Chapter 1 : RFID - Privacy and Security: Research Paper Examples - A Research Guide for Students

2 of the UCC and EAN, the bodies that regulate barcode use in the United States and the rest of the world respectively. EPC tags cost less than thirteen U.S. cents apiece in large.

RFID security and privacy: Abstractâ€”This paper surveys recent technical research on the problems of privacy and security for radio frequency identification RFID. RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next Thanks to dropping cost, they are likely to proliferate into the billions in the next several yearsâ€”and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the nonspecialist, the survey may also serve as a reference for specialist readers. Weis , " Our contribution is threefold: Wireless sensor network security: As wireless sensor networks continue to grow, so does the need for effective security mechanisms. There is currently enormous research potential in the field of wireless sensor network security. Thus, familiarity with the current research in this field will benefit researchers greatly. With this in mind, we survey the major topics in wireless sensor network security, and present the obstacles and the requirements in the sensor security, classify many of the current attacks, and finally list their corresponding defensive measures. RFID tags have very promising applications in many domains retail, rental, surveillance, medicine to name a few. Unfortunately the use of these tags can have serious implications on the privacy of people carrying tagged items. Serious opposition from consumers has already thwarted several trial Serious opposition from consumers has already thwarted several trials of this technology. The main fears associated with the tags is that they may allow other parties to covertly collect information about people or to trace people wherever they go. As long as these privacy issues are not resolved it will not be possible to reap the benefits of these new applications. Radio Frequency Identification RFID systems aim to identify objects in open environments with neither physical nor visual contact. They consist of transponders inserted into objects, of readers, and usually of a database which contains information about the objects. The key point is that author The key point is that authorised readers must be able to identify tags without an adversary being able to trace them. Traceability is often underestimated by advocates of the technology and sometimes exaggerated by its detractors. Whatever the true picture, this problem is a reality when it blocks the deployment of this technology and some companies, faced with being boycotted, have already abandoned its use. Using cryptographic primitives to thwart the traceability issues is an approach which has been explored for several years. However, the research carried out up to now has not provided satisfactory results as no universal formalism has been defined. In this paper, we propose an adversarial model suitable for RFID environments. We define the notions of existential and universal untraceability and we model the access to the communication channels from a set of oracles. Show Context Citation Context Among the actual applications, we can also cite locating people in a public area, e. The aim is to help customers to keep in touch with other members of their group in the p Radio frequency identification systems based on low-cost computing devices is the new plaything that every company would like to adopt. Its goal can be either to improve the productivity or to strengthen the security. Specific identification protocols based on symmetric challenge-response Specific identification protocols based on symmetric challenge-response have been developed in order to assure the privacy of the de-vice bearers. Existing protocols require O n cryptographic operations to identify one device among n. Molnar and Wagner suggested a method to reduce this complexity to O log n. We show that their technique could degrade the privacy if the attacker has the possibility to tamper with at least one device. Because low-cost devices are not tamper-resistant, such an attack could be feasi-ble. We give a detailed analysis of their protocol and evaluate the threat. RFID, time complexity, time-memory trade-off. However, these tags also bring with them security and privacy issues. Security issues rely on classic attacks, e. Proceedings of the 4th ACM workshop on Wireless security , " Like barcodes, EPC tags emit static codes that serve to identify and track shipping

containers and individual objects. EPC tags, though, h EPC tags, though, have a powerful benefit: Some commercial segments, like the pharmaceutical industry, are coming to view EPC tags as an anti-counterfeiting tool. EPC tags are a potent mechanism for object identification, and can facilitate the compilation of detailed object histories and pedigrees. They are poor authenticators, though. EPC tags are vulnerable to elementary cloning and counterfeiting attacks. In this paper, we present techniques that strengthen the resistance of EPC tags to elementary cloning attacks. We show how to leverage PIN-based accesscontrol and privacy enhancement mechanisms in EPC tags to achieve what may be viewed as crude challenge-response authentication. Our techniques can even strengthen EPC tags against cloning in environments with untrusted reading devices. The biggest challenge for RFID technology is to provide benefits without threatening the privacy of consumers. Many solutions have been suggested but almost as many ways have been found to break them. An approach by Ohkubo, Suzuki and Kinoshita using an internal refreshment mechanism seems to protec An approach by Ohkubo, Suzuki and Kinoshita using an internal refreshment mechanism seems to protect privacy well but is not scalable. We introduce a specific time-memory trade-o that removes the scalability issue of this scheme. Additionally we prove that the system truly o ers privacy and even forward privacy. Our third contribution is an extension of the scheme which o ers a secure communication channel between RFID tags and their owner using building blocks that are already available on the tag. Finally we give a typical example of use of our system and show its feasibility by calculating all the parameters. In this paper, we investigate the possible privacy and security threats to RFID systems, and consider whether previously proposed RFID protocols address these threats. We then propose a new authentication protocol which provides the identified privacy and security features and is also efficient. The new protocol resists tag information leakage, tag location tracking, replay attacks, denial of service attacks, backward traceability, forward traceability under an assumption , and server impersonation also under an assumption. We also show that it requires less tag-side storage and computation than other similarly structured RFID protocols. Devices that tell on you: Privacy trends in consumer ubiquitous computing by T. Scott Saponas, Sameer Agarwal, et al. We analyze three new consumer electronic gadgets in order to gauge the privacy and security trends in massmarket UbiComp devices. Our study of the Slingbox Pro uncovers a new information leakage vector for encrypted streaming multimedia. By exploiting properties of variable bitrate encoding schemes, By exploiting properties of variable bitrate encoding schemes, we show that a passive adversary can determine with high probability the movie that a user is watching via her Slingbox, even when the Slingbox uses encryption. We experimentally evaluated our method against a database of over hours of network traces for 26 distinct movies. We also uncover security issues with the way Microsoft Zunes manage their social relationships. We also use some of our attacks to motivate fundamental security and privacy challenges for future UbiComp devices.

