Diss. ETH No. 20837

RFID Authentication: New Techniques and Privacy Implications

A dissertation submitted to
ETH ZURICH

for the degree of
Doctor of Sciences

presented by

DAVIDE ZANETTI

Master of Science in Embedded Systems Design,
University of Lugano

born September 29, 1979

citizen of Isorno, TI

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. David Basin, co-examiner
Prof. Dr. Jean-Pierre Hubaux, co-examiner
Dr. Ari Juels, co-examiner

2012

Abstract

Radio-Frequency IDentification (RFID) technology provides an inexpensive means to identify physical objects. The wide proliferation of RFID devices, or *tags*, in our everyday life, such as electronic identity documents and contactless transportation tickets, raises both security and privacy concerns. On the one hand, RFID tag identification does not guarantee authenticity: the identifiers stored in RFID tags used for object identification can be copied, creating, in fact, indistinguishable *clones* of the original tags/objects. RFID tag authentication solutions provide a means to verify claimed identities. However, a number of challenges must be faced when designing such solutions, in particular related to constrained (in size, power, cost) tags. On the other hand, RFID technology raises several privacy concerns regarding both clandestine tracking of final consumers and disclosure of confidential information by business partners employing RFID systems. These concerns may dramatically limit the deployment of RFID technology.

In this thesis, we first explore *tag authentication* and *clone detection* techniques suitable for constrained RFID tags. Then, we investigate the *privacy implications* of the explored techniques.

In the first part of this thesis, we propose and evaluate tag authentication and clone detection techniques based on physical-layer fingerprinting and tracing information. The proposed physical-layer techniques aim at uniquely distinguishing RFID tags through their physical-layer fingerprints, i.e., using characteristics that tags show in the transmitted RF signals. Differently, the proposed technique based on tracing information aims at detecting cloned RFID tags by analyzing tag-related information collected by the different entities employing an RFID system. We find that our techniques provide reliable tag authentication / clone detection suitable for constrained RFID tags.

In the second part of this thesis, we investigate the privacy implications of the proposed tag authentication / clone detection techniques. We first explore the practicality of tracking people carrying RFID tags by means of the physical-layer fingerprints of their tags. We demonstrate that tracking people carrying RFID tags is feasible and practical, even in the presence of upper-layer protection measures (e.g., encryption). Then, we propose and evaluate a protocol that provides information privacy for clone detection based on tracing information. We show that our protocol allows a set of entities to collaboratively detect clones without disclosing information on their collected tag-related information or their relationships.

Zusammenfassung

Radio-Frequenz IDentifizierung (RFID) ist eine preisgünstige Technologie zur Identifizierung von physischen Objekten. Die weite Verbreitung von RFID Transpondern oder Tags im Alltagsleben, zum Beispiel in Form von elektronischen Identitätskarten oder kontaktlosen Fahrkarten, bringt Bedenken sowohl zur Sicherheit als auch zum vertraulichen Umgang mit sich. Auf der einen Seite garantiert die Identifizierung mittel RFID Tags keine Authentizität, da die Identifikatoren, welche auf den RFID Tags gespeichert sind und für die Identifizierung verwendet werden, kopiert werden können. Dadurch können geklonte Tags erzeugt werden, die von den originalen Tags oder Objekten nicht zu unterscheiden sind. Techniken zur Authentifizierung von RFID Tags sind eine Möglichkeit zur Verifizierung der beanspruchten Identitäten. Jedoch gibt es eine Reihe von Herausforderungen beim Entwurf solcher Lösungen, vor allem in Zusammenhang mit den Beschränkungen der Tags (im Sinne ihrer Grösse, der Energie und Kosten). Auf der anderen Seite verursacht die RFID Technologie Bedenken zur Privatsphäre, die sowohl das heimliche Nachverfolgen der Endbenutzer als auch die Preisgabe vertraulicher Informationen durch Geschäftspartner, die RFID Systeme verwenden, betreffen. Diese Bedenken können den Einsatz der RFID Technologie dramatisch einschränken.

In dieser Arbeit untersuchen wir zunächst Lösungen zur Authentifizierung von Tags und zum Detektieren von Klons, die für ressourcenbeschränkte RFID Tags anwendbar sind. Dann betrachten wir die Auswirkungen der untersuchten Lösungen auf die Privatsphäre.

Im ersten Teil dieser Arbeit schlagen wir Lösungen zur Authentifizierung von Tags und zur Detektion von Klons vor, welche auf Fingerabdrücken auf der physischen Übertragungsschicht und der Nachverfolgung von Informationen basieren, und wir evaluieren diese. Die vorschlagenen Techniken auf der physischen Schicht zielen darauf ab, RFID Tags aufgrund ihrer physischen Fingerabdrücke eindeutig zu unterscheiden, das heisst unter Verwendung von Charakteristika, welche die Tags in ihren übertragenen Funksignalen aufweisen. Auf der anderen Seite zielt die vorgeschlagene Lösung basierend auf der Nachverfolgung von Informationen darauf ab geklonte RFID Tags zu detektieren, indem tagrelevante Informationen analysiert werden, welche von verschiedenen Einheiten, die RFID-Systeme nutzen, gesammelt werden. Unsere Analyse hat ergeben, dass unsere Lösungen die zuverlässige Authentifizierung von Tags sowie

Klondetektion ermöglichen und dass diese für ressourcen-beschränkte RFID Tags geeignet ist.

