Physical-layer Techniques for Secure Proximity Verification and Localization

DISS. ETH No. 23319

Physical-layer Techniques for Secure Proximity Verification & Localization

A thesis submitted to attain the degree of

DOCTOR OF SCIENCES of ETH ZURICH

(Dr. sc. ETH Zurich)

presented by

Aanjhan Ranganathan

Master of Science in Electrical and Electronic Engineering,
EPFL, Switzerland

born on 07.11.1983

citizen of India

accepted on the recommendation of

Prof. Dr. Srdjan Čapkun, examiner
Prof. Dr. Ivan Martinovic, co-examiner
Prof. Dr. Neal Patwari, co-examiner
Prof. Dr. Mani Srivastava, co-examiner
Prof. Dr. Patrick Tague, co-examiner

2016

Abstract

Today, location and proximity information are key to a number of emerging applications. With the advent of the Internet of Things and autonomous cyber-physical systems, the dependency on location and proximity is likely to increase in the future. Current proximity verification and ranging systems are prone to distance modification attacks that can lead to loss of property (e.g., cars [57]) and even human life (e.g., IMDs [119]). Additionally, GPS which is today the de-facto outdoor localization system is vulnerable to spoofing attacks [76] that forces a receiver to compute a false location. Given the safety and security implications of the applications mentioned above, it is important to ensure the security of the location and proximity estimates used in these systems. Existing solutions based on distance bounding are not suitable for a variety of applications or are not secure against all types of attacks. For example, the design and hardware complexity of current solutions make them unsuitable for contactless access control and authentication systems.

In this thesis, we address these shortcomings and make the following contributions. First, we propose a novel distance bounding system design called Switched Challenge Reflector with Carrier Shifting that enhances existing analog designs to be resilient against strong attackers capable of terrorist fraud. Second, we analyze and enhance a new class of chirp-based ranging solutions that enable the realization of low-power ranging systems. We analyze the security of existing chirp-based ranging systems and demonstrate their vulnerability to distance decreasing relay attacks. We then propose a novel design based on frequency modulated continuous wave (FMCW) and backscatter communication techniques, specifically designed for short-range contactless systems. Finally, in the context of outdoor localization, we present SPREE, the first GPS receiver capable of detecting or mitigating all GPS spoofing attacks described in the literature.

Zusammenfassung

Heutzutage sind Geographische und Näheninformationen der Schlüssel zu einer Reihe von neuen Anwendungen. Mit dem Aufkommen von Internet der Dinge und autonomen Cyber-Physikalischen Systemen, wird sich die Abhängigkeit von Geographischen und Näheninformationen in Zukunft wahrscheinlich erhöhen. Aktuelle Systeme, die die geographische Nähe verifizieren, sind anfällig für Angriffe die die Entfernung verfälschen und dadurch zum Verlust von Eigentum (z.B., cars [57]) und sogar Menschenleben führen können (z.B., IMDs [119]). Zusätzlich ist GPS, der Standard für Außenlokalisierung, anfällig für Spoofing Angriffe [76], die einen Empfänger dazu zwingen eine falsche Position zu berechnen. Angesichts der Zuverlässigkeit und Sicherheitsimplikationen der oben genannten Anwendungen, ist es wichtig sicherzustellen, dass die geographischen Lage und Nähe für diese Systeme zuverlässig bereitgestellt wird. Bestehende Lösungen welche die Distanz feststellen, sind für viele Anwendungen ungeeignet und ebenfalls unsicher gegen viele Arten von Angriffen. Das Design und die Komplexität der Hardware der derzeitigen Lösungen sind zum Beispiel ungeeignet für kontaktlose Zugangskontrollen und Authentifizierungssysteme.

In dieser Doktorarbeit wenden wir uns diesen Mängeln zu und leisten die folgenden Beiträge. Als erstes schlagen wir ein neues Abstands-begrenzungssystem vor names *"Switched Challenge Reflector with Carrier Shifting"*, welches die vorhandenen analogen Designs verbessert, indem es sie robust gegen starke Angreifer macht welche Terror Betrug ausführen können. Zweitens analysieren und verbessern wir eine neue Klasse von chirp-basierten Lösungen, welche energiearme Distanzsysteme ermöglichen. Wir analysieren die Sicherheit von existierenden chirp-basierten Distanzsystemen und zeigen deren Anfälligkeit auf Entfernungsreduktion mittels Relais-attacken. Anschliessend schlagen wir ein innovatives Design vor, welches speziell für Kurzstrecken und kontaktlose Systeme zugeschnitten ist und auf kontinuierlichen frequenzmodulierten Wellen (FMCW) und Backscatter-Kommunikationstechniken basiert. Schlus-

sendlich, präsentieren wir SPREE im Rahmen der Outdoor-Lokalisierung, der erste GPS Empfänger, der alle bekannten GPS Spoofing Angriffe der Literatur mildern oder bekämpfen kann.