Some Unresolved Concerns & Future Directions for Resilient RFID Smart Structures in the Supply Chain

Jorge Munilla Fajardo
Dpt. Ing. de Comunicaciones. E.T.S.I. Telecomunicación
Campus de Excelencia Internacional Andalucía Tech. UMA
Málaga, Spain
munilla@ic.uma.es

Mike Burmester
Department of Computer Science.
Florida State University
Tallahassee (FL), USA
burmester@cs.fsu.edu

***Abstract*— Smart structures are highly interconnected adaptive systems that are coordinated by cyber systems to optimize specific system objectives. To capture realistic IoT scenarios we must employ threat models that allow untrusted behavior and address system vulnerabilities, exploits and attack vectors. Resilience is defined in terms of stability, resistance to damage and self-healing. In this paper we analyze the challenges of establishing resilience for smart structures by considering the supply chain paradigm. For this, RFID tagged objects in pallets are scanned by RFID readers and tag ownership is transferred from a current to a new owner. This involves untrusted readers inspecting pallets and identifying missing objects, without being able to trace tagged objects via unauthorized inspections, and the privacy of owners.**

Keywords*— *Smart Structures, Supply Chain, Logistics, IoT, Ownership Transfer, Grouping-Proofs, Grouping-Codes.

I. INTRODUCTION

The Internet of Things (IoT) links identifiable objects to their virtual representation on the Internet making it possible for an end user (process) to monitor and link the objects to additional information regarding their status for efficient control, management and logistics. This extends the scope of the Internet making it possible to control smart systems and structures. In this paper we consider some of the challenges of protecting such applications. To analyze these challenges, we consider a particular application that involves ownership transfer and scanning delegation in the supply chain.

The paper is organized as follows. In Section 2 we model smart structures as tightly coupled ecologies and define resilience in terms of survivability and self-healing. We then introduce the use of RFID for dynamic logistics and supply chain management in Section III and consider two applications: ownership transfer, in Section IV, and group scanning (grouping proofs/codes) in Section V, and show how to capture resilience. We conclude in Section VI.

II. SMART STRUCTURES

Smart structures are highly interdependent systems that integrate a tightly coupled mixed-latency ecology consisting of physical systems (sensors, embedded devices, etc.), social systems (operators, customers), financial systems (procurement/ acquisition, etc.) and the environment, that are coordinated by cyber systems so as to optimize specific system objectives based on their properties and constraints, as well as their current and estimated state (Figure 1). Because of the interdependencies, failure in any one of the components may have a ripple (or cascade) effect on others and lead to infrastructure disruption with potentially disastrous impact on the services provided. Protection must ensure continuity of service, requiring real-time control, and resist a formidable array of natural and man-made hazards that include bad/faulty design, cyberspace attacks and terrorist acts. This shifts the focus of smart structure protection towards resiliency, accentuating self-healing and survivability behavior.

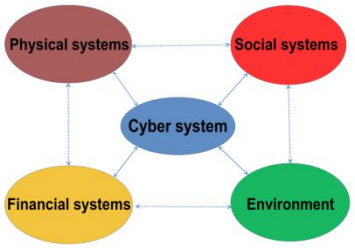

Fig. 1. An infrastructure ecology.

A. Threat Model, Resilience

Any attempt to provide holistic protection for highly interdependent smart structures will fail because of their complexity. The best we can aim for is risk management and threat mitigation. Reliability typically refers to the proper functioning of the structure, as defined by its specifications and policies, and captures fault-tolerance.

There are several definitions that describe different aspects of resilience, depending on the applications. For engineering systems, resilience requires constancy, predictability and stability near an equilibrium steady state; for social systems, a balance of self-organizing systems; and for environmental systems, resistance to damage and quick response to natural perturbation/disturbances.

This material is partly based upon work supported by: Universidad de Málaga, Campus de Excelencia Internacional Andalucía Tech, MINECO and FEDER under project TEC2014-54110-R and NSF under grant numbers CNS 1347113, DUE 1241525, 1027217 and DGE 1538850.

