Security Parallels Between People and Pervasive Devices

Stephen A. Weis [*]
Computer Science and Artificial Intelligence Laboratory
Massachusetts Institute of Technology
Cambridge, MA 02139, USA
sweis@mit.edu

Abstract

Unique and challenging security problems arise due to the scarcity of computational, storage, and power resources in the low-cost pervasive computing environment. Particularly relevant examples of resource-constrained systems are low-cost Radio Frequency Identification (RFID) systems. Surprisingly, the computational abilities of low-cost pervasive devices like RFID tags are similar to another pervasive, weak computing "device": people.

Neither low-cost pervasive devices nor people can efficiently perform public-key or even symmetric cryptographic operations. Neither can store long random strings nor devote too much time or energy to security protocols. Both may need to authenticate themselves over a public channel to an untrusted terminal, without any outside help or external devices. Because of these similarities, pervasive security may benefit by adapting techniques from human-computer security, or vice versa.

This article treats RFID tags as a model for other low-cost pervasive devices, and describes some of their practical constraints. Several parallels between the pervasive and human-computer security settings are discussed. Finally, this article highlights one particular human-computer authentication protocol, due to Hopper and Blum, that is immediately adaptable to low-cost RFID. Borrowing techniques from Hopper and Blum, or other human-computer protocols could lead to practical pervasive security protocols.

1 EPC: A Low-cost Pervasive System

Some of pervasive security's most interesting and difficult problems arise in low-cost systems. In these settings, pervasive devices are entrusted with sensitive data, yet lack the computational resources necessary to perform strong encryption or authentication. Canonical examples of resource-constrained pervasive devices are found in low-cost Radio Frequency Identification (RFID) systems.

Quite briefly, RFID systems consist of transponders, or "tags", attached to physical objects that carry data which may be wirelessly accessed by radio transceivers or "readers". By associating digital data with physical objects, RFID can potentially bridge the gap between the online world and the real world. The name "RFID" actually encompasses a wide range of technologies with varying operating parameters and functionalities.

Much of the recent media buzz over RFID has focused on low-cost Electronic Product Code, or EPC, type tags [10]. EPC tags are extremely cheap RFID tags designed for use in supply-chain management, inventory control, and retail checkout. EPC is the heir apparent to the Universal Product Code (UPC), the optical barcode found on many retail products.

EPC tags could eventually be the most pervasive computing device in history. Philips Electronics, an RFID tag manufacturer, has already shipped over one billion units [41]. Organizations like Wal-Mart and the United States Department of Defense are adopting RFID for their enormous supply chains, and pressing their suppliers to do the same [30]. Eventually, an average person may have dozens of RFID tags embedded in their clothes, shoes, books, drug packaging, or groceries.

Resources in EPC tags are extremely scarce. To be economically viable, the ideal EPC tag would cost in the US$0.05-0.10 range. Batteries are too expensive at these costs, so EPC tags will passively harvest energy from an RFID reader's communication signal. Consequently, EPC tags will lack an on-board clock, cannot perform computations in the absence of a reader, and may be limited to perhaps 10 μW of power consumption per read operation.

Gate counts will be tightly constrained as well. EPC tags may have 1000-10000 gate equivalents, with only about 200-2000 budgeted for security. Public-key cryptosystems like RSA or NTRU are much too computationally inten-

[*] This work conducted while at RSA Laboratories.

sive for EPC tags. Even standardized symmetric encryption algorithms like DES and AES, or the standardized SHA-1 hash function are too costly in terms of gate count.

An EPC tag may have 96-512 bits of non-volatile storage, which may be read-only or re-writable only a limited number of times. Tags may also have a small amount of volatile memory; perhaps 32-128 bits. The storage and memory of an EPC tag are dwarfed by the size of a viable RSA key. Although there are cryptosystems operating over toruses, lattices, or elliptic curves with efficient key representations, they require much more logic than is available on most EPC-type tags.

