Towards a Model for Security and Privacy in the Internet of Things

Saša Radomirović
Laboratory of Algorithmics, Cryptology and Security
University of Luxembourg
Luxembourg
Email: sasa.radomirovic@uni.lu

***Abstract*—We propose and give a high-level, work-in-progress description of a model which will allow us to reason about security and privacy of communication protocols in the Internet of Things and identify the next steps necessary towards a complete formal model.**

The model is built up from a few basic assumptions and observations on likely threats to security and privacy and with a focus on the latter.

We argue that from a security and privacy perspective, the Internet of Things is to be considered as a fusion of an operating system and a network.

I. Introduction

The *Internet of Things* refers in this article to a communication network which extends the present Internet by including everyday items and sensors. The technology used to network these items will likely consist of *Radio Frequency Identification* (RFID) tags attached to cheap and disposable objects and more powerful radio transmitters integrated into large and valuable objects. By means of the RFID tags, any physical object receives a unique digital identity. Information about a tagged object can be stored on the RFID tag itself or in a database. The RFID tagged items' presence and properties are registered by static or mobile RFID readers. The RFID reader's network connection thus extends to the physical object. In addition to the RFID readers, several types of sensors, such as temperature and light sensors, fire and motion detectors, video cameras and biometric scanners are expected to become omnipresent and connected to a local communication network.

The simple fact that the presence of hundreds of RFID tags can be registered nearly instantly by a single RFID reader without a direct line of sight has greatly improved the efficiency of supply chain management. Equipping homes with RFID readers is expected to promote applications ranging from smart appliances to remotely managed health care and promises a more convenient and safer lifestyle. For instance, RFID equipped items could lead to more safety by preventing accidental as well as intentional confusion of products.

However, the continuing effort to connect and network every aspect of our lives comes at a price, too. The pervasiveness of RFID tags and increased access to RFID readers in the Internet of Things will make it possible to cheaply collect and cross-reference a vast amount of data in order to infer sensitive personal information. Unless adequate mechanisms are put in place, this will lead to yet another source of information about our movements, health, and habits.

Perhaps even more significantly, unexpected functionalities and security flaws are almost certain to exist in some sensors, RFID readers, and RFID tags. Several such vulnerabilities are likely to remain unnoticed or uninteresting for a long time, because the context necessary in order to exploit them will not be present yet. We have seen such a development in the present Internet already. The importance of security flaws in operating systems has only become significant once the general public started connecting the personal computer to the Internet.

Once the connectivity of the Internet of Things becomes large enough, that is, once there are sufficiently many networked sensors, RFID readers, and RFID equipped objects in place, lingering flaws will suddenly lead to nontrivial and possibly dramatic threats. This effect can be seen as a consequence of the phase transition property of a large random graph. A similar effect has been observed in software systems and referred to as the *honeymoon effect* [1].

In this paper, we aim to sketch an adversary model for communication protocols in the Internet of Things. To anticipate the capabilities of such an adversary, we consider a network which we call the *dense Internet of Things*. The two key features of this network are its high degree of connectivity and the assumption that every commonplace functionality is ubiquitous. These two assumptions are a consequence of our attempt to predict the implications of the next phase transition the Internet will go through. The main new feature of the adversary, and at present the least developed one, is his ability to invade privacy.

Specifically, our contributions are as follows. Based on existing research, we outline what the implications of the Internet of Things might be for privacy and we discuss how to defend against loss of privacy. We then present the dense Internet of Things model and its adversary model as a consequence of a few basic assumptions and the conclusions of the preceding sections.

Our paper is organized as follows. In the following section we aim to convey our intuition on applications which might exist in the Internet of Things. In Section III we discuss privacy issues and in Section IV methods to defend against the erosion of privacy. In Section V we present the dense Internet of Things model and the adversary model. We discuss

related open research questions in Section VI and conclude in Section VII.