The UC-formalization [1] can be used to analyze the vulnerabilities of interdependent applications and is ideally suited for studying the threats of a system from a holistic point of view. This models all parties, including adversarial parties, by efficient processes (probabilistic polynomial-time Turing machines) and uses a real world simulation to model the actual behavior of the system in the presence of a malicious (Byzantine) adversary A, and an ideal world simulation to model the protected behavior of the system, in which a trusted functionality F enforces its protection policies. In the real world the adversary A controls the communication channels between all parties: A may replay, modify/drop or fabricate messages. In the ideal world the tasks of non-compromised parties are executed by the functionality F that enforces the specifications and policies of the infrastructure, with the adversary replaced by an ideal adversary A' that emulates A. For UC-security, the two simulations should be indistinguishable by any efficient process (the environment). Although the UC formalization is too restrictive for analyzing the resilience of most smart structures, it still can be used to describe specific security features such as privacy, forward/backward secrecy and integrity.

Resilience is established by enforcing security policies to protect system resources. This requires developing security assessment policies as well as procedures, testing methodologies and tools to identify system vulnerabilities. Testing must include static and dynamic threat analysis, and cover intentional and unintentional vulnerabilities including, for example, malicious code, malicious processes, defective software and counterfeits. Next, we consider the smart structure for supply chain in two particular applications: ownership transfer and group scanning.

III. RFID FOR DYNAMIC LOGISTICS AND SUPPLY CHAIN MANAGEMENT

Radio Frequency Identification (RFID) is a wireless technology widely deployed for logistics and supply chain management. There are several advantages of RFID over barcode technology: RFID does not require line-of-sight alignment, RFID tags (in particular UHF tags) can be interrogated at greater distances, faster and concurrently, and RFID technology enables computers to observe/identify/ understand for situational awareness without the limitations of a human in the loop. In particular, RFID extends the scope of the Internet of computers to capture ubiquitous applications involving smart devices, intelligent processes and cyber-physical applications [2].

A typical RFID deployment involves three types of legitimate entities: RFID tags, readers and back-end servers. RFID tags are attached to, or embedded in, host objects to be identified. The most common low cost tags are passive UHF tags. They have no power of their own and get power from the radio waves of the reader. UHF tags operate in the far field and use backscattering, which allows them to work at greater distance (several meters), but the deliverable power is low and only lightweight communication and computation tools can be used. RFID tags with inductive coupling (near field) have restrictive ranges; for example, the operating range of tags in the LF band (125 kHz) is around 1.5 m, while that of tags in the HF band is between 10 cm (ISO-14443) and 70 cm (ISO-15693). However, inductive coupling enables much higher levels of available power, which allows the implementation of complex cryptographic primitives, suitable for applications such as mobile payment, electronic tickets etc., that require physical proximity.

RFID readers have resources at least comparable to those of a cellphone. They implement a radio interface to the tags and a high-level interface to a back-end server that processes captured data. Back-end servers are trusted entities that maintain a database containing all information needed to identify tags. Since the integrity of an RFID system depends entirely on the proper behavior of the server, back-end servers should be physically secure. Servers and readers are sometimes treated as a single entity.

Although initial RFID technology focused on performance and efficiency, it is now used in applications that require the implementation of security mechanisms. The recent ratification of the EPCGen2v2 standard highlights these concerns [3]. Several RFID authentication protocols that address security have been proposed in the literature. Most use hash functions [4], [5], and [6], while others use pseudorandom functions [7], [8]. The Flyweight authentication protocol [9] is one of a few that only uses a pseudorandom number generator.

Apart from identification, clearly there are other security concerns that have to be addressed. For example, who "owns" (has ownership rights) or controls the identified objects (integrity) and who has access to the records, or may track/ monitor objects (privacy)? In this paper we investigate IoT applications that involve the management (integration) of the supply chain of RFID tagged physical objects.

IV. OWNERSHIP TRANSFER PROTOCOLS

A. Definition and security requirements

Ownership transfer protocols (OTP) enable the transfer of ownership rights of a collection G of tagged objects from the current owner Own_c to a new owner Own_n. The following entities participate in an OTP:

G: The collection of tagged objects whose ownership rights will be transferred.

Own_c: The current owner or seller. At the beginning of the OTP only this entity can identify and trace the objects of G, and access any captured information.

Own_n: The new owner or buyer. When the OTP is completed only this entity can identify and trace the objects of G, and access any captured information.

TTP: A Trusted Third Party, used to distribute fresh keys to the tags of G and the new owner.