Finally, a reader must be able to read about 100 tags a second. For some EPC technologies, this represents roughly 10,000 clock cycles of computation on a tag. Clock cycles are actually one of the least constrained aspects of an EPC tag. Regardless, since nearly every resource is scarce on an EPC tag, addressing security issues requires new protocols, constructions, and engineering approaches.

2 RFID and Pervasive Security

As RFID tags and other pervasive devices become commonplace, new security threats may arise. These threats may include espionage, counterfeiting, sabotage, or privacy violations. For instance, the United States Food and Drug Administration (FDA) recently recommended attaching RFID pedigrees to prescription drug bottles with the intention of combating drug counterfeiting [13].

Without proper protection, these tags could violate consumer privacy by revealing sensitive prescription drug data. Ironically, insecure RFID tags could actually function as beacons and help thieves quickly locate high-value drugs. There is also a threat that corporate spies could use tags to derive sales and logistics data. This is valuable information in a corporate setting and critical in a military setting. Saboteurs and vandals could re-label or erase unprotected tag contents to slow down or deny RFID-based services. At the very least, RFID tags attached to products could lull users into a false sense of confidence about their security and their product's origin.

Fortunately, there is a growing body of literature addressing RFID security issues and pervasive security in general. Sarma, Engels, and this author discuss RFID security and privacy threats in [42] and [43]. Rivest and the same authors propose low-cost countermeasures to these threats in [52], which this author extends in [51].

Privacy is a key concern for consumers and could be a barrier to RFID adoption if not protected. Juels and Pappu proposed privacy-preserving mechanisms for RFID-tagged Euro banknotes [26], which were later analyzed by Avoine [2]. Molnar and Wagner analyze privacy in library RFID systems [37]. Garfinkel considers privacy from the policy perspective and offers suggestions for standard policy practices in [14]. Floerkemeier and Lampe discuss how to support various security policies in RFID implementations [12]. Many similar topics were presented at the MIT RFID Privacy Workshop held in 2003 [36].

A growing body of literature offers various security constructions and countermeasures appropriate for low-cost RFID and perhaps other pervasive systems. Jules, Rivest, and Szydlo's "blocker tag" [27] is a privacy-protecting device that consumers can carry to prevent unauthorized parties from scanning their tags. Juels' offers a set of "minimalist" cryptographic primitives for authentication and privacy [24]. Juels' also introduces the notion of RFID "yoking proofs" which can attest that two tags were scanned in close proximity [25]. Both Henrici and Müller [19], and Ohkobu, Suzuki, and Kinoshita [40] describe hash-based RFID privacy enhancements. Vajda and Buttyan offer lightweight authentication protocols appropriate for RFID tags [48]. Feldhofer, Dominikus, and Wolkerstorfer propose a low-cost AES implementation, possibly suitable for future EPC tags [11].

The FDA's RFID proposal [13] and recent moves by the casino industry to adopt RFID-tagged casino chips [18] increases the need to authenticate tags to readers (although reader-to-tag authentication may be equally important). Readers need to be able to wirelessly authenticate a tag's identity, otherwise counterfeiters could trivially manufacture cloned casino chips, access control cards, or stored-value cards. Interestingly, authenticating tags to readers is similar in many ways to authenticating humans to computers.

3 Human-Computer Security

Many pervasive security issues must be addressed within the resource constraints of low-cost devices. Surprising, low-cost devices like EPC tags share many properties with another pervasive, weak-computing device: human beings. In particular, there are many similarities in authenticating identities of both people and tags.

Neither people nor tags can perform complex computations. EPC tags lack the necessary gate count to efficiently perform modular arithmetic operations over large fields or to compute standard cryptographic algorithms like DES, AES, or SHA-1. One may assume that most people cannot perform these operations in their head, either.

In general, both tags and people have a limited capacity to store random PINs or passwords. An EPC tag may have a few hundred bits of password storage, which might only be re-writable a limited number of times. Although humans can store huge amounts of data, we are not well adapted to remembering strings of random bits.

