International Journal on Recent Researches in Science, Engineering & Technology (IJRRSET)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. Journal Indexed in JIR, DIIF and SJIF.
Available online at: www.jrrset.com

Received on: 03.9.2015 Published on: 2.10.2015 Pages : 33-37

ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

Volume 3, Issue 10
October 2015.
JIR IF : 2.54
SJIF IF : 4.334
Cosmos: 5.395

SECURE AND FLEXIBLE AUTHENTICATION FOR DENIABLE ENCRYPTED STORAGE SYSTEM

[1] K.Arun Prasad [2]K.Pushpavalli [3] G.Keerthana
[1] Associate Professor, Department of Information Technology,
Agni College of Technology, Chennai, India
[2] Assistant Professor, Department of Information Technology,
Agni College of Technology, Chennai, India
[3] Assistant Professor, Department of Information Technology,
Agni College of Technology, Chennai, India

Abstract -- Deniable storage encryption mechanisms exist for PCs. However, at the time of writing this dissertation, no such system is available for mobile devices. The tight-coupling between mobile device hardware and software, along with the boot procedure, and distinctive storage features do not lend themselves to simply porting existing PC PDE schemes. Mobile devices also open up new existence-leakage vectors, and sources of compromise that can betray deniability. To assess the feasibility and efficacy of PDE for mobile devices, and address the aforementioned obstacles, the scheme was designed and implemented for the Android OS. We analyse the performance of the prototype on two mobile devices. We also explore the sources of leakage inherent to mobile devices that may compromise deniable storage encryption. Several of these leakage vectors have notbeen analysed for existing desktop PDE solutions. It is unrealistic to expect a user to remember 64 random bytes, so random keys are often protected by encrypting them with a password-derived key. This reliance on user-chosen secrets to protect encryption keys reduces the overall security of the cipher to the complexity of the password. This problem is compounded, as users tend to choose poor passwords, such as short numeric PIN codes, on mobile devices, to contend with constrained input mechanisms. Data confidentiality can be effectively preserved through encryption.

Index Terms—File system security, mobile platform security, storage encryption, deniable encryption.

1.Introduction

Smart phones and other mobile computing devices are being widely adopted globally. For instance, there is more than 119 million smart phone users in the USA alone, as of November 2012. With this

increased use, the amount of personal/corporate data stored in mobile devices has also increased. Due to the sensitive nature of this data, all major mobile OS manufacturers now include some level of storage encryption. Some vendors use file based encryption, such as Apple's iOS, while others implement full disk encryption (FDE).

Google introduced FDE in Android 3.0 FDE is now available for all Android 4.x devices, including tablets and smart phones. While Android FDE is a step forward, it lacks deniable encryption a critical feature in some situations, e.g., when users want to provide a decoy key in a plausible manner, if they are coerced to give up decryption keys. Plausibly deniable encryption (PDE) is used for parties to communicate over a network. As it applies to storage encryption, PDE can be simplified as follows: different reasonable and innocuous plaintexts may be output from a given cipher text, when decrypted under different decoy keys. The original plaintext can be recovered by decrypting with the true key. In the event that a cipher text is intercepted, and the use is coerced into revealing the key, she may instead provide a decoy key to reveal a plausible and benign decoy message. Our contributions: The main contributions of are the following: We explore sources of leakage inherent to mobile devices that may compromise deniable storage encryption. Several of these leakage vectors have not been analyzed for existing desktop PDE solutions.

We present the PDE scheme based on hidden encrypted volumes the first such scheme for mobile systems to the best of our knowledge. We introduce two variants of to address several challenges specific to different Android hardware profiles.

2. Preliminaries

APDE-enabled storage encryption system is used for the Android OSes. It includes countermeasures for known attacks against desktop PDE implementations. We also explore challenges more specific to using PDE systems in a mobile environment, including: collusion of cell phone carriers with an adversary; the use of ash-based storage as opposed to traditional magnetic disks; and systems such as Ext4 (as used in Android) that are not so favourable to PDE. It addresses several of these challenges. However, to effectively offer deniability, it must be widely deployed, As such, we implement our prototype to be compatible with Android 4.x.15.

3. Existing work

True Crypt is a discontinued source-available freeware utility used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition or the entire storage device.

Disadvantages of Existing work

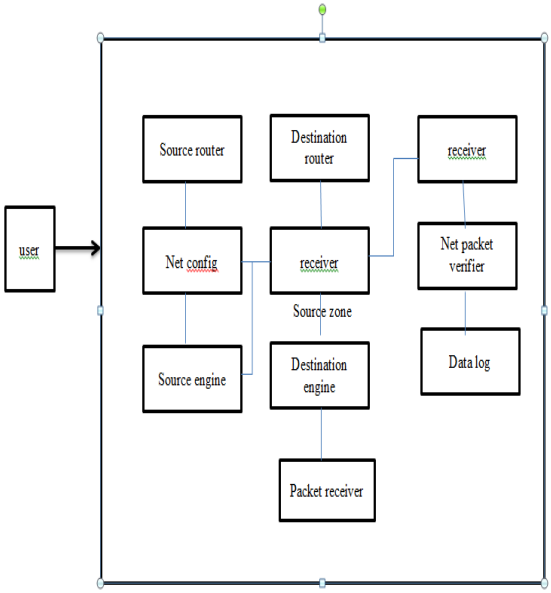
- Encryption keys stored in memory
- Physical security
- Malware
- Incompatibility with other security software

