, the APC can then launch a second round using the information learned in the first round to seed the selection of Pico nodes. Performing Regionalization allows the APC to select a small subset of the Pico nodes believed to be nearby the client. In so doing, the APC can reduce the interference caused by an office-wide localization attempt. The size of this subset can be directly related to the granularity required by a policy. For instance, a policy requiring that a client be located in a specific office may require all Pico nodes surrounding that office to participate. Alternatively, a policy requiring a client to be in any one of a block of offices may use a small number of machines. Tokens can then be broadcast randomly from the subset of Pico nodes. Note that tokens are broadcast at a fixed transmission power in the Localization phase as Bluetooth does not currently offer an API for power. If the protocol was initiated by a client and the included location policy successfully verified, the APC returns confirmation of the location submitted by the client (which includes the identification of the node, a timestamp, the policy and a digital signature of all of these fields). Figure 1 provides an overview of this process.

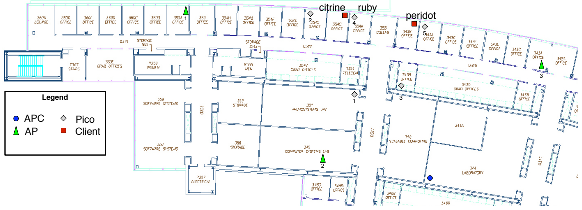

Fig. 2. Deployment environment: The number below each unit corresponds to its identity.

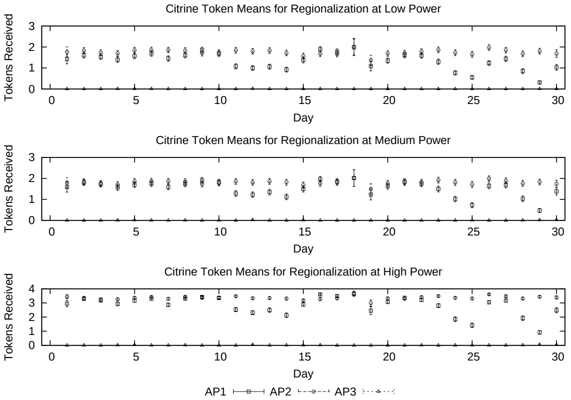

Fig. 3. The observed token reception patterns of client Citrine in the Regionalization phase when analyzed over one month.

IV. Reception Characteristics

As presented in the preceding pages, it is the recognition of a location's token unique reception pattern that makes localization possible. Intuitively, for the proposed system to perform adequately (e.g., correctly locate a client), the number of tokens received at a location must be *stable* and *distinct*. This section attempts to prove the hypothesis that token reception does in practice fulfill these requirements using the environment shown in Figure 2. For space reasons, we only show the stability results from two clients for the Regionalization phase named, Citrine and Peridot. However, we performed similar experiments at 15 additional locations throughout the testing and collected similar results (see the technical report [25]).

A. Stability

We now view the real-world measured stability. These experiments raise an interesting problem for our solution: *if transient errors cause radical changes in reception patterns, then what hope is there that we can develop models that are robust enough to allow for reliable localization?* The answer is in the distribution of the received packets. Our complete hypothesis is therefore that while the instantaneous measurements of received packets may not be stable, their distributions over time will be.

To evaluate this hypothesis, we study aggregated samples. Figure 3 shows the mean number of tokens received for every round for each hour and annotate those means with a 95% confidence interval. The graphs indicate that the means for these samples approach zero. Moreover, the reception variance decreases inversely with transmission power.

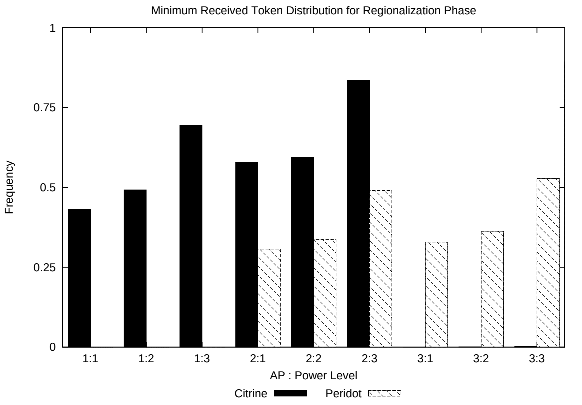

Fig. 4. Fingerprints for the Regionalization phase using a 95% confidence interval.

