An ALLIED UNIVERSAL® Company

DESFire Hack & Solutions
White Paper

FIPS 201 COMPLIANT SOLUTIONS: FROM CARD ISSUANCE OPERATIONAL USE

Introduction

In June 2011, a group from a German university presented at RFIDsec (an RFID security conference) a methodology for a hack of the common NXP Mifare DESFire security. In the hack, a method called Differential Power Analysis was used to ascertain the symmetric key value of an encoded DESFire card. The hack was demonstrated to be successful at a separate conference (CHES Workshop) in September 2011.

This document describes the attack in simplified terms, identifies what cards are subject to this attack, elaborates on what the availability of this attack means to customers using DESFire card, and provides recommendations for a solution.

While it may be of concern that thieves may have tools to read, or perhaps write, to cards unbeknownst to those in possession or in charge of such credentials; the reader should have their mind put at ease to know that the attack is fruitless against DESFire cards encoded through Symmetry.

The Attack

A group from the University of Bochum, led by Professor Paar, is one of the largest groups in Europe working in the field of security of embedded systems. The group specializes in an area called "Side Channel Attacks". A Side Channel Attack (SCA) is any one of a variety of methods that don't try to read or write the card directly. Instead, they measure the power consumed by the card reader, or they measure the electromagnetic field around the card and reader during a communication session. These other measurements are then associated with information about the operation of the card as determined in the laboratory. In effect, they look for patterns during real operation that match patterns they have observed in the laboratory and make inferences from those observations.

The particular SCA that was used is the Differential Power Analysis (DPA) Attack. The DPA does not damage the card or reader in any way, so would not leave any indication that the card was attacked, nor would the card know it had to protect itself.

Concerns for Use in Practice

The DPA attack requires well controlled laboratory settings and cannot be performed in a casual manner in a typical card use scenario. The attack also cannot be performed by simply walking past a cardholder. The attack typically takes from hours to days to collect and analyze the data.

DESFire Cards

The DESFire card attacked was the MF3ICD40 ("D40"). This is the version of Mifare DESFire that has been around since the late 1990's. This card is in wide use but has been in a phase out plan by the manufacturer (NXP) since June 2010. The last product delivery for this chip/card will be June 2012. Future orders will be replaced by the DESFire EV1. The EV1 version has been certified for Common Criteria EAL 4+ (and thus is immune to the specified DPA attack) and is backward compatible with systems that use the D40 cards. Therefore, Symmetry users can easily migrate to the more secure card.

How to Avoid the Attack

First, and foremost, the readers should know that the attack can only determine the symmetric (secret) key as transmitted by the reader. Therefore, the most that could be ascertained during a read of the Symmetry encoded DESFire card is the read key of the card – the secret key needed to read the card number. Furthermore, since Symmetry uses "key diversification" (a means by which the secret key on each card is unique) the DPA attack would only be able to read the secret key of the one card – thus limiting the risk exposure to the facility.

The DPA attack is not a new attack. The science behind this attack has been well understood for many years, however, the situation remains that the attack requires significantly controlled environment of a laboratory setting. Furthermore, since such an attack is understood, various smart card certification standards such as Common Criteria (at EAL 4+) test for these types of attacks. Therefore, cards that have undergone this level of security certification are immune to such attacks.

There are a variety of countermeasures to the DPA attack:

- Key diversification – as explained, Symmetry utilizes this mechanism. This limits the information attained to only be valid on the individual card. Other cards have different keys and would reject the key retrieved from the compromised card.

- Card + PIN use – Symmetry supports two-factor authentication which employs not only the card (something you have), but also a PIN (something you know). The DPA attack would not be able to determine the PIN since this is done at the reader and does not rely on the card. If a compromised card were used in a card + PIN scenario, a wrong PIN error message would be transmitted to the server. This can be used to detect fraud and inactivate the card.

- Use an electromagnetic shield when card is not in use. Such a shield is standard issue for cards issued by the federal government under FIPS 201. This is also the standard for cards issued by U.S. Customs and Border Patrol and is the standard for ePassports issued by a number of countries.

- Migration to the DESFire EV1 card – the EV1 variant of the DESFire card family is Common Criteria certified and is not subject to the DPA attack described in this paper. This finding was included in the technical document submitted to the CHES group. Symmetry offers an expiration date for the cards, and part of the migration plan can be to have all existing D40 cards expire over time and replace them with the EV1 card.

REVISION HISTORY
14 November 2011 Initial draft release, Issue 0.1