After ownership of the collection G of tagged objects is transferred, the previous owner should not be able to trace or access the tagged objects, and the new owner should not be

able to trace or access data captured by the objects of G prior to ownership transfer. More specifically:

- *Privacy of Own_c, or forward secrecy*. The new owner Own_n of the collection of tagged objects G cannot trace past interrogations of G with Own_c.
- *Privacy of Own_n, or backward secrecy*. The current owner Own_c of the tagged objects G cannot identify interrogations of G after ownership is transferred.

In addition, OTPs are sometimes designed [5], [10], and [11], to provide extended capabilities such as:

- *Undeniable Ownership Transfer*. Previous ownership cannot be denied.
- *Current Ownership Proof.* Corroborative evidence of current ownership.
- *Ownership Delegation*. Ownership of a tag is delegated for a limited number of times.
- *Authorized Recovery*. A previous owner can gain back control of a tag without requiring the execution of an OTP.

B. Security concerns and future trends

1. *Spatio-temporal connectivity*. OTPs proposed in the literature do not discuss spatio-temporal connectivity issues, typically assuming (e.g. [12],[13], and 14]) channels that allow high-level parties, including a TTP, to communicate with a tag T in real-time during the execution of the OTP; for example, to restart the protocol if it fails. This implies, if one takes into account the restriction of the RFID communication channel, that T must be physically close to the corresponding high-level parties during the execution of the protocol, which in many practical scenarios is not the case. Suppose for example that a client purchases via the Internet items that are RFID tagged for tracking and counterfeit prevention. The seller dispatches the items and when these reach the destination the client requests the transfer of ownership rights. Figure 2 illustrates the traditional communication flow model and the extended flow model required for this new applications. To address spatio-temporal connectivity issues future OTP models must be designed to be compatible with this new communication model.

2. *Forward and backward secrecy without TTPs or Isolated Environments (IsE).* The current approach for privacy is to either employ a TTP to break the trust link between a tag and its owner (e.g. [13]), or to assume an IsE (e.g. [10]), without any adversarial interference. The first approach is centralized and not appropriate when tags belong to different authorities /companies. In fact, the TTP can be considered as the real holder of the tag's rights while the different owners have simply delegated ownership. The second approach assumes a weak threat model and, as claimed in [12]: "if such protection is adequate then there no need for security". Future OTP models must be designed do that they do not rely on TTPs or IsEs.

The challenging aspect of this problem is that: Own_c knows all the private information of T and can also eavesdrop on the communication between T and the new owner Own_n, and if there is no TTP and an IsE, then it does not seem possible for T to exchange a fresh key with Own_n without Own_c getting access to it, unless public key cryptography is used. Thus a possible solution is to use of Elliptic Curve Cryptography, which although not lightweight, is within the computational capability of many non-basic RFID tags. However there are lightweight solutions that can be implemented with regular UHF tags that use channels with positive secrecy capacity [15].

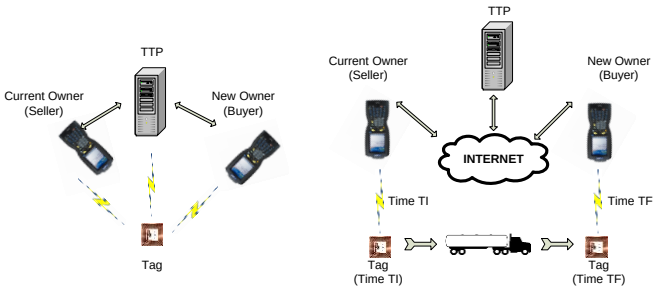

Fig. 2. Traditional (left) and extended (right) OTP communication models.