II. Intuition

A. Applications

At present, items are principally equipped with communication capabilities for a clear purpose and with a specific scenario in mind. For instance, lamps and other home appliances can be operated through the home network, motion and fire detectors can report activity to a specific network address. RFID tags are attached to merchandise, library books and airline baggage for sorting and tracking purposes, built into keys for access control to automobiles and buildings. Medicine and luxury items are receiving RFID tags to support anti-counterfeiting measures. A variety of communication technologies is used for highway toll payment and road pricing.

Over time, as the number of items that can be remotely controlled or queried increases, unexpected applications start to emerge. To give a mostly academic example, suppose agricultural products are RFID tagged for automated processing and quality control. Thus, a milk container's RFID tag would contain information regarding the fat content in the milk, a particular expiration date, and a code linking its provenance to a particular farm. As a consequence of a multitude of products being RFID tagged, refrigerators equipped with RFID readers are marketed. The intended purpose of such refrigerators would be to report on quantity and expiration dates of products within them. Customers may see an added value in the fact that they can query their home refrigerator remotely. Grocery chains may value the fact that they can peek into a customer's refrigerator in exchange for offering discounted products. An unanticipated application in this scenario could be the emergence of services which track reports on contaminated food and query a customer's refrigerator in order to determine whether the customer needs to be warned about a particular item in the refrigerator.

For the future, we can expect that items will be equipped with wireless communication abilities as a matter of course and with a less specific purpose. Inventions will be made based on the fact that communicating items are ubiquitous. To continue the academic example, if smart refrigerators become popular, RFID-equipped cabinets will be introduced next, leading to an even greater number of RFID tagged products. Smart robots taking care of household chores will be designed, not with specific items in mind, but taking advantage of the fact that nearly every item in the household can identify itself.

B. Impact on Security and Privacy

We have argued above that items currently designed for a specific purpose will be used in a new context, that items will be given communication capabilities without a specific purpose, and that eventually communicating items will be ubiquitous. This three-step development will almost certainly be accompanied by security and privacy breaches. By changing the context in which an item operates or by creating a specific context not envisioned by design, hidden flaws may get exposed and unwanted side-effects may occur. The simultaneous transition from few, isolated, and local communicating items to ubiquitous, fully networked communicating items, has the potential to turn harmless protocol flaws into critical flaws.

We have already experienced such a three-step development with the rise and growth of the Internet and witnessed its strong impact on security. In retrospect, we see how initial, isolated attacks on Internet hosts for amusement and political statements have evolved into coordinated attacks for profit and led to a veritable black market supply chain in which information on vulnerabilities is offered for sale and control over botnets is for rent.

In comparison, threats to the privacy of Internet users have only recently begun to receive considerable attention. We expect that attacks on privacy will become more popular with the growth of the Internet of Things, since an increasing number of personal items will be reachable for queries and intrusions. In the following section, we will therefore focus on recent developments regarding privacy in communication protocols and technologies to fingerprint electronic devices.

III. Fingerprinting and profiling

We define fingerprinting as the measuring of an identifying characteristic of an individual or a physical or digital item. We define profiling as the analysis of measurements of several characteristics of an individual or a physical or digital item, potentially over an extended period of time.

While the Internet of Things will consist of a variety of communicating devices, cost and energy considerations dictate that a significant number of these devices will be passively powered RFID tags. Unlike actively powered communication devices, by design passive RFID tags have no choice but to respond to an RFID reader's query.

To fingerprint an RFID tag, it frequently suffices to merely query it for its ID. The ability to fingerprint an RFID tag violates what is known as RFID privacy or untraceability. A large number of RFID protocols have been proposed aiming to achieve RFID privacy. A significant number of these protocols is later shown to be flawed and it is known from work of Vaudenay [2], Paise and Vaudenay [3] as well as Damgård and Pedersen [4] that there are trade-offs between strong privacy and authentication. Aside from flawed communication protocols, methods to distinguish between RFID tags based on hardware implementations have been reported [5], [6]. Analogous methods are conceivable to fingerprint any communication device. Van Deursen [7] demonstrates that even if application, protocol, and hardware are perfectly privacy preserving, an attacker can still trace individuals with an *RFID profiling* attack. The idea behind this attack is that a particular person is likely to carry the same set of RFID tags over time, while different individuals are likely not to have the same number or same type of tags on them.

