Strong Data Security Over *Bluetooth*

1. Introduction

New wireless data security guidelines are being discussed by the Payment Card Industry Data Security Standard, PCI DSS. Currently, with the formation of a Special Interest Grougp, SIG, they are reviewing the security needs and weaknesses found in WiFi wireless networks used for payment applications. *Bluetooth*, is also gaining strong market acceptance in the payments industry, and similar guidelines will likely be applied soon.

In order to advance *Bluetooth* wireless applications into this area now, Amp'ed RF is presenting a scheme for strong data security over a *Bluetooth* system, *BlueGuard*, described in this paper.

2. Scope

This document will present a strong data security scheme which may be incorporated into an application and/or system using *Bluetooth* technology for card payment data communication. New *Bluetooth* profiles or standards are not suggested in this document. *BlueGuard* is an application product designed by Amp'ed RF, Inc.

3. Standard *Bluetooth* Security Gaps

According to a recent commissioned security review, conducted by InfoGard Laboratories, Inc., *Bluetooth* v2.1 was not found to be compliant with FIPS 140-2, Level 3. The deficiencies were determined to be:

1. The FIPS Level 3 authentication model requires identification of individual users and proof of authenticity of such users using one or more authentication factors (something you know, something you have or something you are).
    - *Bluetooth* technology does not enforce prior knowledge of an operator (user) and the secret used to authenticate such operator, but rather allows anonymous link authentication using SSP.
2. FIPS requires the use of specific ciphers such as AES
    - *Bluetooth* technology uses a SAFER+ block cipher which is not on the FIPS 140-2 approved list
    - *Bluetooth* technology uses E0 stream cipher which is not on the FIPS 140-2 approved list
3. FIPS requires the use of 80+ bits of entropy in all connections
    - *Bluetooth* supports negotiable key sizes (56 and 128bit)

Bluetooth devices are able to address these gaps through application specific security measures, such as *BlueGuard*.

3.1. Mutual Authentication

The first deficiency of standard *Bluetooth* is due to lack of user authentication. The *BlueGuard* application enforces a strong mutual authentication, using a data encryption key.

Mutual Authentication Steps:

1. Remote device initiates *Bluetooth* connection.
2. *BlueGuard* issues a security challenge.

3. A random phrase is exchanged and mutually validated using 3-DES encryption.
4. The *Bluetooth* connection is allowed to proceed once the challenge is passed, or blocked if the challenge fails.

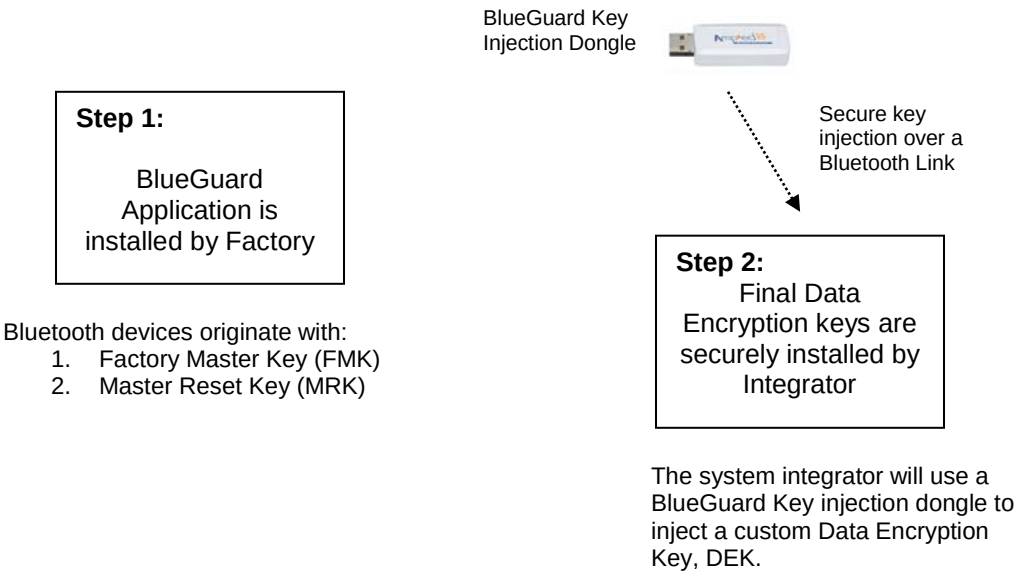
3.2. 3-DES Encryption

BlueGuard uses a 3-DES cipher, with a 16 byte, double length key strength. A 24 byte key is also optional. This fulfils the FIPS 140-2, Level 3 requirements for encryption algorithm and key strength.

The native link level security of *Bluetooth* is not sufficiently strong for the PCI industry.

4. Key Management

One of the main security features of an encryption scheme, is to enforce a proper Key Management. In order to support this, *BlueGuard* requires a hardware device, a *BlueGuard* Key Injection Dongle, to use while injecting the DES keys.



- Initially, the key loaded at Amp'ed RF will be the Factory Master Key, FMK: 16 byte key.
- When delivered to a customer/installer, they will replace the FMK, with a Data Encryption Key, DEK: 16 bytes key.
- A Master Reset Key is also supported, to erase a DEK. This key will not be supplied to customers.

4.1. Key Injection Dongle

BlueGuard does not expose the FMK, but rather requires a Key Injection dongle. Using a PC and this dongle, a customer is able to securely inject a set of final keys, DEK, into the device. Without the DEK, *BlueGuard* will not allow *Bluetooth* connections.

4.2. DEK Replacement

A DEK may be replaced or re-keyed using the same Key Injection dongle, while the DEK is known.

4.3. Master Reset Key

BlueGuard supports a MRK used to re-issue equipment or recover from lost DEKs.

4.4. Session Keys

As part of the Mutual Authentication process, a successful Challenge result produces as Session Data Encryption Key, SDEK. This 16 byte key, is used on the data link.

5. System and Public Network Protection

The local card usage wireless network is protected with *BlueGuard* encryption. However, in many systems, a cellular phone or *Bluetooth* Ethernet bridge device will be used to route the card data over a WAN or public network. Data that is transmitted beyond the local card usage environment should also be protected by this encryption system. The terminating server or device will then be able to decrypt transaction data safely.