IT | SECURITY
RESEARCH GROUP

Secure Pairing

"Getting from nothing to something"

Johannes Gilger <Gilger@UMIC.RWTH-Aachen.de>
RWTH Aachen University

Smart Object Security Workshop, 23 March 2012

Introduction

Definition / Terminology

Secure Pairing: Definition

> *Secure Pairing is the process of bootstrapping a secure communication channel between two previously unassociated electronic devices communicating over some insecure channel.*

Terminology

- *Devices*: Smart Objects, PCs, routers, smartphones
- *Channel*: IEEE 802.15.4, IR, NFC, Buttons, LEDs

We need to talk about Secure Pairing for Smart Objects because ...

- these devices sometimes lack even the most basic user interfaces.
- current pairing approaches would simply take too long for Smart Objects.
- certain assumptions regarding security may no longer hold.

Problem statement

What we need

We need a channel between two devices that provides integrity (not confidentiality). This channel will be used to exchange a shared secret (Diffie Hellman), which is used to authenticate any subsequent DTLS handshake. Pairing two devices over this channel should be relatively quick (a few seconds) and easy to perform for untrained personnel. The owner of the Smart Object has to be able to confirm that the object was actually paired with him (i.e. nobody ''stole'' it).

These will likely not work with Smart Objects

- Lack of interface: Comparing PIN, reading/entering PIN, creating PIN
- Cost/Power: Aux. channel exchange: NFC, Bluetooth, IR
- Security: Vulnerable period, fixed PIN

Pairing schemes

Schemes, not protocols!

IT | SEC

Interesting and realistic avenues of research in my opinion

- CGAs: Secure storage for private key needed (PUF, TPM-like). Scales well.
- In-Band Pairing: No addtl. interface needed, question of applicability for IEEE 802.15.4.
- Out-of-Band: Button-to-Button, LED-to-Button. Nice and easy, yet time-intensive.
- Proximity-based: RF signal propagation characteristics, distance bounding.
- RF-fingerprinting: reliably re-establish the identity of a radio signal using transients.

Things to discuss

- How do the secure pairing schemes fit into protocols and roles?
- What kind of attackers and attacks do we want to protect against?
- How do realistic deployment scenarios look like in the industry?