Van Deursen's attack is analogous to the Internet browser fingerprinting attack reported in [8] and showing that nearly all Internet browsers can be fingerprinted. But these are by far not

the only methods to fingerprint an individual or a device. As reported in [8], cameras, typewriters, and quartz crystal clocks have been shown to possess small but measurable variations. In other works, researchers have successfully distinguished individuals by their Internet browsing history [9], their speech patterns in encrypted but variable bit-rate encoded voice-over-ip traffic [10], their wireless sensors at home [11], or even their fingerprint bacteria found on a keyboard [12]. Thus we are seeing an increasing number of technologies and methods to identify, track, correlate, and profile individuals and devices. Today's advances in forensics are tomorrow's fingerprinting and profiling technologies.

Fingerprinting by applying any of the aforementioned methods can be considered a passive attack in that the item or individual is voluntarily (or by nature) exhibiting a particular characteristic. But even in cases where no such characteristic can be measured, an adversary may flag or mark his target in order to be able to fingerprint it. It suffices to attach an RFID tag to the target.

Thus, it can be expected that in the future fingerprinting an area, a household, an individual, or an item will become easier.

IV. Defensive measures

A. An operating system analogy

To defend against fingerprinting attacks, specific countermeasures will need to be taken, but novel ways to measure the characteristics of various devices will be developed. This arms race can be seen in analogy to operating system security.

The measures to keep operating systems secure include filtering and scanning techniques such as firewalls and malware scanners. We argue that in the Internet of Things it will be necessary to apply the same techniques in order to maintain privacy and as a consequence improve security.

We will have to expect that malicious items can be introduced into our vicinity or household with the purpose to fingerprint or infiltrate our *private space*. The Trojan horse will thus become a physical object again. Advertising pamphlets and other junk mail might contain RFID tags, larger advertising gifts might even contain RFID readers. Viruses may be introduced by swapping items or possibly by just being near each other. The mere presence of another person may affect one's home network. The trust we extend to a visitor or a gift will be analogous to the trust settings we apply to somebody's email attachment.

B. Specific measures

As defensive measures, Faraday cages connected to the outside world through a wired gateway might seem extreme at this point in time, but could become as natural as networking firewalls are today. Alternatively, all wireless traffic will need to be monitored and incoming items scanned for communication abilities.

In the opposite direction, any item that has been in our private space could contain private information thus it would need to be scanned and cleared before it may be released. In particular, such scans may even have to be applied to ourselves as we might have been sprinkled with RFID dust in order to be traced through a shop or to our home.

Many such specific scenarios are conceivable. However, regardless of whether any given scenario is at present considered to be plausible, it is clear that all communication must be secured equally, be it near-field communication confined to a private space or long-distance communication.

V. The dense Internet of Things model

In order to reason about security and privacy in a future Internet of Things we are proposing a model which is a limit point of our present expectation that eventually

- every item will be connected and able to communicate with any other item and
- every "commonplace" functionality[1] will be ubiquitously present.

We refer to this model as the *dense Internet of Things* model.

While such a highly connected network and ubiquitous functionality may never become reality, for each attack one discovers in the model, there is a certain connection threshold and constellation of devices which enables the attack. Thus as the connectivity of the Internet of Things increases, eventually a point in time will be reached at which an attack becomes feasible.

A. Assumptions

1) Communication: Our basic assumptions are that wireless communication is ubiquitous and that there is a communication path between any two devices. We assume that all items carrying information have equal communication abilities and, in particular, are able to communicate with each other. Thus, for instance, we do not distinguish between a passive RFID tag and a networked computer. All items are assumed to be able to respond to or initiate a communication protocol.