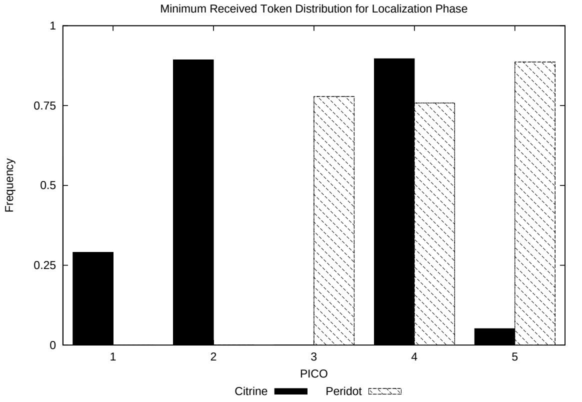

Fig. 5. Fingerprints for the Localization phase using a 95% confidence interval.

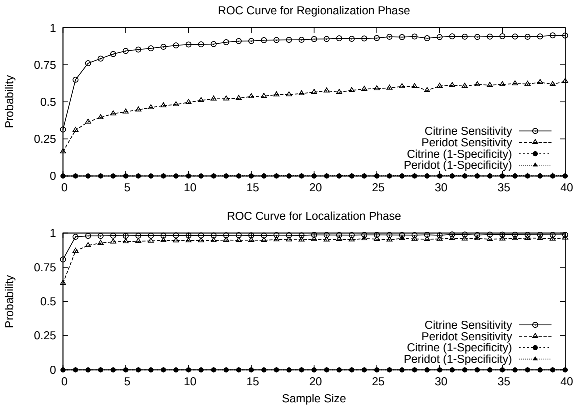

Fig. 6. The Relative Operating Characteristic curve. Localization is accurate after a small number of rounds.

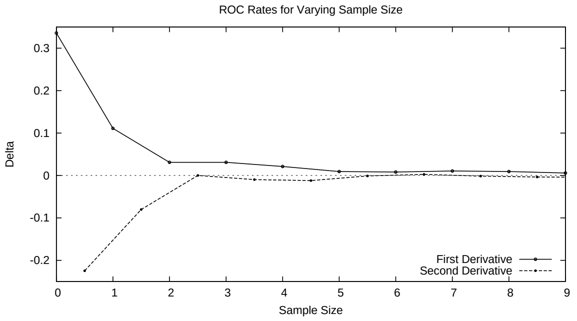

Fig. 7. The rate of change for the Regionalization ROC curve. As these lines approach zero, the gains from performing additional iterations of the protocol rapidly approach zero.

These experiments show that reception is subject to instantaneous interference, but over larger time scales is exceptionally stable. Because of this, we can use reception as a key metric in determining location. What remains is whether reception characteristics are sufficiently distinct to tell one location from another.

B. *Distinction*

To assess how distinct each location's reception rates are, we gathered a one week sample of rounds from Citrine and Peridot and computed the 95% confidence intervals for the means of reception for each locating device. Each of these reception rates represents a test of knowledge for each location. Since tokens cannot be forged, our system only requires that a client can demonstrate knowledge of *at least* as many tokens as required by a fingerprint.

Thus, we can consider the lower bounds for each mean, represented by the bars in Figures 4 and 5, as the minimum threshold for matching client responses to location fingerprints. The fingerprints of each client have distinct differences. In the Regionalization phase, Citrine never receives a token from AP3. Also, Peridot never hears any tokens from AP1. The Localization phase demonstrates similar results for Pico devices. We demonstrate the ability to differentiate between users less than one meter apart in our full technical report [25].

V. Algorithm Evaluation

We now evaluate the system's ability to correctly localize clients. As previously discussed, when the number of iterations of a phase of the protocol (sample size) increases for a fixed starting time, the chance of successfully receiving sufficient tokens to meet a location's fingerprint will increase. We therefore determine how many iterations of the protocol a client must go through before its position is identified with high confidence.

A Relative Operating Characteristic (ROC) curve is a well established tool for graphically comparing and evaluating classification algorithms. The ROC demonstrates sensitivity versus (1 - specificity) for all values of a diagnostic parameter. We use the ROC curves to identify the sample size that optimizes the performance of our protocol.