The Wiretap Channel (WC) model was defined by Wyner in 1975 [16] and involves a communication channel that is wiretapped via a noisy channel. The objective is to obfuscate transmitted data in such a way that the wiretapper's level of confusion is complete (perfect secrecy), or as high as possible (positive secrecy). Munilla et al. [15] propose the use of noisy tags that are controlled by the receiver to achieve the secrecy capacity. The messages x that are transmitted by the tags are obfuscated by the signals $n_1, n_2, \dots, n_t$ of t noisy tags. Let y be the resulting signal. The secrecy capacity of the channel is the conditional entropy $C_x = H(H|Y)$ where X, Y are random variables with values x,y respectively. The secrecy capacity satisfies: $C_s = C_{main} - C_{eav}$, where C_{main} is the capacity of the receiver (that is, Own_n), and C_{eav} is the capacity of the capacity of the eavesdropper (Own_c). If $C_s > 0$ then we have positive secrecy for the messages x transmitted by the tags. It is shown that for $t = 3$ noisy tags the security capacity is roughly $C_s = 0.78$ bits, so the capacity of the wiretapper is bounded by 0.22 bits. We thus get n-bit secrecy for a Key Update Protocol by increasing the length of the messages by a factor of $1/C_s = 1.28$.

V. Grouping Proofs and Grouping Codes

Tag identification protocols involve RFID readers interrogating tagged objects in their range to obtain evidence that corroborates their presence. For supply chain management, the single tag interrogation paradigm can be extended to interrogating collections G of tagged objects. This leads to two different, although sometimes confusing, applications: *grouping codes* and *grouping proofs*. Next, we will briefly define both applications and explain how they can be parallelized and complement the group identification protocols.

A. Grouping codes

Grouping codes make it possible to find the identifiers of all the tags of a collection, including those of missing tags, without requiring a packaging list or an external database. The code uses information previously encoded on each tag to determine if all the tags are present and if not, the identities of the missing tags (see Figure 3). *Grouping codes are not intended to provide any security features* as they usually assume trusted readers, but they are forward error correction mechanisms which can increase the operating speed and reduce cost when it is difficult to access a database with the corresponding information.

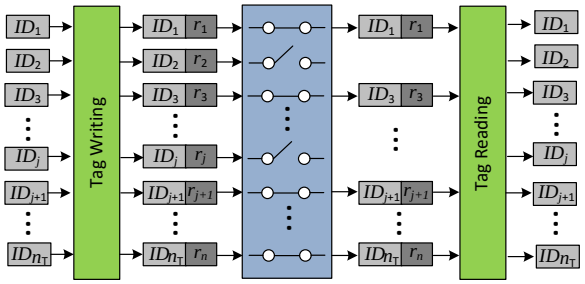

Fig. 3. The write-transmit-read process with RFID grouping codes.

B. Grouping proofs

When RFID technology is used for supply-chain management, concerns regarding the monitoring of tags and transfer of ownership or control of tags need to be addressed. If the transfer is permanent, or even temporal, ownership transfer protocols can be used. However there are cases when the owner does not want to cede control, even though this may be temporal. For example, a manufacturer may use the services provided by a carrier who, in turn, uses other carriers to transport their products (Figure 4). In such cases it is desirable that the owner can periodically check the integrity of a shipment via the carrier. This requirement is referred to as group scanning, and involves a collection of tags G generating a grouping-proof of "simultaneous" presence in the range of an RFID reader [17].

There are several practical scenarios where grouping-proofs can substantially expand the capabilities of RFID-based systems. For example, some products may need to be shipped together and one may want to track their progress through the supply-chain—e.g., hardware components of a system or kits. A different scenario would involve enforcement of safety regulations requiring that drugs be shipped, or dispensed, with information leaflets.

Grouping-proofs are security applications that provide evidences of temporal events to corroborate the "simultaneous" presence of a collection of tags: the proof is generated if (completeness) and only if (soundness) all the tags of the group are simultaneously in the range of a reader (in practice, within a determined interval window). It is important to note that when symmetric key cryptographic is used, grouping-proofs are not real "proofs" in the sense that they are not transferable and can only be validated by those who share the private keys used to generate them. As a result, grouping-proofs applications are only really meaningful when the verifier is offline during the interrogation (i.e. batch connectivity). Indeed, checking the integrity of a collection G when the verifier has permanent connectivity with the reader, and therefore with the tags, is straightforward. It is sufficient for individual tags to get authenticated by the verifier, who can then check simultaneous presence by using auxiliary data, e.g., an identifier of G. Thus, grouping-proof protocols should be focused on offline solutions where the interactions of the verifier are restricted to: i) broadcasting a challenge that is valid for a (short) time span and, ii) checking responses from the tags of G via intermediate readers.

