A Configuration Protocol for Embedded Networked Devices on Secure Wireless Networks

Larry M. Sanders, Joseph B. Evans
Info. & Telecom. Tech. Center
University of Kansas
Lawrence, Kansas 66045
{lsanders, evans}@itc.ku.edu
www.itc.ku.edu

Benjamin J. Ewy
Ambient Computing, Inc.
Lawrence, Kansas 66047
bewy@ambientcomputing.com
www.ambientcomputing.com

Seventh Annual Workshop on High Performance Embedded Computing
September 2003

University of Kansas
Motivation

Wireless networks based on the IEEE 802.11 standard require lengthy layer two configuration parameters to be set

SSID (Network Name)
WEP Encryption Keys

Embedded devices with limited input capabilities are unable to join the wireless network until properly configured

Traditional layer three configurations protocols like DHCP can be utilized once data layer communication is established
802.11 Encapsulation

- 802.11 headers are unencrypted
- Access Points copy MAC addresses during the bridging process
- Data portion encrypted
  - No use to a station without keys
- Source address - 6 octets of data
- Broadcast
Wi-Fi-Co Protocol

The Configurator host sends wireless network parameters to an embedded device via broadcast packets.

A Wi-Fi station is able to capture the configuration frames and assemble the data from the cleartext 802.11 headers.

- **Header**: Cont., Identifier, Data
- **MAC Source Address**: ff ff ff ff ff ff ff
- **MAC Destination Address**: ff ff ff ff ff ff ff
- **Broadcast**

**Wi-Fi-Co Configuration Buffer**

- **SSID**: Configuration data is embedded in the source MAC address.
- **WEP KEY(s)**
- **Default Key**
- **Integrity Check**

**802.11 MAC Header**

- **Frame Control**
- **Duration**
- **Addr 1**
- **Addr 2**
- **Addr 3**
- **Seq**
- **Addr 4**
- **WEP IV**
- **DATA**
- **FCS**

**Cleartext**

- **Encrypted**
- **Cleartext**

---

University of Kansas
Wi-Fi-Co Timing Diagram

- **Configurator** constantly broadcasts configuration data in fragmented packets
- The **target** assembles configuration data and decodes link level parameters
- Must “hop” Wi-Fi channels to guarantee that configuration data will be received

University of Kansas
Protecting WEP Keys

- Broadcast packets easily intercepted
  - On wired Ethernet network portion
  - On wireless network portion

- Configuration data Encrypted
  - Shared key symmetric cipher
  - Embedded devices ship with unique, pre-programmed key
  - Certificate with product code
  - Additional input required on the Configuration host where it is much easier than input to embedded device