This assumption is a consequence of our attempt to capture the state the Internet of Things is aiming for. For instance, it allows a milk container to initiate a communication with a smart phone to indicate that the expiration date is near. We believe this to be a sufficiently accurate approximation to the more realistic scenario of the smart refrigerator scanning the milk container and reporting the expiration date to the smart phone.

The assumptions this far allow us to model the Internet of Things as a fully connected asynchronous communication network.

2) Items and households: We make the simplifying assumption that there are two types of devices, mobile devices and static devices.[2] For instance, a smart refrigerator would typically be a static device while a smart phone would be a

[1] What constitutes a commonplace functionality is debatable and subject to change. Examples of what we presently would expect to become commonplace functionalities are RFID readers, biometric scanners, and smoke and motion detectors.

[2] Instead of the discrete mobile/static distinction, in a continuous model one could assign probabilities to items to be within a certain perimeter of a particular location.

mobile device. This distinction is irrelevant from a classical security of communication protocols point of view, since we assume any two items to be able to communicate with each other. It allows us, however, to simplify the modeling of corruption (discussed below) and introduces the ability to model *hardware tokens*. Hardware tokens are uncloneable items which could be used in authentication protocols as well as for "proofs of presence". Biometric features of people can be uniformly modeled, for instance, by considering individuals as hardware tokens. Examples of other items that can be considered hardware tokens are (RFID tagged) passports and public transportation tickets.

We can bundle several static devices and consider them to be part of one "household". As discussed in the preceding section, we may consider a household to be analogous to the operating system of a computer. The devices comprising a household correspond to the operating system's applications. A household can be infiltrated by "trojan" items which spy on and leak information about household items or cause household items to malfunction.

B. Adversary

1) Communication: In the present paper, we make assumptions which permit us to ignore the resources an adversary needs to expend in order to attack a system. This corresponds to how the security of communication protocols is analyzed in symbolic formal models such as the applied pi calculus [13], the extended Cremers-Mauw model [14], the strand spaces model [15] or CSP [16]. Thus we assume, for instance, that the cost of deploying communication devices as well as the cost of communication itself is negligible for the adversary. In a more accurate model, such costs would be considered in a manner analogous to the computational model of an adversary used in cryptography. That is, security guarantees are stated relative to the adversary's cost to successfully attack the system.

Our simplification allows us to assume that the communication network is controlled by a Dolev-Yao adversary [17], that is an adversary capable of blocking communication channels, eavesdropping on communication channels, and injecting arbitrary messages into the communication channels. These capabilities are justified by the fact that a suitably placed rogue device can jam signals, communicate with any device within a certain range and forward communication to any other device controlled by the adversary in the network. As a consequence of the negligible cost of deploying communication devices, an adversary will eventually succeed in placing a communication device at any location, unless specific precautions, such as the ones discussed in the preceding section, are taken. Simple examples for deploying rogue communication devices involve mailing a letter with an embedded rogue device or giving away "Trojan" items.

2) Corruption and Fingerprinting: Any item may be corrupted and turned into an item controlled by the adversary. We refer to such an item as a *malicious item* and we assume that all cryptographic keys of the item are known to the adversary. To emphasize that an item is not malicious we may refer to it as an *honest item.*

By bundling several static devices into one household, we can simplify the modeling of complex systems. The intra-household communication is assumed to be secure unless it has been corrupted.

We distinguish two forms of corruption of households. A *weak* corruption allows the adversary to control the communication network of the household, that is, the adversary has Dolev-Yao capabilities.

A *strong* corruption of a household allows the adversary to control the devices of a household, thus turning some of the devices into malicious items.

A novel ability the adversary is equipped with are *passive* and *active fingerprinting* of a household or item in the sense defined in Section III. This gives the adversary the ability to infer which items belong together or to the same user.