Im zweiten Teil dieser Arbeit untersuchen wir die Auswirkungen der vorgeschlagenen Tagauthentifizierungs- und Klondetektionslösungen auf die Vertraulichkeit. Wir erforschen zunächst die praktische Machbarkeit, Menschen mit RFID Tags durch Fingerabdrücke der Tags nachzuverfolgen. Wir zeigen, dass die Nachverfolgung von Personen mit RFID Tags machbar und praktisch umsetzbar ist, selbst wenn Schutzmassnahmen auf höherer Schicht (wie Verschlüsselung) zum Einsatz kommen. Anschliessend schlagen wir ein Protokoll vor, welches die Vertraulichkeit von Informationen bei der Klondetektion basierend auf dem Nachverfolgen von Informationen gewährleistet. Wir evaluieren das Protokoll und zeigen, dass dieses es einer Menge an Geräten ermöglicht gemeinsam Klone zu detektieren, ohne dabei Informationen zu den gesammelten Daten der Tags oder ihren Beziehungen preiszugeben.

Sommario

La tecnologia RFID (*Radio-Frequency IDentification*) permette l'identificazione di oggetti in modo automatico e a basso costo. L'uso sempre più frequente di questa tecnologia in diversi ambiti della nostra vita quotidiana, ad esempio nei passaporti o nei titoli di viaggio, ha sollevato numerose preoccupazioni in termini di sicurezza e privacy. Da un lato, l'identificazione di un oggetto tramite un *tag* RFID, ossia il dispositivo elettronico che applicato (o integrato) sull'oggetto permette l'identificazione di questo, non garantisce l'autenticità dell'oggetto stesso. I dati immagazzinati nei tag RFID ed usati per l'identificazione (ad esempio, un numero univoco che identifica uno specifico oggetto) possono essere facilmente copiati, creando, di fatto, delle copie indistinguibili dall'originale, e quindi dei *cloni*. Sebbene esistano delle soluzioni che permettono l'autenticazione dei tag, ovvero la verifica dell'identità dichiarata, queste devono tenere conto di numerose problematiche, in modo particolare riguardanti la natura stessa dei tag RFID. Questi, infatti, sono dispositivi concepiti per essere a basso costo, di piccole dimensioni e con limitate risorse di calcolo e memorizzazione. Dall'altro lato, la tecnologia RFID ha sollevato numerose preoccupazioni in termini di privacy, in modo particolare riguardanti il tracciamento e la localizzazione (non autorizzati) di persone e la divulgazione di dati sensibili relativi alle operazioni effettuate sui tag RFID da parte delle diverse entità che operano all'interno di un sistema basato sulla tecnologia RFID. Queste preoccupazioni possono frenare in maniera drastica l'adozione su vasta scala della tecnologia RFID.

In questa tesi, in primo luogo esploriamo nuove soluzioni per autenticazione di tag RFID a basso costo, ossia dispositivi RFID con limitate risorse di calcolo e memorizzazione. Secondariamente, investighiamo le implicazioni in termini di privacy delle soluzioni precedentemente esplorate.

Nella prima parte di questa tesi, proponiamo delle soluzioni per l'autenticazione di tag RFID basate su tecniche di identificazione a livello fisico, o *physical-layer identification* e di tracciamento, o *tracing*. Le tecniche basate su physical-layer identification hanno come obbiettivo l'identificazione univoca dei tag RFID tramite impronte digitali basate su specifiche caratteristiche della comunicazione tra dispositivi a livello fisico, cioè specifiche caratteristiche dei segnali radio trasmessi dai tag durante la comunicazione con altri dispositivi. Diversamente, le tecniche basate su tracing hanno lo scopo di rilevare la presenza di cloni all'interno di un sistema basato sulla tecnologia RFID tramite l'analisi dei dati relativi alle operazioni ef-

fettuate sui tag da parte delle diverse entità che operano all'interno del suddetto sistema. I nostri risultati mostrano che le soluzioni proposte sono compatibili con tag a basso costo.

Nella seconda parte di questa tesi, investighiamo le implicazioni in termini di privacy delle soluzioni proposte nella prima parte. In primo luogo, esploriamo la fattibilità di tracciare in maniera non autorizzata mediante tecniche di physical-layer identification persone che portano tag RFID. Ovvero, tracciare persone tramite le impronte digitali dei tag RFID che queste portano. I nostri risultati mostrano che tracciare persone che portano tag è fattibile e pratico. Questo, anche in presenza di misure di protezione come, ad esempio, la criptazione della comunicazione tra dispositivi. In secondo luogo, proponiamo un protocollo crittografico che ha lo scopo di proteggere dati potenzialmente sensibili usati per il rilevamento di cloni tramite tecniche basate su tracing. Il protocollo che proponiamo permette ad un gruppo composto da diverse entità, ognuna delle quali possiede dati rilevanti per il tracing ma che considera sensibili, di rilevare la presenza di cloni in maniera collettiva senza la divulgazione di dati sensibili tra le varie entità.