Diss. ETH No. 19644

Physical-layer Identification of Wireless Devices

A dissertation submitted to
ETH Zurich

for the degree of
Doctor of Sciences

presented by

Boris Danev

MSc en informatique EPFL
born June 28, 1979
citizen of Bulgaria

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. David Basin, co-examiner
Prof. Dr. Wayne Burleson, co-examiner
Prof. Dr. Refik Molva, co-examiner

2011

Abstract

Wireless technologies are becoming increasingly present and important in our daily lives. They are being incorporated in more and more applications such as identity documents, payment systems, intelligent homes, environmental monitoring, supply chains, medical devices. Certain critical issues in the security and privacy of these applications relate to the identification of devices.

There are two major ways to identify devices in the network. The first one, mostly used in today's networks, relies on what devices hold (e.g., unique identification numbers, cryptographic keys). The second one, which is the focus of this thesis, consists of extracting unique characteristics which are inherent to the device and can be observed.

In this thesis, we study the feasibility of uniquely identifying wireless devices using physical characteristics of their analog radio circuitry. These characteristics are the result of hardware impairments introduced during the manufacturing process. We focus on those features that appear in the transmitted radio signals and are therefore measurable during the physical-layer device communication. We propose techniques that enable the accurate identification of several types of wireless devices, analyze the underlying assumptions and clarify the implications on the security and privacy of wireless applications.

In the introductory part of this thesis, we provide a real-world example that illustrates one problem with authenticating devices by what they hold. We realize a practical attack on car access control systems and discuss the potential of device identification to complement traditional authentication and prevent this and other device identity attacks.

Secondly, we study the problem of identifying same-model-same-manufacturer active and passive wireless devices using physical-layer characteristics. We consider low-power wireless transceivers and passive RFID transponders. We explore timing, modulation and spectral properties of the radio signals and show that wireless devices can be accurately identified under certain assumptions.

Finally, we evaluate the resilience of physical-layer device identification methods to impersonation. We show that physical-layer identification is vulnerable to certain types of impersonation attacks. We also provide a classification of attacks and discuss the implications of the use of physical-layer device identification in applications such as intrusion detection, device cloning detection and device privacy protection.

Zusammenfassung

Drahtlose Technologien werden zunehmend allgegenwärtig und wichtig in unserem täglichen Leben. Sie werden in immer mehr Anwendungen eingesetzt, wie zum Beispiel in Identitätskarten, Zahlungsystemen, intelligenten Häusern, bei der Überwachung, in Lieferketten und medizinischen Geräten. Für die Sicherheit der Anwendungen spielt auch die eindeutige Identifizierung dieser Geräte eine wichtige Rolle.

Es gibt zwei Wege um Geräte im Netzwerk zu identifizieren. Erstens können Geräte aufgrund von Informationen wie MAC-Adressen oder kryptographischen Schlüsseln identifiziert werden. Zweitens, und dies ist der Fokus dieser Arbeit, können Geräte aufgrund von einzigartigen Charakteristika identifiziert werden, welche bei jedem Gerät beobachtet werden können.

In dieser Arbeit erforschen wir die Durchführbarkeit der eindeutigen Identifizierung von drahtlosen Geräten durch physikalische Charakteristika ihrer analogen Funkschaltkreise. Diese Charakteristika resultieren aus Abweichungen im Produktionsprozess. Wir konzentrieren uns auf Charakteristika, welche im übertragenen Signal auftauchen und dadurch auf der physikalischen Ebene beim Empfänger messbar sind. Wir stellen Techniken vor, welche die genaue Identifizierung mehrerer Klassen von drahtlosen Geräten ermöglichen, analysieren die zugrundeliegenden Annahmen und erläutern die Folgen für die Sicherheit der drahtlosen Anwendungen.