With this ability we are trying to model the fact that erosion of privacy aggravates security problems. It is an abstract analogue of both the fact that perpetrators increasingly use private information about their victims in order to carry out sophisticated social engineering attacks on the Internet today as well as the fact that planning and execution of physical attacks are simplified.

The corruption and fingerprinting abilities allow us to abstract away from the precise method used to achieve an intrusion.

VI. Related Work and Open Problems

A. Threats and density thresholds

As the work of Clark et al. [1] shows, security flaws in software systems may be dormant for a period of time (the "honeymoon") before they are being widely exploited. We believe this to be an example of a phase transition effect which is applicable to other systems as well. These effects are easy to spot in retrospective. Their analysis might lead to a better understanding of what to look out for when designing new systems, particularly large systems such as the Internet of Things whose emerging behavior is hard to predict.

B. Formal model

Formal verification methods are an invaluable tool for identifying weaknesses in security protocols. To formally verify whether a communication protocol satisfies a certain security property, one creates a model which specifies what powers an adversary is given, how the adversary interacts with his environment, and what the definition of the security property within the model is. There are several different symbolic formal models in use, for instance [13], [14], [15], [16] mentioned in Section V-B and automatic tools to verify a wide range of security protocols, such as ProVerif [18] and AVISPA [19].

We have sketched an initial adversary model for the dense Internet of Things based on the classical Dolev-Yao adversary [17] . It specifies the adversary's abilities to control

network communication and corrupt items. We have also given the adversary fingerprinting abilities.

Natural questions to ask are, whether there are restrictions or other abilities an adversary should have in the Internet of Things. The adversary model of Schaller et al. [20] considers, for instance, time and network topology as limiting factors for the adversary. In addition to these, we may need to define the adversary's abilities to manipulate hardware tokens. Examples of such abilities are the stealing, duplication, and modification of tokens.

A bigger task is to develop a full formal security and privacy model for the dense Internet of Things. A starting point could be the work on RFID system security and privacy. Computational models for security and privacy of RFID systems have been proposed by Vaudenay [2], Paise and Vaudenay [3], and Damgård and Pedersen [4]. A symbolic formal model and operational semantics for RFID systems have been developed by Van Deursen et al. [21], [14].

C. Hardware tokens

At present, all of the formal models mentioned lack support for hardware tokens. We have merely postulated the existence of mobile and static items and their usefulness in security protocols. While no comprehensive formal treatment of hardware tokens exists, several specific aspects related to the security of systems have been considered. The fact that RFID tags are hardware tokens, together with a manufacturing method that is believed to create physically uncloneable functions on RFID tags, has led to protocols which provide anti-counterfeiting measures [22], [23], [24], [25]

In distance-bounding protocols [26], physical properties of mobile wireless devices are used for proofs of presence. Several RFID distance-bounding protocols have been proposed [27], [28], [29], [30], and a discussion of location privacy in distance-bounding applications as well as a protocol providing location privacy while allowing distance bounding have been presented in [31]. A cryptanalytical framework for distance-bounding protocols has been developped in [32]. Meadows et al. [33] have developed a framework for verifying distance-bounding protocols in by extending the authentication and secrecy logics [34] and [35].

Hardware tokens have also been the tool for and target of attacks. The potential loss of privacy due to traceability of RFID tags and other mobile wireless devices is well-known and has sparked a vast amount of research into untraceability [36], [2], [37]. Side channel attacks have been considered since the inception of smart cards. Such attacks have recently been modeled from an information-theoretic point of view [38]. Several examples of hardware tokens being abused as a tool for attacks can be found in the works of Cambridge's security group, e.g. [39], [40]. An extortion attack based on disabling RFID tags due to a flawed protocol has been given in [41].

VII. Conclusion

We have argued that privacy will be very hard to protect in the Internet of Things, but that it will aggravate security problems. By drawing an analogy to the development of the Internet, we see the risk that the future Internet of Things will suffer from security and privacy threats due to legacy devices.