People and tags may need to authenticate themselves under similar settings: across a public channel to an untrusted party with no outside help. A naive password would only be valid for a single session, since it could be easily captured by an eavesdropper. Neither tags nor people can always rely on a trusted token or third-party to aid in authenticating their identity. We cannot always assume that people have a PDA, calculator, or RSA SecureID-type token to help authenticate themselves.

Furthermore, tags must meet minimum performance requirements, so cannot devote too much time authenticating themselves. Similarly, people have a patience threshold and will not tolerate a long, complicated login process.

However, there are (hopefully) significant differences between tags and people. Tags are better at logical operations and at generating random bits. People can authenticate themselves using visual or text aids, or deductive reasoning. Unless specially equipped, tags are "worse" at performing base-10 arithmetic. Internal secrets on tags can be extracted using low-cost physical attacks [1]. Physically attacking people for their secrets tends to yield unreliable results [47].

Human authentication protocols are the subject of Carnegie Mellon University's HumanAut project [22]. Early work by Lamport described a one-time password authentication scheme [31]. Matsumoto and Imai [34] and Matsumoto [33] also proposed authentication protocols that could authenticate a person a limited number of times [49]. "Visual cryptography", proposed by Naor and Pinkas, allows humans to verify cryptographic data printed on plastic transparencies [38]. Chaum proposes voting systems based on visual cryptography that require little human effort [7]. A particularly notable human authentication protocol is by Hopper and Blum [20, 21].

4 Hopper-Blum Authentication

We offer the Hopper-Blum (HB) protocol as an example human-computer protocol that may be adapted to pervasive computing. The HB protocol does not require complex computations and can be computed entirely in someone's head. As an experiment, Tollinger configured a vending machine to dispense free soft drinks to Carnegie Mellon University students able to authenticate themselves using Hopper and Blum's protocol [46]. The HB protocol is based on the hardness of the *learning parity with noise*, or LPN, problem:

Definition 1 (LPN Problem) *Given an $q \times n$ matrix **A**, where q is a polynomial of n in size, a q-bit vector **z**, and a noise parameter $\eta \in (0, \frac{1}{2})$, find an n-bit vector **x** such that $|\mathbf{Ax}\text{-}\mathbf{z}| \leq \eta q$.*

Hopper and Blum's LPN-authentication protocol is quite simple. Suppose two parties, Alice and Bob, share a random n-bit secret **x**. Alice sends Bob a random challenge $\mathbf{a} \in \{0,1\}^n$. Both Alice and Bob compute the boolean inner product $\mathbf{a} \cdot \mathbf{x}$, denoted the *parity bit* z. Bob returns his parity bit z to Alice, who accepts only if their parity bits match.

If **a** and **x** are random, someone who does not know **x** can guess Bob's parity bit half the time. If Alice repeats the protocol for q rounds, someone only has a 2^{-q} chance of naively guessing all rounds correctly. However, an eavesdropper capturing $O(n)$ rounds can trivially compute **x** through Gaussian elimination.

To combat eavesdroppers, Bob will inject noise into his parity bit responses. Bob will intentionally send the wrong parity bit for a fraction η of the rounds. Alice will authenticate Bob's identity if less than ηq rounds are incorrect.

Passive eavesdroppers capture Alice's q challenges as a matrix **A** and Bob's parity bit responses **z**, then try to compute **x** such that $|\mathbf{Ax}\text{-}\mathbf{z}| \leq \eta q$. An adversary able to successfully complete the protocol could efficiently solve the LPN problem. Thus, the security of the protocol rests on the hardness of LPN.

The LPN problem is closely related to the *minimum disagreement problem*, or MDP [9]. The LPN is also similar to the problem of finding the closest vector to a random linear error-correcting code - also referred to as syndrome decoding [3, 15, 32]. The McEliece public-key cryptosystem is based on the hardness of syndrome decoding [35], as is the Niederreter cryptosystem [39], Stern's public-key identification scheme [44, 45], and Courtois et al.'s digital signature system [8]. Although infeasible in practice, Chabaud offers attacks that establish practical security parameters for some error-correcting code based cryptosystems [6] .

