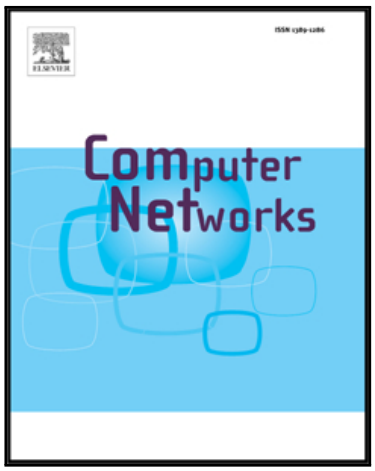

Authenticated Key Establishment for Low-Resource Devices Exploiting Correlated Random Channels

Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, Christof Paar

PII: S1389-1286(16)30194-3
DOI: 10.1016/j.comnet.2016.06.013
Reference: COMPNW 5931

To appear in: *Computer Networks*

Received date: 16 October 2015
Revised date: 29 March 2016
Accepted date: 12 June 2016

Please cite this article as: Christian T. Zenger, Mario Pietersz, Jan Zimmer, Jan-Felix Posielek, Thorben Lenze, Christof Paar, Authenticated Key Establishment for Low-Resource Devices Exploiting Correlated Random Channels, *Computer Networks* (2016), doi: 10.1016/j.comnet.2016.06.013

Authenticated Key Establishment for Low-Resource Devices Exploiting Correlated Random Channels

Christian T. Zenger[1,2], Mario Pietersz[1,2], Jan Zimmer[2], Jan-Felix Posielek[2], Thorben Lenze[2], Christof Paar[2]

[1]*PHYSEC GmbH, Universitätsstr. 150, 44801 Bochum, Germany,* www.physec.de
{christian.zenger, mario.pietersz}@physec.de
[2]*Horst Görtz Institute for IT-Security (HGI), Ruhr-University Bochum, Germany*
{jan.zimmer, jan-felix.posielek, thorben.lenze, christof.paar}@rub.de

Abstract

Authenticated key establishment is a central requirement for securing IoT devices. For efficiency and management reasons, it might be desirable to avoid public-key-based solutions that are ubiquitous in traditional Internet settings but have many drawbacks for resource-constrained (RC) nodes. We introduce a novel *Vicinity-based Pairing* (VP) mechanism that allows authenticating arbitrary 'unloaded' RC-nodes by delegating trust from already authenticated and secured, we call it 'loaded', RC-nodes. For authenticating RC-nodes, VP exploits the correlation between channel profiles from devices that are in close physical proximity. In our setting, only devices that are within a few centimetres from the 'loaded' RC-nodes are authenticated after a user initiates such a process. Subsequently, the embedded end device can extract an unique shared symmetric key with another device such as a SCADA gateway, again by exploiting channel parameters. Based on extensive experiments, we propose new techniques for extracting time-varying randomness from channel parameters for use in VP. We describe the first MITM-resistant device pairing protocol purely based on a single wireless interface with an extensive adversarial model and protocol analysis. We show that existing wireless devices can be retro-fitted with the VP protocol via software updates, i.e. without changes to the hardware. Implementation results of our embedded prototype demonstrates that the approach has the potential to dramatically reduce the cost and efforts of securing low-resource devices that are common in the IoT.

Keywords:
Authenticated key agreement over wireless channels, experimental results, proximity-based pairing, embedded implementation

1. Introduction

We are in the midst of the evolution towards the Internet of Things (IoT). Myriads of resource-constrained (RC) nodes from a wide spectrum of applications will communicate with each other. A surprisingly large number of IoT systems will be security sensitive, e.g., automotive controllers, medical devices, supervisory control and data acquisition (SCADA) systems, and many other resource-constrained cyber-physical systems in smart factories. It is thus paramount that future IoT applications are equipped with security mechanisms. Also, to enjoy a broad acceptance, a crucial requirement for securing the IoT is ease-of-use. We present a detailed approach solving what is arguably the most difficult part in the majority of security systems, namely entity authentication and key establishment. The system offers an easy way of providing shared secrets for wireless nodes, which covers many IoT systems and also many other, non-IoT, applications. Therefore, we utilize complex-valued channel properties to establish symmetric key material and to tag key material with proximity based authentication flags. This allows us to overcome the many drawbacks of PKI-based key management for embedded environments, including costly asymmetric crypto operations and *certificate revocation lists* (CRLs). In contrast to previous systems that attempt to use physical channel properties for the key establishment, the solution at hand is resistant against active MITM attackers and provides implicit device authentication. Therefore, the presented approach extends works which exploit proximity-dependent properties of the communication channels between two or