We have proposed the dense Internet of Things model which consists of an asynchronous communication network and a Dolev-Yao adversary with fingerprinting abilities. We distinguish between mobile and static devices. Static devices remain within a certain perimeter and are considered to be part of a system which much like today's operating systems needs to be actively scanned and protected against intrusion. Mobile devices have the additional property of being useful for applications related to proofs of presence and proofs of possession.

Thus to reason about security and privacy in the Internet of Things, it seems helpful to consider it as a fusion of an operating system and a communication network. In order to maintain privacy and security an individual's private space ought to be considered akin to an operating system. Incoming and outgoing items, as well as the private space itself need to be scanned for rogue devices and malicious software. We have argued that communication between devices should be considered to be taking place under the control of a Dolev-Yao adversary.

References

[1] S. Clark, S. Frei, M. Blaze, and J. Smith, "Familiarity breeds contempt: The honeymoon effect and the role of legacy code in zero-day vulnerabilities," in *26th Annual Computer Security Applications Conference (ACSAC 2010)*, 2010, to appear.

[2] S. Vaudenay, "On privacy models for RFID," in *Advances in Cryptology - ASIACRYPT 2007*, ser. Lecture Notes in Computer Science, vol. 4833. Kuching, Malaysia: Springer-Verlag, December 2007, pp. 68–87.

[3] R.-I. Paise and S. Vaudenay, "Mutual authentication in rfid: security and privacy," in *ASIACCS '08: Proceedings of the 2008 ACM symposium on Information, computer and communications security*. New York, NY, USA: ACM, 2008, pp. 292–299.

[4] I. Damgård and M. Ø. Pedersen, "RFID security: Tradeoffs between security and efficiency," in *CT-RSA*, 2008, pp. 318–332.

[5] T. Chothia and V. Smirnov, "A Traceability Attack Against e-Passports," in *14th International Conference on Financial Cryptography and Data Security – FC'10*, ser. Lecture Notes in Computer Science. Springer, 2010.

[6] S. C. G. Periaswamy, D. R. Thompson, and H. P. Romero, "Fingerprinting Radio Frequency Identification Tags Using Timing Characteristics," in *Workshop on RFID Security – RFIDSec Asia'10*, ser. Cryptology and Information Security, Y. Li and J. Zhou, Eds., vol. 4. Singapore, Republic of Singapore: IOS Press, February 2010, pp. 73–81.

[7] T. v. Deursen, "50 ways to break RFID privacy," University of Luxembourg, Technical Report, 2010. [Online]. Available: http://satoss.uni.lu/papers/D10.pdf

[8] P. Eckersley, "How unique is your web browser?" in *Privacy Enhancing Technologies, 10th International Symposium, PETS 2010*, ser. Lecture Notes in Computer Science, vol. 6205. Springer, 2010, pp. 1–18.

[9] A. Janc and L. Olejnik, "Feasibility and real-world implications of web browser history detection," in *W2SP 2010: Web 2.0 Security and Privacy 2010*, 2010. [Online]. Available: http://w2spconf.com/2010/papers/p26.pdf

[10] C. V. Wright, L. Ballard, S. E. Coull, F. Monrose, and G. M. Masson, "Spot me if you can: Uncovering spoken phrases in encrypted voip conversations," in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2008, pp. 35–49.

[11] V. Srinivasan, J. Stankovic, and K. Whitehouse, "Protecting your daily in-home activity information from a wireless snooping attack," in *UbiComp '08: Proceedings of the 10th international conference on Ubiquitous computing*. New York, NY, USA: ACM, 2008, pp. 202–211.

[12] N. Fierer, C. L. Lauber, N. Zhou, D. McDonald, E. K. Costello, and R. Knight, "Forensic identification using skin bacterial communities," *Proceedings of the National Academy of Sciences*, vol. 107, no. 14, pp. 6477–6481, 2010.