The LPN problem is known to be NP-Hard [3] and is difficult to approximate within a factor of 2 [17]. The difficulty of solving a random LPN instance is unknown, although there are several pieces of evidence indicating that it is indeed hard. Blum, Furst, Kearns, and Lipton show that an adversary given only a random vector **a** who is able to weakly predict the value $\mathbf{a} \cdot \mathbf{x}$ with advantage $\frac{1}{n^c}$ could efficiently solve the LPN problem [4].

Kearns later proved that the LPN is not efficiently solvable in the statistical query model [29]. Hopper and Blum establish that the LPN is pseudo-randomizable and log-uniform [20, 21]. The best known algorithm for solving the LPN problem by Blum, Kalai, and Wasserman (BKW) has an asymptotic run time of $2^{\Theta(\frac{n}{\lg n})}$ [5].

In 1993, several random instances of the LPN problem were converted to CNF form and presented by DIMACS as challenging instances of the satisfiability problem [23]. Several years later, the instances were solved by separate researchers using brute force algorithms [16, 50]. Warners and van Maaren were eventually able to solve the DIMACS instances of the LPN problem with $n = 32$ in a matter of minutes.

Based on a concrete analysis of the BKW algorithm, we estimate that the BKW algorithm would take roughly 2^{56} steps of computation for keys of length $n = 128$, 2^{64} for $n = 160$, and 2^{80} steps for $n = 224$.

5 A New Direction in Pervasive Security

Although adapted for ease of use by humans, Hopper and Blum's scheme is very efficient for low-cost devices. Their protocol could be implemented on tags with only the logic necessary to compute the inner product of two boolean vectors and storage for the key **x**. Computing the inner product entails simply performing AND and XOR operations. If computed bitwise, the parity bit can be computed on-the-fly without storing any of the challenges **a**. The author offers a more detailed analysis of the HB protocol in [28].

In many ways, the LPN-authentication protocol is more suited for hardware devices than for people. Hopper and Blum have translated the LPN problem to base-10 to make it more palatable to people. However, people are not adapt at choosing random noise bits, which are crucial to the security of the protocol. In contrast, devices like EPC tags can cheaply generate randomness from diode breakdown, shot, or thermal noise, cellular automata, metastability, oscillation jitter, or a slew of other methods.

Unfortunately, the HB protocol is only secure against passive adversaries who cannot actively send challenges. An attacker able to send non-random challenges could quickly determine noise-free parity bits. The author offers an enhanced HB protocol secure against active adversaries in [28].

Hopper and Blum also offer a second human authentication protocol based on the "Sum of k Mins problem" that is designed to be secure against active adversaries [21]. This scheme is tailored to be carried out by people, and relies on base-10 arithmetic. It could potentially be adapted for low-cost devices, although there is not a conversion as clearly apparent as for the LPN-based protocol. An open line of research might be to try to remove the human-specific aspects of Hopper and Blum's "Sum of k Mins" protocol, and adapt it to low-cost pervasive devices.

The HB protocol is just one human-computer security protocol that could be adapted to pervasive computing. There may be many other opportunities for cross-pollination where human-computer security could benefit from developments in pervasive computing security, or vice versa. Finding further parallels between the two could be an interesting line of research that yields efficient and practical security protocols.

6 Acknowledgments

This work was conducted at RSA Security. Thanks to Ari Juels and Mike Szydlo for contributing ideas and references.

References

[1] R. Anderson and M. Kuhn. Low Cost Attacks on Tamper Resistant Devices. In *International Workshop on Security Protocols*, volume 1361 of *Lecture Notes in Computer Science*, pages 125–136, 1997.

[2] G. Avoine. Privacy Issues in RFID Banknote Protection Schemes. In *Smart Card Research and Advanced Applications (CARDIS)*, pages 33–48, August 2004.

[3] E. R. Berlekamp, R. J. McEliece, and V. Tilborg. On the Inherent Intractability of Certain Coding Problems. *IEEE Transactions on Information Theory*, 24, 1978.