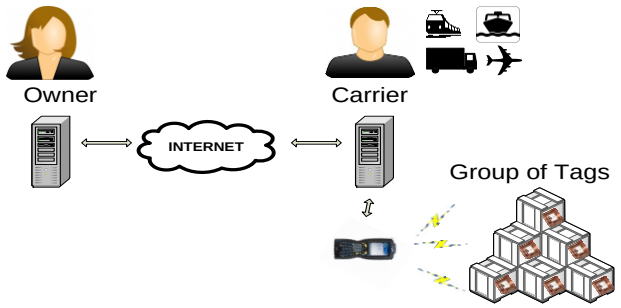

Fig. 4. A collection of tagged objects (pallet) is given to an untrusted Carrier that must provide the owner with periodic grouping-proofs.

C. Security concerns and future trends

1. Efficient use of the tag memory. Most of the grouping codes proposed in the literature are based on low-density parity check matrices (LDPC). For example the Sato et al. grouping codes [19] use Gallager matrices. However the randomized nature of these matrices makes it difficult to get specific decoding guarantees, and LDPC variants have been proposed to overcome this issue (e.g. [20, 21, 22]). However, although LDPC codes are doubtless one of the most powerful forward error correction mechanism, as well as being a very useful tool for Internet multicast communication because of their linear decoding complexity, they do not seem particularly suitable for grouping codes because of their low efficiency in terms of memory consumption [23]. Thus, despite the fact that Reed-Solomon codes have quadratic decoding complexity, they can be more suitable for RFID application, at least with groups of up to 100 tags, because of their optimal use of the redundancy. It must be taken into account that the cost of sending Internet multicast (virtual) packets cannot be compared with the cost of (physical) RFID tag memory. For those cases when we are not interested in determining the *identities* of missing tags but just the *number* of missing tags then neither LDPC nor Reed-Solomon codes are required, and much more simple solutions are available.

2. Preventing privacy leaks and coping with incomplete groups. Despite considerable research interest, many of the proposed RFID grouping-proofs make assumptions that are

not practical (e.g. assume trusted RFID readers or omit tag singularization), and leak some private information. For example, the adversary may learn the number of tags that take part in the protocol and the order in which tags reply. These problems are often related to tag-chaining protocol structures, where each tag in the group authenticates a message coming from the previous tag in the chain. Finally, while grouping-proofs provide integrity evidence for complete groups of tags, they do not address incomplete groups, in particular, they do not provide any information about missing tags.

Burmester and Munilla [23] combine both paradigms to describe a two-pass grouping-proof (in contrast to tag-chaining structures) that allows an untrusted reader to identify missing tags, and if the group is complete, to compile a grouping-proof of integrity that the verifier can check. More specifically, they propose an anonymous RFID grouping-proof of integrity for collections of tagged objects, that supports tag privacy (in particular, untraceability) such that:

a) Only the verifier (a trusted entity) can check the proof.
b) The verifier can authorize an untrusted reader to inspect the group and identify any missing tagged objects.
c) The authorization is for one only inspection, and the tags are untraceable while the group is not inspected.
d) The reader cannot generate a grouping-proof for a group with missing tags.

VI. CONCLUSIONS

We have considered in this paper RFID smart structures for the supply chain. We have analyzed, describing possible solutions, security concerns related to ownership transfer and the presence of untrusted RFID readers of delegated carriers. Unauthorized parties should not share any private information with the tags and should not be able to trace them in other cases than those previously specified.

ACKNOWLEDGMENT

We thank Prof. Kesheng Wang for inviting us to give this Keynote Talk.

REFERENCES

[1] R. Canetti, "Universally composable security: a new paradigm for cryptographic protocols". Proceedings, 42nd IEEE Symposium on Foundations of Computer Science, pp. 136-145, 2001.

[2] E. Welbourne, L. Battle, G. Cole, K. Gould, K. Rector, S. Raymer, M. Balazinska, and G. Borriello, "Building the internet of things using rfid: The rfid ecosystem experience," Internet Computing IEEE, vol.13, no.3.

[3] EPC-Global, " Radio-Frequency Identity Protocols, Generation-2 UHF RFID." Tech. Rep., Brussels, Belgium, April, 2015.