Figure 6 shows that for the Regionalization phase, the sensitivity rises rapidly. However, as Figure 7 shows, the improvement levels out quickly at the inflection point near the sixth iteration. This indicates that clients are able to obtain sufficient tokens with a higher probability as more iterations of the phase are performed, but the improvement is limited. By contrast, the Localization phase in Figure 6 shows the protocol approaches a high confidence of discrimination within just a few rounds. The short range of Bluetooth ensures that clients within range of a Pico device will receive the expected number

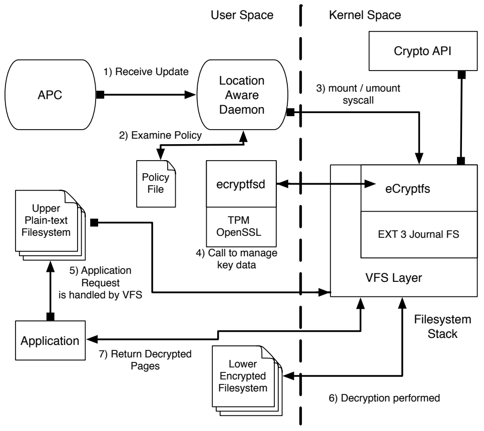

Fig. 8. The location-based file access control system.

of tokens within a few rounds.

These results demonstrate that, while the Regionalization phase can eventually obtain a general region of the client, *the overall classification performance and accuracy can be significantly improved by switching to the Localization phase as soon as a small enough set of Pico devices are established.*

VI. Applications

A. Location-Based Access Control

The leakage of sensitive information from lost or stolen laptops is a serious threat to the security of an organization and its members. Reports of devices with unencrypted personal [1] and financial [28] data are becoming more common. Given the potentially huge liability for the loss of such information, organizations must develop mechanisms capable of mitigating such threats. A mandatory access control (MAC) overlay based on a user's location may be one such solution. For instance, when an employee is in the non-public portions of an office, the localization infrastructure should allow them to access sensitive files as normal. However, once a laptop enters a public area (e.g., the cafeteria, the employee's car, etc), these files should be automatically encrypted to prevent leakage. We design, implement and measure such a system below.

1) Access Control Framework: The location-based access control overlay shown in Figure 8 describes the various components involved in the framework and how they are connected. This system is designed to provide the following funcionality: 1) the location sensitive content and resources must not be accessible except to those permitted to use them; 2) The data must be confidential even in the absence of the localization infrastructure; 3) The system must be simple to administer yet flexible for variability in locating service accuracy requirements; 4) The system must be transparent to the user.

To satisfy the first two design goals, we use eCryptfs [8]. A recent addition to the 2.6.19 mainline Linux Kernel, eCryptfs is a stackable cryptographic virtual filesystem that provides the cryptographic functions needed to protect the location-sensitive files. Specifically, eCryptfs uses per file symmetric keys embedded in the extra attributes of each file header. These keys are then protected using a filesystem-wide key. Through the user-space daemon `ecryptfsd`, eCryptfs also supports asymmetric ciphers, programs including OpenSSL and commodity hardware such as the Trusted Platform Module [26].

TABLE I
Microbenchmark of Framework

Function	Time (μsec)	95% CI
Mount (regular)	3977.678	±137.07
Mount (eCryptfs)	529470.727	±556.771
Unmount (regular)	3481.135	±192.007
Unmount (eCryptfs)	2411.087	±2332.72

2) Accessing Files: Figure 8 provides an overview of our access control overlay. After successfully completing the secure localization protocol, the APC sends a signed location update to the *Location Aware Daemon* (LAD). After verifying the signature, the LAD examines the policy file. If mounts[1] for the current location exist, the objects associated with those mounts become available to the user. Should an open mount no longer comply with its policy (i.e., the location has changed since mounting), this mount is made unavailable to the user.

Assuming that a change in location has caused a corresponding change in the available mount, the third step of this process contacts the kernel crypto API and key manager to encrypt/decrypt data. If a public key is used, a callback to the user-space daemon `ecryptfsd` is instead made. The encrypted "lower" filesystem is then exposed by the VFS layer as a plain-text "upper" filesystem. Requests to access these virtual files are redirected to eCryptfs. For reads, unencrypted blocks corresponding to the file are placed into memory and made available to applications. Writes are simply encrypted and written to disk. Because the contents of lower filesystem are encrypted, attempts to do direct reads leak no information.

Control need not be limited to single user systems. A multi-user system such as a laptop shared between employees could also benefit from the location-based access control framework. By only mounting the filesystem associated with the employee using a laptop, the workspaces of each user could be better separated.