[13] M. Abadi and C. Fournet, "Mobile values, new names, and secure communication," in *POPL*, 2001, pp. 104–115.

[14] T. v. Deursen, S. Mauw, S. Radomirović, and P. Vullers, "Secure ownership and ownership transfer in RFID systems," in *Proc. 14th European Symposium On Research In Computer Security (ESORICS'09)*, ser. Lecture Notes in Computer Science, vol. 5789. Springer, 2009, pp. 637–654.

[15] F. Thayer Fàbrega, J. C. Herzog, and J. D. Guttman, "Strand spaces: Why is a security protocol correct?" in *Proc. 1998 IEEE Symposium on Security and Privacy*, Oakland, California, 1998, pp. 66–77.

[16] P. Ryan and S. Schneider, *The modelling and analysis of security protocols: the CSP approach*. Pearson Education Limited, 2001.

[17] D. Dolev and A. Yao, "On the security of public key protocols," *IEEE Transactions on Information Theory*, vol. IT-29, no. 2, pp. 198–208, Mar. 1983.

[18] B. Blanchet, "An efficient cryptographic protocol verifier based on prolog rules," in *Proc. 14th IEEE Computer Security Foundations Workshop*. IEEE Computer Society, 2001, pp. 82–96.

[19] A. Armando, D. A. Basin, Y. Boichut, Y. Chevalier, L. Compagna, J. Cuéllar, P. H. Drielsma, P.-C. Héam, O. Kouchnarenko, J. Mantovani, S. Mödersheim, D. von Oheimb, M. Rusinowitch, J. Santiago, M. Turuani, L. Viganò, and L. Vigneron, "The AVISPA tool for the automated validation of internet security protocols and applications," in *CAV*, 2005, pp. 281–285.

[20] P. Schaller, B. Schmidt, D. Basin, and S. Capkun, "Modeling and verifying physical properties of security protocols for wireless networks," in *22nd IEEE Computer Security Foundations Symposium*. IEEE Computer Society Washington, DC, USA, 2009, pp. 109–123.

[21] T. v. Deursen, S. Mauw, and S. Radomirović, "Untraceability of RFID protocols," in *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, ser. Lecture Notes in Computer Science, vol. 5019. Seville, Spain: Springer, 2008, pp. 1–15.

[22] H. Balinsky, E. McDonnell, L. Chen, and K. Harrison, "Anti-Counterfeiting using Memory Spots," in *Workshop on Information Security Theory and Practice – WISTP'09*, ser. Lecture Notes in Computer Science, vol. 5746. Brussels, Belgium: Springer, September 2009, pp. 52–67.

[23] S. Devadas, E. Suh, S. Paral, R. Sowell, T. Ziola, and V. Khandelwal, "Design and Implementation of PUF-Based "Unclonable" RFID ICs for Anti-Counterfeiting and Security Applications," *IEEE International Conference on RFID*, pp. 58–64, April 2008.

[24] P. Tuyls and L. Batina, "Rfid-tags for anti-counterfeiting," in *CT-RSA*, ser. Lecture Notes in Computer Science, vol. 3860. Springer, 2006, pp. 115–131.

[25] A. Juels and S. Weis, "Authenticating pervasive devices with human protocols," in *Advances in Cryptology – CRYPTO'05*, ser. Lecture Notes in Computer Science, V. Shoup, Ed., vol. 3126, IACR. Santa Barbara, California, USA: Springer-Verlag, August 2005, pp. 293–308.

[26] S. Brands and D. Chaum, "Distance-bounding protocols (extended abstract)," in *EUROCRYPT*, 1993, pp. 344–359.

[27] G. Hancke and M. Kuhn, "An RFID Distance Bounding Protocol," in *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm 2005*, IEEE. Athens, Greece: IEEE Computer Society, September 2005, pp. 67–73.

