INTERNATIONAL JOURNAL OF ENGINEERING AND MANAGEMENT SCIENCES
© 2004 -14 Society For Science and Nature (SFSN). All Rights Reserved
www.scienceandnature.org

Short Communication

THREATS CAUSED BY SIM CARD HACKING AND THEIR REMEDIES

Kour Tejasvit,
Chandigarh Group of Colleges, India

ABSTRACT
We present a set of twelve principles in management manifesting, used in public universities in some developing countries. The scientific base of the arguments and results demonstrate the efficacy and efficiency of those principles

KEYWORDS: Sandboxing, Cryptography, Homerouting, DES

INTRODUCTION

About 7 billion SIM cards are used worldwide. SIM i.e. Subscriber Identification Number is a small card that is inserted into; a device that authenticates commands and software updates. Even though SIM cards are believed to be safe from hacking but recent studies have proved that even SIM cards are being hacked and misused. It is estimated that one SIM in every eight SIM cards can be hacked i.e. around half billion SIM cards can be hacked.

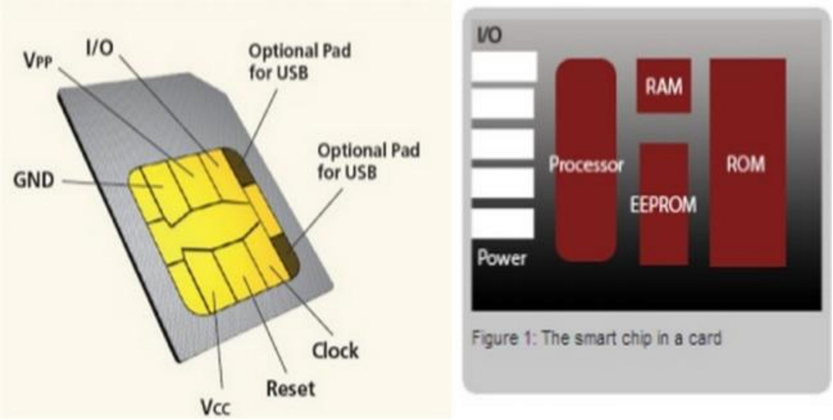


Figure1

Owing to the worldwide usage of SIM cards for example in online banking and other sensitive personal information, SIM card hacking can prove to be very serious privacy disaster.

Various ways in which SIM card hacking can prove to be a serious threat

Severe implications for business world

With the latest trend of business data being shifted from PCs to mobile devices, employees carry tons of important data in their mobile phones. Hence hacking of these mobiled devices via SIM cards can prove to be a weak link. With the increasing popularity of phone based business hackers can interfere with the payments and the amounts involved which can totally disrupt the transactions involved.

Millions may be affected worldwide

Recently a bug has been discovered that allows hackers to duplicate mobile cards and gain their complete access and control. This bug has been considered to be quite a significant one which can be used for electronic spying and financial offences. Various telecommunication managers and other government agencies have been informed about the possible danger in nearly 200 countries to reach out to 100s of mobile companies and other industry specialists. SIM card hacking may be caused due to a number of reasons. Here are some of the main reasons responsible for SIM card hacking:

Outdated encryption standard:

Many SIMs use an encryption standard which is old and dated from the 70s time. It is called the data encryption standard (DES). It is considered to be a weak form of encryption because it is easy to discover the private key which is used to sign content. Thus weak encryption is one of the first causes of SIM card hacking. New encryption standards must therefore be used and old ones totally abolished.

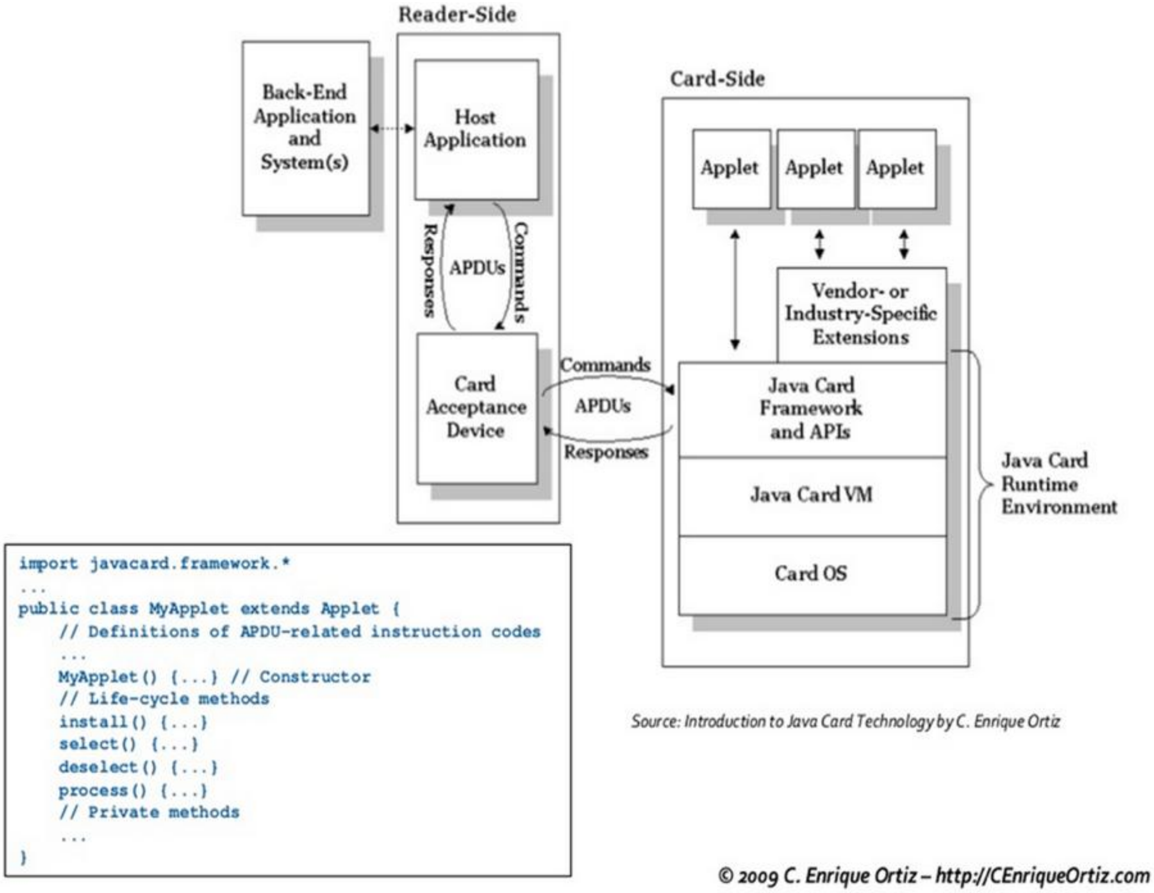
Cracking SIM update keys:

Researchers at the Security Research lab conducted an experiment in which a binary code was sent through SMS to a device using a DES SIM. The code was not signed cryptographically in a proper way so the code would not run on the device. But when the code was rejected, the

SIM made a major error. It sent back over SMS an error code that contained its own 56 bit private key. This took place because the SIM used DES which is a weak encryption form .hence it is possible to decrypt private keys using any of the familiar cracking technique.

Java Sandboxing

Java card is a programming language which is used on over 6 billion SIM cards worldwide. Java card uses a concept which is called 'sandboxing'. A sandbox is a kind of security measure or a set of rules that are used when an applet is created and it prevents several functions when this applet is sent as part of webpage. This sandboxing mechanism is broken in most of the SIM cards. The researchers have found a few cases in which the SIM card protocols allowed the virus sent to the SIM to check the files of an app that was installed on the card**.**



```
import javacard.framework.*
...
public class MyApplet extends Applet {
    // Definitions of APDU-related instruction codes
    ...
    MyApplet() {...} // Constructor
    // Life-cycle methods
    install() {...}
    select() {...}
    deselect() {...}
    process() {...}
    // Private methods
    ...
}
```

Source: Introduction to Java Card Technology by C. Enrique Ortiz

© 2009 C. Enrique Ortiz – http://CEnriqueOrtiz.com

To summarize, a hacker who wants to use this method may start with around 100 phones. A binary SMS can be sent to all of them with the help of a programmable cell phone which is connected to a computer. Approximately they might get a total of 25 responses having cryptographic signatures and half of them are dismissed because of high security standards. From the remaining encryption key of around 13 can be cracked and a virus can be sent that is able to break through the java sandbox barriers and is able to read the master keys of the SIM card and payment application details. It is believed that java sandboxing is a fault of the chief SIM card vendors like Oberthur and Gemalto. Even though inefficient cryptographic and other shortcomings pose a threat of SIM card hacking, still SIM card hacking can be controlled by using the methods described below:

SMS firewall

An extra layer protection layer can be affixed in handsets. The user should be able to differentiate which binary SMS is to be selected and which to be rejected. SMS fire wall can also other situations like 'silent SMS'.

SMS filtering

Generally hackers depend on networks for the exchange of binary networks to and from the target victim phones. Such exchange of SMS should be allowed only from a few reliable sources. But the problem is that most networks have not implemented this type of filtering. Home routing which is a technique used by mobile networks in SMS reception process should provide more protection to customers while roaming. This would also be helpful in providing protection against remote tracking.

Improved SIM cards

It is required that the SIM cards need to have cryptography with sufficiently long keys, and the signed plain text to attackers should not be disclosed and also secure java virtual machines must be implemented. Various techniques have come around over the years in this regard. But more steps and measures need to be taken.

CONCLUSION

To conclude SIM card hacking poses a a serious threat to mobile phones and hence proper measures should be taken. Newer encryptions should be upgraded by the carriers. This will not only ensure safety of users but proper revenue too. OTA protocol should be used by payment providers like Master card and Visa to fill SIM cards with java applications for example java based applets. SIM card hacking can be controlled without much problem if proper measures are taken.

REFERENCES

Hacking mobile phones by Ankit Fadia

Hacking the art of exploitation by Jon Ericson

Hacking exposed 7 by Stuart Mcclure,Joel Scambray,George Curtz

www.edition.cnn.com/2013/08/01/tech/mobile/SIM-card-hac

www.endgadget.com

www.pcworld.com

Violent python by TJ o'Connor

Hacking secret ciphers with Python by Al Sweigart