Chapter 2 : PPT - RFID Security and Privacy: A Research Survey PowerPoint Presentation - ID

RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work.

Internet of Things IoT: This offers the ability to measure, infer, and understand environmental indicators, from delicate ecologies and natural resources to urban environments. The proliferation of these de The proliferation of these devices in a communicating-actuating network creates the Internet of Things IoT , wherein, sensors and actuators blend seamlessly with the environment, and the information is shared across platforms in order to develop a common operating picture COP. Fuelled by the recent adaptation of a variety of enabling device technologies such as RFID tags and readers, near field communication NFC devices and embedded sensor and actuator nodes, the IoT has stepped out of its infancy and is the the next revolutionary technology in transforming the Internet into a fully integrated Future Internet. As we move from www static pages web to web2 social networking web to web3 ubiquitous computing web , the need for data-ondemand using sophisticated intuitive queries increases significantly. This paper presents a Cloud-centric vision for worldwide implementation of Internet of Things. The key enabling technologies and application domains that are likely to drive IoT research in the near future are discussed. A cloud implementation using Aneka, which is based on interaction of private and public Clouds is presented. We conclude our IoT vision by expanding on the need for the convergence of WSN, the Internet, and distributed computing. Show Context Citation Context This has resulted in many applications, particular RFID-enabled credit cards are widely deployed in the United States and other countries, but no public study has thoroughly analyzed the mechanisms that provide both security and privacy. Some cautionary notes are in order, however. While the nominal read range of an RFID tag may be quite short, on the order of several centimeters, for example, a non-standard reader or larg Practical attacks on proximity identification systems short paper by Gerhard P. The number of RFID devices used in everyday life has increased, along with concerns about their security and user privacy. Focusing mainly on the RF communication i Focusing mainly on the RF communication interface we discuss the results and implementation of eavesdropping, unauthorized scanning and relay attacks. Although most of these attack scenarios are regularly mentioned in literature little technical details have been published previously. We also present a short overview of mechanisms currently available to prevent these attacks 1. This has understandably driven research into RFID security. In response to this danger, unlinkable protocols aim to make it impossible for a third party to identify two runs of In response to this danger, unlinkable protocols aim to make it impossible for a third party to identify two runs of a protocol as coming from the same device. We present a framework for analysing unlinkability and anonymity in the applied pi calculus. We show that unlinkability and anonymity are complementary properties; one does not imply the other. Using our framework we show that the French RFID e-passport preserves anonymity but it is linkable therefore anyone carrying a French e-passport can be physically traced. Some other attempts to formalise unlinkability In this paper, we analyze the security vulnerabilities of two ultra-lightweight RFID mutual authentication protocols: We identify two effective attacks, namely De-synchronization attack and Full-disclosure attack, against t We identify two effective attacks, namely De-synchronization attack and Full-disclosure attack, against their protocols. The former attack can break the synchronization between the RFID reader and the tag in a single protocol run so that they can not authenticate each other in any following protocol runs. The latter attack can disclose all the secret information stored on a tag by interrogating the tag multiple times. Thus it compromises the tag completely. Moreover, we point out the potential countermeasures to improve the security of above protocols. Some of the earlier research works draw assumptions on practical limitations of RFID deployments: Devices that tell on you: Privacy trends in consumer ubiquitous computing by T. Scott Saponas, Sameer Agarwal, et al. We analyze three new consumer electronic gadgets in order to gauge the privacy and security trends in massmarket UbiComp devices. Our study of the Slingbox Pro uncovers a new information leakage vector for encrypted streaming multimedia. By exploiting properties of variable bitrate encoding schemes, By exploiting

properties of variable bitrate encoding schemes, we show that a passive adversary can determine with high probability the movie that a user is watching via her Slingbox, even when the Slingbox uses encryption. We experimentally evaluated our method against a database of over hours of network traces for 26 distinct movies. We also uncover security issues with the way Microsoft Zunes manage their social relationships. We also use some of our attacks to motivate fundamental security and privacy challenges for future UbiComp devices. One important problem in RFID systems is how to quickly estimate the number of distinct tags without reading each tag individually. This problem plays a crucial role in many real-time monito This problem plays a crucial role in many real-time monitoring and privacy-preserving applications. In this paper, we present an efficient and anonymous scheme for tag population estimation. This scheme leverages the position of the first reply from a group of tags in a frame. Results from mathematical analysis and extensive simulation demonstrate that our scheme outperforms other protocols proposed in the previous work. Identifying each tag ID increases individual security and privacy risks. However, the cryptographic techniques require additional modification to the tag hardware, as well as increase the computational complexity on both tags and readers. Prior work in [12] and [

DOWNLOAD PDF RFID SECURITY AND PRIVACY A RESEARCH SURVEY

Chapter 3 : CiteSeerX â€” A RESEARCH SURVEY: RFID SECURITY & PRIVACY ISSUE

This paper surveys recent technical research on the problems of privacy and security for radio frequency identification (RFID). RFID tags are small, wireless devices that help identify objects and.