[4] M. Ohkubo, K. Suzuki, and S. Kinoshita, "Cryptographic approach to "privacy-friendly" tags," Proc. RFID Privacy Workshop, 2003

[5] D. Henrici and P.M. Müller, "Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers," pp.149–153, Proc. IEEE Intern. Conf. on Pervasive Computing and Communications, 2004.

[6] D. Molnar, A. Soppera, and D. Wagner, "A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags," Proc. Workshop on Selected Areas in Cryptography (SAC 2005), LNCS, vol.3897, Springer, 2006.M.

[7] T. van Le, M. Burmester, and B. de Medeiros, "Universally Composable and Forward-Secure RFID Authentication and Authenticated Key Exchange," Proc. ACM Symp. on Information, Computer, and Communications Security (ASIACCS 2007), pp.242–252, 2007.

[8] M. Burmester and B. de Medeiros, "The Security of EPC Gen2 Compliant RFID Protocols," ACNS, ed. S.M. Bellovin, R. Gennaro, A.D. Keromytis, and M. Yung, Lecture Notes in Computer Science, vol.5037, pp.490–506, Springer, 2008.

[9] M. Burmester and J. Munilla, "Lightweight RFID authentication with forward and backward security," ACM Trans. Inf. Syst. Secur., vol.14, no.1, pp.11:1–11:26, jun 2011.

[10] B. Song, "RFID Tag Ownership Transfer," Workshop on RFID Security – RFIDSec'08, Budapest, Hungary, July 2008.

[11] C.Y. Ng, W. Susilo, Y. Mu, and R. Safavi-Naini, "Practical RFID Ownership Transfer Scheme," Journal of Computer Security, vol.19, no.2, pp.319–341, 2011.

[12] G. Kapoor, S. Piramuthu, Single RFID Tag Ownership Transfer Protocols, IEEE Transactions on Systems, Man, and Cybernetics, Part C 42 (2) (2012) 164–173.

[13] S. Sundaresan, R. Doss, W. Zhou, S. Piramuthu, Secure ownership transfer for multi-tag multi-owner passive rfid environment with individual owner privacy, Computer Communications 49.

[14] C. Y. Ng, W. Susilo, Y. Mu, R. Safavi-Naini, Practical RFID Ownership Transfer Scheme, Journal of Computer Security 19 (2) (2011) 319–341.

[15] J. Munilla, A. Peinado, G. Yang, and W. Susilo, "Enhanced ownership transfer protocol for RFID in an extended communication model," IACR Cryptology ePrint Archive, vol.20 13, p.187, 2013.

[16] A.D. Wyner, "The Wire-Tap Channel," Tech. Rep. E-print #2009/147, Bell Systems Technical Journal, Vol 54, 1975.

[17] Burmester and J. Munilla, Security and Trends in Wireless Identification and Sensing Platform Tags: Advancements in RFID. IGI Global, 2013,ch. RFID Grouping-Proofs.

[18] N. Ben Mabrouk and P. Couderc, "EraRFID: Reliable RFID systems using erasure coding," in RFID, 2015 IEEE International Conference on, April 2015, pp. 121–128.

[19] Y. Sato, Y. Igarashi, J. Mitsugi, O. Nakamura, and J. Murai, "Identification of missing objects with group coding of RF tags," in RFID, 2012 IEEE International Conference on, April 2012, pp. 95–101.

[20] Y. Su and C. Wang, "Design and analysis of unequal missing protection for the grouping of rfid tags," Communications, IEEE Transactions on, vol. PP, no. 99, pp. 1–1, 2015.

[21] Y.-S. Su and O. K. Tonguz, "Using the Chinese Remainder Theorem for the Grouping of RFID Tags," Communications, IEEE Transactions on, vol. 61, no. 11, pp. 4741–4753, November 2013.

[22] Y.-S. Su, "Extended Grouping of RFID Tags Based on Resolvable Transversal Designs," Signal Processing Letters, IEEE, vol. 21, no. 4,pp. 488–492, April 2014.

[23] M. Burmester and J. Munilla, "Tag-Memory Tradeoff of RFID Grouping Codes". in *IEEE Communications Letters* , vol.PP, no.99, pp.1-1. doi: 10.1109/LCOMM.2016.2546857, April 2016.

[24] M. Burmester and J. Munilla, "An Anonymous RFID Grouping-Proof with Missing Tag Identification," in 10th IEEE International Conference on RFID, May 2016.