[4] A. Blum, M. Furst, M. Kearns, and R. J. Lipton. Cryptographic Primitives Based on Hard Learning Problems. In *Advances in Cryptology – CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 278–291, 1994.

[5] A. Blum, A. Kalai, and H. Wasserman. Noise-Tolerant Learning, the Parity Problem, and the Statistical Query Model. *Journal of the ACM*, 50(4):506–519, July 2003.

[6] F. Chabaud. On the Security of Some Cryptosystems Based on Error-Correcting Codes. In *Advances in Cryptology - EUROCRYPT*, volume 950 of *Lecture Notes in Computer Science*, pages 131–139, 1995.

[7] D. Chaum. Secret-Ballot Receipts: True Voter-Verifiable Elections. *IEEE Security and Privacy*, 2(1):38–47, January-February 2004.

[8] N. Courtois, M. Finiasz, and N. Sendrier. How to Achieve a McEliece-based Digital Signature Scheme. In *Advances in Cryptology - ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 157–174, 2001.

[9] J. M. Crawford, M. J. Kearns, and R. E. Shapire. The Minimal Disagreement Parity Problem as a Hard Satisfiability Problem. Technical report, Computational Intelligence Research Laboratory and AT&T Bell Labs, 1994.

[10] EPCglobal. Website. http://www.epcglobalinc.org/, 2004.

[11] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer. Strong Authentication for RFID Systems using the AES Algorithm. In *Cryptographic Hardware in Embedded Systems (CHES)*, 2004.

[12] C. Floerkemeier and M. Lampe. Issues with RFID Usage in Ubiquitous Computing Applications. In *Pervasive Computing (PERVASIVE)*, volume 3001 of *Lecture Notes in Computer Science*, pages 188–193, 2004.

[13] Food and Drug Administration. Combating counterfeit drugs. Technical report, US Department of Health and Human Services, Rockville, Maryland, Februrary 2004.

[14] S. L. Garfinkel. Adopting Fair Information Practices in Low-Cost RFID Systems. In *Ubiquitious Computing*, September 2002.

[15] O. Goldreich. *Foundations of Cryptography*, chapter 2.2.4.2, page 41. Cambridge University Press, 2000.

[16] Greentech Computing. GT6 Algorithm Solves the Extended DIMACS 32-bit Parity Problem. Technical report, Greentech Computing Limited, London, England, 1998.

[17] J. Håstad. Some Optimal Inapproximability Results. In *Symposium on Theory of Computing*, pages 1–10, 1997.

[18] J. Hecht. Casino chips to carry RFID tags. *New Scientist*, January 2004.

[19] D. Henrici and P. Müller. Hash-based Enhancement of Location Privacy for Radio-Frequency Identification Devices using Varying Identifiers. In *Pervasive Computing and Communications (PerCom)*, IEEE Computer Society, pages 149–153, 2004.

[20] N. Hopper and M. Blum. A Secure Human-Computer Authentication Scheme. Technical Report CMU-CS-00-139, Carnegie Mellon University, 2000.

[21] N. J. Hopper and M. Blum. Secure Human Identification Protocols. In *Advances in Cryptology - ASIACRYPT*, volume 2248 of *Lecture Notes in Computer Science*, pages 52–66, 2001.

[22] HumanAut. Carnegie Mellon University HumanAut Project. http://www.captcha.net/humanaut/, 2004.

[23] D. S. Johnson and M. A. Trick, editors. *Cliques, Coloring, and Satisfiability: Second DIMACS Implementation Challenge*, volume 26. American Mathematical Society, 1993.

[24] A. Juels. Minimalist Cryptography for RFID Tags. In *Security in Communication Networks*, 2004. To Appear.

[25] A. Juels. ”Yoking Proofs” for RFID Tags. In *Pervasive Computing and Communications Workshop*. IEEE Press, 2004.

[26] A. Juels and R. Pappu. Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121, 2003.

[27] A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *Computer and Communications Security*, pages 103–111. ACM Press, 2003.

[28] A. Juels and S. A. Weis. Authenticating Pervasive Devices with Human Protocols. In *In Submission*, 2005.