3) Experimental Results: We performed a performance analysis of this framework to better characterize the entire system. Each test was performed 1,000 times We used the AES-128 cipher in CBC mode for both upper and lower layer encryption. Each read and write operation occurred over 50MB datasets in an ext3 filesystem. Table I summarizes our results.

The use of encrypted mounts significantly increases the time required to access data. When compared to a standard mount operation, an eCryptfs mount requires just over two orders of magnitude more time to execute. From a user perspective, however, an average of 0.5 seconds to mount a drive is certainly within the lower range of observable delay. Such a system is therefore practical for use in real systems.

B. Enabling Additional Services

The applications enabled by a secure localization system need not only restrict the operations performed by a user.

[1] We refer to location-bound filesystems as mounts as they are described as mount points by eCryptfs.

Instead, services beneficial to the user experience can also be provided by such an infrastructure. Any application potentially requiring a large amount of user configuration or knowledge may be augmented by such a service.

One such example is print services in a large office. As an example, a user giving a presentation in a conference room may need to make copies of their proposal. Requiring that user to select the closest printer based on their knowledge of the building may result in incorrect or inefficient decisions. Alternatively, by allowing the print server to make decisions based on the user's location in conjunction with its own access rules (e.g., nobody but the CEO may send documents to the printer in the executive boardroom), the network could help the user more efficiently print his/her documents.

Given the ability to adjust the granularity with which a client's location is resolved, this infrastructure may also support multi-level security (MLS) policies. In particular, users willing to engage in additional rounds of the protocol may be allowed to gain access to *Top Secret* files, whereas those users only participating in the first round may only be allowed to view *Secret* resources.[2]

VII. Conclusion

Identity alone is insufficient information for making authorization decisions in a mobile environment. In many scenarios, a user's physical location may be equally as critical. In order to provide such information in an unforgeable manner, we have designed, implemented, deployed and measured a new secure localization system. Unlike previous localization schemes that use guessable information such as signal strength or dedicated hardware, our system uses a challenge-response protocol to verify a user's location. In the Regionalization phase of our protocol, 802.11 access points triangulate a user's approximate position by transmitting a series of unique tokens at different power levels. Having determined the general region in which a device is located, we then execute Localization using Bluetooth. These short-range radios allow a client to be located on a per-office ($<$ one meter) basis. Each phase of the protocol is only executed until a location policy is met, thereby restricting the location knowledge learned by the system and providing a measure of privacy for users. Moreover, we use only commodity equipment that is likely to already be deployed in most corporate environments, *thereby providing a strong approach to localization that does not require the purchase of additional expensive dedicated hardware.* In a time when corporate sending is being tightened, such a solution is potentially more attractive than related solutions. In spite of instantaneous fluctuations on the air interface, this approach and wireless networking in general are possible because transmissions at a given power level are stable within a reasonably tight confidence interval over time.

References

[1] M. Apuzzo. Vets Can Sue VA Over Stolen Laptop. http://ap.google.com/article/ALeqM5gqGfy6HNMsTyAGUesRe43dQCGsDgD8SV20PO2, 2007.

[2] Aruba Networks, Inc. Dedicated Air Monitors? You Decide. http://www.arubanetworks.com/technology/tech-briefs/dedicated-air-monitors/, 2006.

[3] P. Bahl and V. N. Padmanabhan. RADAR: An In-Building RF-Based User Location and Tracking System. In *Proceedings of IEEE Infocom*, 2000.

[4] B. Brenner. More laptops stolen, 300,000 customer records at risk. http://searchcrm.techtarget.com/originalContent/0,289142,sid11_gci1192626,00.html, 2006.

[5] J. Clulow, G. Hancke, M. Kuhn, and T. Moore. So near and yet so far: Distance-bounding attacks in wireless networks. In *Security and Privacy in Ad-hoc & Sensor Networks*, 2006.

[6] Dodgeball.com. http://www.dodgeball.com/, 2006.

[7] S. Drimer and S. J. Murdoch. Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks. In *Proceedings of the USENIX Security Symposium (SECURITY)*, 2007.

[8] eCryptfs. http://ecryptfs.sourceforge.net/, May 2007.

[9] P. Enge and P. Misra. Special Issue on GPS: The Global Positioning System. *Proceedings of the IEEE*, pages 3–172, Jan 1999.