[28] Y.-J. Tu and S. Piramuthu, "RFID Distance Bounding Protocols," in *First International EURASIP Workshop on RFID Technology*, Vienna, Austria, September 2007. [Online]. Available: http://www.eurasip.org/Proceedings/Ext/RFID2007/pdf/s5p2.pdf

[29] C. H. Kim and G. Avoine, "Rfid distance bounding protocol with mixed challenges to prevent relay attacks," in *Cryptology and Network Security, 8th International Conference, CANS 2009, Kanazawa, Japan, December 12-14, 2009. Proceedings*, ser. Lecture Notes in Computer Science, J. A. Garay, A. Miyaji, and A. Otsuka, Eds., vol. 5888. Springer, 2009, pp. 119–133.

[30] C. H. Kim, G. Avoine, F. Koeune, F.-X. Standaert, and O. Pereira, "The swiss-knife rfid distance bounding protocol," in *Information Security and Cryptology - ICISC 2008, 11th International Conference, Seoul, Korea, December 3-5, 2008, Revised Selected Papers*, ser. Lecture Notes in Computer Science, P. J. Lee and J. H. Cheon, Eds., vol. 5461. Springer, 2009, pp. 98–115.

[31] K. B. Rasmussen and S. Čapkun, "Location privacy of distance bounding protocols," in *CCS '08: Proceedings of the 15th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2008, pp. 149–160.

[32] G. Avoine, M. A. Bingöl, S. Kardaş, C. Lauradoux, and B. Martin, "A Framework for Analyzing RFID Distance Bounding Protocols," *Journal of Computer Security – Special Issue on RFID System Security*, 2010, to appear.

[33] C. Meadows, R. Poovendran, D. Pavlovic, L. Chang, and P. Syverson, "Distance bounding protocols: Authentication logic analysis and collusion attacks," in *Secure Localization and Time Synchronization for Wireless Sensor and Ad Hoc Networks*, ser. Advances in Information Security, R. Poovendran, S. Roy, and C. Wang, Eds. Springer US, 2007, vol. 30, pp. 279–298.

[34] I. Cervesato, C. Meadows, and D. Pavlovic, "An encapsulated authentication logic for reasoning about key distribution protocols," in *Proceedings of CSFW 2005*, J. Guttman, Ed. IEEE, 2005, pp. 48–61.

[35] D. Pavlovic and C. Meadows, "Deriving secrecy in key establishment protocols," in *Proceedings of ESORICS 2006*, ser. Lecture Notes in Computer Science, D. Gollmann, J. Meier, and A. Sabelfeld, Eds. Springer Berlin / Heidelberg, 2006, vol. 4189, pp. 384–403.

[36] G. Avoine, "Adversary model for radio frequency identification," Swiss Federal Institute of Technology (EPFL), Security and Cryptography Laboratory (LASEC), Lausanne, Switzerland, Technical Report LASEC-REPORT-2005-001, September 2005.

[37] A. Juels and S. Weis, "Defining strong privacy for RFID," in *International Conference on Pervasive Computing and Communications – PerCom 2007*, IEEE. New York, USA: IEEE Computer Society Press, March 2007, pp. 342–347.

[38] B. Köpf and D. Basin, "Automatically deriving information-theoretic bounds for adaptive side-channel attacks," *Journal of Computer Security*, 2010, to appear.

[39] S. Drimer, S. J. Murdoch, and R. J. Anderson, "Thinking inside the box: System-level failures of tamper proofing." in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2008, pp. 281–295.

[40] ——, "Optimised to fail: Card readers for online banking." in *Financial Cryptography*, ser. Lecture Notes in Computer Science, R. Dingledine and P. Golle, Eds., vol. 5628. Springer, 2009, pp. 184–200.

[41] T. v. Deursen and S. Radomirović, "Security of an RFID protocol for supply chains," in *ICEBE '08: Proceedings of the 2008 IEEE International Conference on e-Business Engineering*. Washington, DC, USA: IEEE Computer Society, 2008, pp. 568–573.