4. Proposed Solution

The proposed system aims the incorporation of secure and reliable mechanism of data transfer in the network environment. Deniable encryption ciphers are classified in three ways,

- By which parties are being coerced (sender, receiver, or bi-deniable)
- By the underlying encryption schemes (symmetric or public-key)

- By the time at which the decoy messages can be created/either at the time of coercion (ad-hoc), or at the time of encryption (plan-ahead).
- It is a plan-ahead construction, in that the user must decide on a fixed number of decoy messages. Mobiflage is a plan-ahead construction, in that the user must decide on a fixed number of decoy messages. The advantages of proposed system, Incorporation of reliable and secure mechanism.
- Data and File system is injected with data security.
- AES / DES / PDE standards. Incorporation of Engines to handle the security and perform data integration in a seamless manner
- The dynamic model dominates interactive interfaces. Objects in the model represent interaction elements, such as input and output tokens and output formats. The functional model describes which application functions are executed in response to output event sequences, but the internal structure of the function is usually unimportant to the behavior of the interface.



4.2 Architecture Diagram

4.2.1 Description

When the user sends data or file, it reaches sender zone. Sender zone includes source router, network configuration and source engine. Source router routes the file to the specific destination router and network configuration creates the network for file transmission. Source engine encrypts the file data by using AES and DES algorithm, which provides the data security. Destination includes destination router, engine and packet receiver. Destination engine decrypts the encrypted data and packet verifier confirms that all the packets are received without data loss.

5. System Implementation

List of Modules

The work flow of the proposed system is divided into five modules such as

1. Authentication

2. Routing Engine
3. Security Engine
4. PDE

5.1. Authentication

Authentication is the act of confirming the truth of an attribute of a single piece of data or entity. It might involve confirming the identity of a person by validating their identity documents, verifying the validity of a Website with a digital certificate, tracing the age of an artifact by carbon dating, or ensuring that a product is what its packaging and labeling claim to be. One of their solutions uses a series of covers initially filled with random data, and assumes the attacker has no knowledge of the plaintext content of a file.

5.2 Routing Engine

The routing engine is implemented as a Java 2 Enterprise Edition (J2EE) Web application that you can deploy in either an Oracle Application Server or standalone Oracle Application Server Containers for J2EE (OC4J) environment.

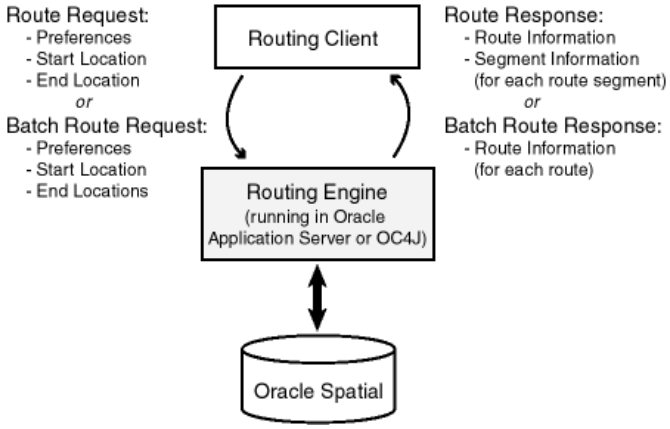


Figure 5.1 Spatial Routing Engines

5.3 Security Engine

The binary form of programs running on the Java platform is not native machine code but these files must be relatively large but an intermediate byte code or junk data. The JVM performs verification on this byte code before running it to prevent the program from performing unsafe operations such as branching to incorrect locations, which may contain data rather than instructions.

5.4 Plausibly Deniable Encryption

Plausibly deniable encryption describes encryption techniques where the existence of an encrypted file or message is deniable in the sense that and versify cannot prove that the plaintext data exists. The file system meta-data blocks are:

(a) The backup super blocks and group descriptor tables in sparse lock.
(b) The block/node bitmaps and in node tables in all block groups.

6. Performance

Performance analysis chart is in progress.

7. Conclusion

Mobile devices are increasingly being used for capturing and spreading images of popular uprisings and civil disobedience. To keep such records hidden from authorities, deniable storage encryption may offer a viable technical solution. Such PDE-enabled storage systems exist for mainstream desktop/laptop operating systems. Mobiflage's design is partly based on the lessons learned from known attacks and weaknesses of desktop PDE solutions. We compiled a list of rules the user must follow to prevent leakage of information that may weaken deniability. Even if users follow all these guidelines, we do not claim that Mobiflage design is completely safe against any leaks we want to avoid giving any false sense of security.

References:

[1] Skillen and M. Mannan, "On Implementing Deniable Storage Encryption for MobileDevices," Proc., Feb. 2013.
[2] ComScore, "comScore Reports September 2012 U.S. Mobile subscriber Market Share,"2012.
[3] R. Canetti, C. Dwork, M. Naor, and R. Ostrovsky, "Deniable Encryption," Proc. 17th Ann.Int'(CRYPTO '97), 1997.
[4] J. Assange, R.-P.Weinmann, and S. Dreyfus, "Rubberhose: Cryptographically Deniable Transparent Disk Encryption System," Project Website: http://marutukku.org/,1997.
[5] Fruhwirth, "New Methods in Hard Disk Encryption," technical report, Vienna university of Technology, http://clemens.endorphin.org/nmihde/nmihde-A4-ds.pdf, July 2005.