Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.351 – 355

RESEARCH ARTICLE

PLAUSIBLY DENIABLE ENCRYPTION OF DATA STORAGE AS HIDDEN FOLDER IN CLOUD

G.DIVYEDHARSHINI[1], M.AKILA RANI[2]
PG STUDENT, ASSISTANT PROFESSOR
NPR COLLEGE OF ENGINEERING AND TECHNOLOGY, TAMIL NADU, INDIA
EMAIL: *divya11188@gmail.com* , *akilakamalam@gmail.com*

ABSTRACT: *Data confidentiality can be performed through the encryption of data.* ***Confidentiality of data at rest can be effectively preserved through storage encryption. All major mobile operating systems now incorporate some form of storage encryption. In certain situations, this is inadequate, as users may be coerced into disclosing their decryption keys. In this case, the data must be hidden so that its very existence can be denied. Steganographic techniques and deniable encryption algorithms have been devised to address this specific problem.*** *To address obstacles, use Plausibly Deniable Encryption (PDE) in a mobile environment, design a system called Mobiflage. Mobiflage enables PDE on mobile devices by hiding encrypted volumes within random data in a devices free storage space. The lessons learned from deniable encryption in the desktop environment, and designed several counter measures for threats specific to mobile systems. Two implementations have been provided for the Android OS, to appraise the feasibility and performance of Mobiflage on different hardware profiles at any place anywhere.* ***Secure Computing provides a global leader in enterprise security solutions. In security risk management is the most comprehensive and integrated endpoint, gateway, and hybrid security offerings. Steganographic methods and deniable encryption algorithms have been constructing to hide the very presence of encrypted information. The file can be stored in the cloud environment as a hidden folder.*** *Preserving exercises for the Android OS, to appraise the utility and achievement of Mobiflage on various hardware profiles.* ***So the data can be accessed by the person any time by storing it as a hidden folder in the cloud environment.***

Index Terms— File System Security, Storage Encryption, Decoy key and Password, Triple DES algorithm, Plausible Deniable Encryption (PDE)

1. INTRODUCTION

Secure computing has become widely traded process. Over the next several years, Secure Computing morphed from a small defense contractor into a commercial product vendor, largely because the investment community was much less interested in purchasing security goods from defense contractors than from commercial product vendors, especially vendors in the growing internet space. The usage of smart phones is tremendous and the securing of the confidential data from the unauthorized person has to increase in level. To process this method here the hidden folder method has been introduced and stored the file in the cloud environment with some secure key and password. Storing the data in the cloud environment in a secure way is difficult so here with high security process the data is maintained and it is retrieved only the particular person anywhere anytime. Cloud platform is most widely used platform to store the data. This can be accessed through some IP address provided by the cloud environment while creating an account in the environment.

2. LITERATURE SURVEY

2.1. On Implementing Deniable Storage Encryption for Mobile Devices

The users may be coerced into disclosing their decryption keys. The data must be hidden so that its very existence can be denied. Steganographic techniques and deniable encryption algorithms have been devised to address this specific problem. Examine the feasibility and efficacy of deniable storage encryption for mobile devices. This design a system called Mobiflage that enables PDE on mobile devices by hiding encrypted volumes within random data on a device’s external storage.

2.2 Defeating Encrypted and Deniable File Systems: True Crypt v5.1a and the Case of the Tattling OS and Applications

The security requirements for creating a Deniable File System (DFS), and the efficacy with which the True Crypt disk-encryption software meets those requirements. In a DFS, the very existence of certain files and directories cannot be ascertained by the attacker. The results show that deniability, even under a very weak model, is fundamentally challenging. If the adversary continue to demand the file, to disclose the password to such a deniable file system.

2.3 Halting Password Puzzles: Hard-to Break Encryption from Human-Memorable Keys

By throwing a Halting-Problem wrench in the works of guessing that iteration count, we widen the security gap with any attacker to its theoretical optimum. Halting Key Derivation Functions are practical and universal: they work with any password, any hardware, and a minor change to the user interface. It shows how works "pure password"-based encryption can best with stand the most dedicated offline dictionary attacker regardless of password strength. It can be typed quickly and discreetly on a variety of devices, and remain effective in constrained environments with basic input and no output capabilities.

2.4. Reliably Erasing Data from Flash-Based Solid State Drives

Reliably erasing data from storage media is a critical component of secure data management. Verifying digital sanitization operations uses the lowest-level digital interface to the data in a Solid State Drives (SSD). Sanitizing storage media to reliably destroy data is an essential aspect of overall data security. This found that none of the available software techniques for sanitizing individual files were effective.

2.5. Baseband Attacks: Remote Exploitation of Memory Corruption in Cellular Protocol Stacks

The practical exploitation of memory corruptions on this processor has become a time-consuming endeavor. The risk is demonstrated remotely exploitable memory corruptions in cellular baseband stacks. Two widely deployed baseband stacks and it give exemplary cases of memory corruptions that can be leveraged to inject and execute arbitrary code on the baseband processor.

3. CONCLUSION

In certain situations, users require a level of protection beyond the semantic security that is offered by encryption. Deniable encryption techniques can be used to augment standard encryption, to contend with a coercive adversary. This dissertation examined the feasibility and efficacy of deniable storage encryption for mobile devices. The Mobiflage tool was designed and prototyped to assess the effective security and usability of the mobile deniable storage concept. The results are promising, as Mobiflage addresses several leakage vectors while incurring a tolerable impact on performance and usability. The implementation relies on a conscientious user that will adhere to usage guidelines devised to prevent leakage or compromise through inappropriate behavior. One such directive is to choose a high entropy password to protect the volume encryption keys. This dissertation also discussed a new password scheme for that specific purpose. So that the file can be maintained in a high secured way from the hackers through hidden folders in cloud environment.

REFERENCES

[1] A. Skillen and M. Mannan, "On Implementing Deniable Storage Encryption for Mobile Devices," Proc. Network and Distributed System Security Symp. (NDSS '13), 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'l Cryptology Conf. Advances in Cryptology (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] Toronto Star, "How a Syrian Refugee Risked His Life to Bear Witness to Atrocities," News Article, http://www.thestar.com/ news/world/article/1145824, Mar. 2012.