[29] M. Kearns. Efficient Noise-Tolerant Learning from Statistical Queries. *Journal of the ACM*, 45(6):983–1006, November 1998.

[30] S. Lacy. Inching Toward the RFID Revolution. *Business Week*, August 2004.

[31] L. Lamport. Password Authentication with Insecure Communication. *Communciations of the ACM*, 24(11):770–772, November 1981.

[32] F. MacWilliams and N. Sloane. *The Theory of Error-Correcting Codes*. North-Holland, 1977.

[33] T. Matsumoto. Human-computer Cryptography: An Attempt. In *Computer and Communications Security*, pages 68–75. ACM Press, 1996.

[34] T. Matsumoto and H. Imai. Huamn Identification through Insecure Channel. In *Advances in Cryptology - EUROCRYPT*, volume 547 of *Lecture Notes in Computer Science*, pages 409–421, 1991.

[35] R. J. McEliece. DSN Progress Report. Technical Report 42–44, JPL-Caltech, 1978.

[36] MIT RFID Privacy Workshop. http://www.rfidprivacy.org, November 2003.

[37] D. Molnar and D. Wagner. Privacy and Security in Library RFID : Issues, Practices, and Architectures. In *Computer and Communications Security*. ACM, 2004. To Appear.

[38] M. Naor and B. Pinkas. Visual Authentication and Identification. In *Advances in Cryptology - CRYPTO*, volume 1294 of *Lecture Notes in Computer Science*, pages 322–336, 1997.

[39] H. Niederreiter. Knapsack-Type Cryptosystems and Algebraic Coding Theory. *Problems of Control and Information Theory*, 15(2):159–166, 1986.

[40] M. Ohkubo, K. Suzuki, and S. Kinoshita. Efficient Hash-Chain Based RFID Privacy Protection Scheme. In *Ubiquitous Computing (UBICOMP)*, September 2004.

[41] M. Rivas. RFID Technology and Applications. RFID Privacy Workshop - http://www.rfidprivacy.org, November 2003.

[42] S. E. Sarma, S. A. Weis, and D. W. Engels. RFID Systems and Security and Privacy Implications. In *Workshop on Cryptographic Hardware and Embedded Systems*, volume 2523, pages 454–470. Lecture Notes in Computer Science, 2002.

[43] S. E. Sarma, S. A. Weis, and D. W. Engels. Radio Frequency Identification: Risks and Challenges. *CryptoBytes (RSA Laboratories)*, 6(1), Winter/Spring 2003.

[44] J. Stern. A New Paradigm for Public Key Identification. In *Advances in Cryptology - CRYPTO'93*, volume 773 of *Lecture Notes in Computer Science*, pages 13–21, 1993.

[45] J. Stern. A New Paradigm for Public Key Identification. *IEEE Transactions on Information Theory*, 42(6):1757–1768, 1996.

[46] P. Tollinger. A Secure, Device-Free, Challenge-Response Protocol. CMU Senior Thesis, 2000.

[47] United Nations. Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment, December 1984.

[48] I. Vajda and L. Buttyan. Lightweight Authentication Protocols for Low-Cost RFID Tags. In *Ubiquitious Computing (UBICOMP)*, 2003.

[49] C.-H. Wang, T. Hwang, and J.-J. Tsai. On the Matsumoto and Imai's Human Identification Scheme. In *EuroCrypt '95*, volume 921 of *Lecture Notes in Computer Science*, pages 382–392, 1995.

[50] J. P. Warners and H. van Maaren. A Two Phase Algorithm for Solving a Class of Hard Satisfiability Problems. *Operations Research Letters*, 23(3–5):81–88, 1999.

[51] S. A. Weis. Security and Privacy in Radio-Frequency Identification Devices. Master's thesis, Massachusetts Institute of Technology, Cambridge, MA 02139, May 2003.

[52] S. A. Weis, S. E. Sarma, R. L. Rivest, and D. W. Engels. Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In *Security in Pervasive Computing*, volume 2802 of *Lecture Notes in Computer Science*, pages 201–212, 2004.