In der Einführung dieser Arbeit stellen wir ein Beispiel aus der Praxis vor, welches das Problem der ausschliesslich kryptographischen Identifizierung verdeutlicht. Wir erläutern unseren Versuchsaufbau, der Angriffe auf Fahrzeugschliesssysteme ermöglicht und, diskutieren das Potential der Identifizierung von Geräten auf der physikalischen Ebene als Ergänzung zu traditionellen Authentifizierungssystemen, um diesen und ähnliche Angriffe zu verhindern.

Zweitens erforschen wir das Problem der Identifizierung von aktiven und passiven drahtlosen Geräten aus der gleichen Serie eines Herstellers, aufgrund von physikalischen Charakteristika. Wir betrachten Charakteristika mit Bezug auf Zeit, Modulation und Spektraleigenschaften der Funksignale und zeigen, dass drahtlose Geräte unter bestimmten Voraussetzungen eindeutig identifiziert werden können.

Schliesslich werten wir die Widerstandsfähigkeit unserer Identifizierung auf der physikalischen Ebene gegen Imitationsangriffe aus. Wir

zeigen, dass die physikalische Identifizierung anfällig gegenüber einigen Arten von Imitationsangriffen ist. Wir klassifizieren diese Angriffe und diskutieren die Folgen für die Nutzung der Identifizierung auf der physikalischen Ebene für Anwendungen wie die Erkennung von Eindringlingen, Gerätekopien und Methoden zum Schutz der Privatsphäre.

Résumé

Les technologies sans fil deviennent de plus en plus présentes et importantes dans la vie quotidienne. Elles sont incorporées dans de nombreuses applications telles que documents d'identité, systèmes de paiements, maisons intelligentes, surveillance, chaînes d'approvisionnement, équipements médicaux. La sécurité de ces applications est fortement liée à l'identification de ces équipements radio.

Il existe deux moyens pour identifier les équipements radio dans le réseau. Le premier, le plus couramment utilisé, est basé sur ce que l'équipement en question possède (des numéros d'identification uniques, clés cryptographiques). Le deuxième consiste à extraire des caractéristiques uniques, intrinsèques à l'équipement et qui peuvent être mesurées.

Dans cette thèse, nous étudions la faisabilité d'identifier d'une manière unique les équipements radio en utilisant des caractéristiques physiques de leurs circuits intégrés. Ces caractéristiques sont dues à des imperfections de fabrication de leurs composants. Nous nous concentrons sur les caractéristiques qui apparaissent dans les signaux radio transmis et en conséquence peuvent être mesurées pendant la transmission au niveau physique. Nous proposons et analysons des méthodes pour identifier plusieurs types d'équipements de manière précise, et nous expliquons les conséquences possibles pour la sécurité et la protection de la vie privée de leurs utilisateurs.

Dans la première partie de la thèse, nous présentons un exemple de la vie réelle qui montre un problème important d'authentification des équipements basés sur des clés cryptographiques. Nous effectuons des attaques contre des systèmes de contrôle d'accès de véhicules, et nous discutons le potentiel de l'identification basée sur les caractéristiques physiques pour prévenir ce type d'attaques, ainsi que pour d'autres attaques liées à l'identité de l'équipement.

Deuxièmement, nous explorons le problème d'identification d'équipements radio du même fabriquant et du même modèle en utilisant des caractéristiques extraites de la communication au niveau physique. Nous considérons des émetteurs-récepteurs radios actifs et des transpondeurs RFID passifs. Nous étudions des propriétés de temps, de modulation et les propriétés spectrales des signaux émis par l'équipement. Nous montrons que les équipements radio peuvent être identifiés de manière précise sous certaines conditions.

Finalement, nous évaluons les possibilités de compromettre les méthodes d'identification d'équipements. Nous montrons que certaines attaques basées sur l'imitation des signaux sont possibles et efficaces. Nous classifions l'ensemble de ces attaques et discutons les conséquences de l'utilisation de ces techniques d'identification d'équipements radio sur la détection d'intrusion, la détection de clones et la protection de la vie privée.