[10] D. B. Faria and D. R. Cheriton. No Long-term Secrets: Location-based Security in Overprovisioned Wireless LANs. In *Proceedings of the ACM Workshop on Hot Topics in Networks (HotNets)*, 2004.

[11] A. Gunther and C. Hoene. Measuring Round Trip Times to Determine the Distance Between WLAN Nodes. *Networking*, pages 768–779, 2005.

[12] Y. Gwon, R. Jain, and T. Kawahara. Robust Indoor Location Estimation of Stationary and Mobile Users. In *Proceedings of IEEE INFOCOM*, 2004.

[13] A. Haeberlen, E. Flannery, A. M. Ladd, A. Rudys, D. S. Wallach, and L. E. Kavraki. Practical Robust Localization over Large-Scale 802.11 Wireless Networks. In *Proceedings of the Tenth ACM International Conference on Mobile Computing and Networking (MOBICOM)*, 2004.

[14] M. Hassan-Ali and K. Pahlavan. A New Statistical Model for Site-Specific Indoor Radio Propagation Prediction Based on Geometric Optics and Geometric Probability. *IEEE Transactions on Wireless Communications*, 1(1):112–124, Jan 2002.

[15] A. Hills, J. Schlegel, and B. Jenkins. Esstimating Signal Strengths in the Design of Indoor Wireless Networks. *IEEE Transactions on Wireless Communications*, 3(1), Jan 2004.

[16] Y. Ji, S. Biaz, S. Pandey, and P. Agrawal. ARIADNE: A Dynamic Indoor Signal Map Construction and Localization System. In *Proceedings of the Fourth ACM/USENIX Conference on Mobile Systems, Applications and Services (MobiSys)*, 2006.

[17] J. Krumm, S. Harris, B. Meyers, B. Brumitt, M. Hale, and S. Shafer. Multi-Camera Multi-Person Tracking for EasyLiving. In *IEEE Workshop on Visual Surveillance*, 2000.

[18] F. Lantz. Pac-manhattan. http://www.pacmanhattan.com/, 2004.

[19] S. Pandey, F. Anjum, B. Kim, and P. Agrawal. A Low-cost Robust Localization Scheme for WLAN. In *Proceedings of the Second International Conference on Wireless Internet (WICON)*, 2006.

[20] N. B. Priyantha, A. K. L. Miu, H. Balakrishnan, and S. Teller. The Cricket Compass for Context-Aware Mobile Applications. In *Proceedings of the Sixth Annual ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2001.

[21] N. Sastry, U. Shankar, and D. Wagner. Secure Verification of Location Claims. In *Proceedings of the Second ACM Workshop on Wireless Security (WiSe)*, 2003.

[22] S.Capkun and J. Hubaux. Secure positioning of wireless devices with application to sensor networks. In *Proceedings of IEEE INFOCOM*, 2005.

[23] P. Tao, A. Rudys, A. M. Ladd, and D. S. Wallach. Wireless LAN Location-Sensing for Security Applications. In *Proceedings of the Second ACM Workshop on Wireless Security (WiSe)*, 2003.

[24] N. O. Tippenhauer and S. Capkun. ID-based Secure Distance Bounding and Localization. In *Proceedings of the European Symposium on Research in Computer Security (ESORICS)*, 2009.

[25] P. Traynor, J. Schiffman, T. La Porta, P. McDaniel, A. Ghosh, and F. Anjum. Constructing Secure Localization Systems with Adjustable Granularity. Technical Report NAS-TR-0084-2007, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, 2009.

[26] Trusted Computing Group. http://www.trustedcomputinggroup.org/, Mar. 2005.

[27] R. Want, A. Hopper, V. Falcao, and J. Gibbons. The Active Badge Location System. *ACM Transactions on Information Systems*, 10(1):91–102, January 1992.

[28] T. Weiss. Laptop with credit card info for 80,000 DOJ workers stolen. http://www.computerworld.com/governmenttopics/government/legalissues/story/0,10801,102146,00.html, 2005.

[29] M. Youssef, A. Youssef, C. Rieger, U. Shankar, and A. Agrawala. Pinpoint: An asynchronous time-based location determination system. In *Proceedings of the Fourth ACM/USENIX Conference on Mobile Systems, Applications and Services (MobiSys)*, 2006.

[2] Assuming the principle has the requisite subject, object, permission rights.