RFID security and privacy: Abstractâ€”This paper surveys recent technical research on the problems of privacy and security for radio frequency identification RFID. RFID tags are small, wireless devices that help identify objects and people. Thanks to dropping cost, they are likely to proliferate into the billions in the next Thanks to dropping cost, they are likely to proliferate into the billions in the next several yearsâ€”and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings, and even the bodies of consumers. This survey examines approaches proposed by scientists for privacy protection and integrity assurance in RFID systems, and treats the social and technical context of their work. While geared toward the nonspecialist, the survey may also serve as a reference for specialist readers. Show Context Citation Context Removable RFID tags support a similar approach. These RFID tags, however, reside in price tags, and are therefore easily removed and discarded. Killing or discarding tags enforces consumer privacy effectively, but it eliminates all of the post-pu Proceedings of the 4th ACM workshop on Wireless security , " Like barcodes, EPC tags emit static codes that serve to identify and track shipping containers and individual objects. EPC tags, though, h EPC tags, though, have a powerful benefit: Some commercial segments, like the pharmaceutical industry, are coming to view EPC tags as an anti-counterfeiting tool. EPC tags are a potent mechanism for object identification, and can facilitate the compilation of detailed object histories and pedigrees. They are poor authenticators, though. EPC tags are vulnerable to elementary cloning and counterfeiting attacks. In this paper, we present techniques that strengthen the resistance of EPC tags to elementary cloning attacks. We show how to leverage PIN-based accesscontrol and privacy enhancement mechanisms in EPC tags to achieve what may be viewed as crude challenge-response authentication. Our techniques can even strengthen EPC tags against cloning in environments with untrusted reading devices. Although some tagging of individual retail items is already taking place in, e. While RFID is a decades-old concept, it is becoming viable now as a ubiquitous technology thanks to dropping cos Abstractâ€”Radio frequency identification RFID is an important part in mobile and ubiquitous domain, and brings enormous productivity benefits in applications where objects require automatic identification. However, this pervasive use of RFID tags opens up the possibility of various attacks that vio However, this pervasive use of RFID tags opens up the possibility of various attacks that violate user privacy and authentication. Security mechanisms for RFID systems are therefore of the utmost important. Previous works in the literature proposed schemes that were proven to be secure, but they had scalability problems. A feasible and scalable protocol to guarantee privacy is presented in this paper. The proposed scheme uses elliptic curve cryptography with the addition of zero knowledge based authentication. An analysis that proves that the systems is secure, and even forward secure, is also provided. The main problem of this approach relies on its scalability, as the number of stored identifiers grows exponentially when the number of tags increases. Later [7], [8] and [9] suggested bringing some changes in this approach. A Research Survey by Ari Juels , " Thanks to dropping cost, they are likely to proliferate into the billions in the n Thanks to dropping cost, they are likely to proliferate into the billions in the next several years â€” and eventually into the trillions. RFID tags track objects in supply chains, and are working their way into the pockets, belongings and even the bodies of consumers. While geared toward the non-specialist, the survey may also serve as a reference for specialist readers.

Chapter 4 : CiteSeerX â€” RFID security and privacy: A research survey

You just clipped your first slide! Clipping is a handy way to collect important slides you want to go back to later. Now customize the name of a clipboard to store your clips.

DOWNLOAD PDF RFID SECURITY AND PRIVACY A RESEARCH SURVEY

Chapter 5 : CiteSeerX â€" Citation Query expands RFID retail trial

A research survey conducted in shows that many issues regarding security and privacy with respect to RFID technology have not been resolved satisfactorily (Pateriya and Sharma,).

Chapter 6 : CiteSeerX â€" Citation Query RFID security and privacy: a research survey

Along with meeting the security and privacy needs of RFID technology, solutions must be inexpensive, practical, reliable, scalable, flexible, inter-organizational, and long lasting.

Chapter 7 : RFID Security and Privacy: A Research Survey | Dhanraj Neelakandan - www.nxgvision.com

Other valuable research problems remain, however, reader and tag played by NFC devices. of which we mention just a couple: Another important aspect of RFID security that of user â€¢ Is it possible to construct a fully privacy-preserving, perception of security and privacy in RFID systems.

Chapter 8 : The Evolution of RFID Security and Privacy: A Research Survey

"Information security and privacy" is one of the major challenges in the communication world of IT as each and every information we pass need to be secured enough to the extent that it doesn.