Protecting Digital Evidence Integrity by Using Smart Cards

Shahzad Saleem and Oliver Popov

Department of Computer and Systems Sciences, DSV Stockholm University
Forum 100, SE-164 40 Kista, Sweden
shahzads@dsv.su.se, popov@dsv.su.se

Abstract. RFC 3227 provides general guidelines for digital evidence collection and archiving, while the International Organization on Computer Evidence offers guidelines for best practice in the digital forensic examination. In the light of these guidelines we will analyze integrity protection mechanism provided by EnCase and FTK which is mainly based on Message Digest Codes (MDCs). MDCs for integrity protection are not tamper proof, hence they can be forged. With the proposed model for protecting digital evidence integrity by using smart cards (PIDESC) that establishes a secure platform for digitally signing the MDC (in general for a whole range of cryptographic services) in combination with Public Key Cryptography (PKC), one can show that this weakness might be overcome.

Keywords: Digital Evidence, Integrity Protection, Smart Card, Message Digest, Digital Signature, Forensics Examination Tools and Procedures.

1 Introduction

RFC 3227 [1] and IOCE's guidelines [2] describe the procedures of forensic examination with an emphasis on gathering and preserving digital evidence. Indeed, RFC 3227 outlines the entire process of collection and archiving digital evidence starting from the principles that should be observed during evidence collection to the tools eventually required. One of the major things stressed in the RFC document is the need for tools that would ensure integrity of the collected and archived digital evidence such as programs to generate checksums and signatures. The implication is obvious, namely even if all the prior steps follow the recommendations; integrity of the evidence is not necessarily protected. This makes protection of the integrity one of the key elements in digital evidence preservation.

Several vulnerabilities and methods to forge integrity have been discussed in [3] [4] [5] [6] [7] [8]. Moreover, message digests alone are not enough to ensure integrity [8], as one can forge them. Considering these factors, one of the solutions to protect integrity of digital evidence is proposed by Seokhee Lee [8] which depends on digital signatures as shown in Figure 1.

I. Baggili (Ed.): ICDF2C 2010, LNICST 53, pp. 110–119, 2011.

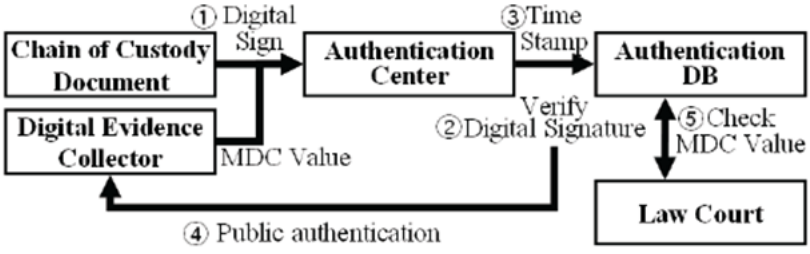

Fig. 1. MAC Authentication Method Scheme [8]

This scheme relies on an assumption that no one can generate a proper and verifiable digital signature without knowing the private key of a relevant entity. When an insecure environment such as a PC is used for safekeeping and/or using private key for cryptography services then there is a possibility that an adversary can steal it. Hence, the core assumption of the scheme is undermined and so is the trust in digital signatures, which points towards the necessity of keeping and using private keys in a secure environment.

It appears that the concept of a Smartcard is an excellent candidate for the aforementioned secure environment. As Smart Card Alliance (SCA) points out that, [9] *"Smart Card is a device with its own embedded integrated circuit chip acting as a secure micro controller with internal memory"*. It connects intelligently and securely to a card reader for storing and or carrying out on-card processing such as encryption, decryption, signing, verification and authentication etc. Smart card technology conforms to international standards ISO/IEC 7816 and 14443.

This paper is organized in seven sections including references. While the current, first, section explains the problem and provides the basic idea behind our approach and solution to the problem of digital evidence integrity protection, second and third sections deal with the current practices and their shortcoming. Then we proceed explaining our model (or solution) PIDESC and how it works. Fifth section analyses the proposed solution and contrasts it with other solutions present in the market against several criteria that range from cost to time complexity. The paper ends with the conclusions and some directions on possibilities for continuing this work in the future.

2 Current Practices for Integrity Protection

A brief discussion of the integrity protection offered by FTK Imager 2.9 [10] and Encase [11] is the subject of this section.

2.1 Integrity Protection by FTK Imager 2.9

FTK Imager 2.9 [10] facilitates forensic extraction of an image of a whole drive or contents of a folder and then exports it into four different formats namely AD1,

RAW, SMART and E01. Integrity of the digital evidence is ensured by generating MD5 and SHA1 Digital Hashes of the original contents and then appending them at the end of the evidence file. Furthermore, there is an optional encryption operation available to ensure confidentiality of the digital evidence; including the appended hashes based upon either a password or a digital certificate.

FTK Imager documentation suggests using "Write Blocking Hardware" to prevent contamination during data extraction phase.

2.2 Integrity Protection by Encase

EnCase [11] provides a tool to forensically extract an image of whole drive and then save it in E01 format. Integrity of the evidence is ensured by CRC and Digital Hashes such as MD5 and SHA1. Optionally, the digital evidence can also be protected by a password providing confidentiality services to the underlying data.

EnCase, like FTK, suggests using "Write Blocking Hardware" to prevent any contamination during data extraction phase.

3 Problems with Current Practices

As underlined in Section 2, current practices employ CRC and digital hashes to ensure integrity and optional password or certificate based encryption and password protection to ensure confidentiality of the digital evidence and its associated MDCs. These practices can be employed in the following scenarios:

1. Only integrity services are turned on by using digital hashes and CRCs. Following instance scenarios can be discussed in this case:
   - 1.1 Digital Hashes alone are used to ensure Integrity of Digital Evidence as employed by FTK Imager. The intent is to show that it is fairly easy to modify the contents, regenerate the hash value, and replace the original hash with the modified one. The procedure is following:
     - i. Digital evidence is extracted from a USB stick which contained a file with information about "heroin" deal.
     - ii. The word "heroin" is replaced with "sugar"; then the digital evidence is extracted again and the original values in the appropriate loci of original digital evidence file are replaced with the values from corresponding loci of modified digital evidence file which included data items and digital hashes leaving the original time stamps intact.
     - iii. When the modified digital evidence is opened one could notice that the modification went undetected.
   - 1.2 Digital Hashes and CRC are used together to ensure integrity of digital evidence, where CRC is used to ensure integrity at block level and digital hash is used to ensure integrity for all the digital evidence.

     In this scenario, compromising the integrity of the digital evidence is more difficult than the previous case. However, it is still possible to modify the digital evidence without being detected. Namely, we modified

the contents of digital evidence and then CRC was recomputed for the modified blocks. The same was done with the digital hashes for the modified contents and replaced effected CRCs and Digital Hashes with the modified one.

The experiment was repeated with the addition of CRCs and produced the same results.

2. Digital hashes and CRCs are used to ensure integrity, while symmetric or asymmetric encryption or password protection is used to provide confidentiality services. This scenario can be further divided into two different cases:
   2.1 Digital hashes are used for integrity protection and:
      2.1.1 Symmetric encryption is used to provide confidentiality to digital evidence including the digital hashes appended with it such as by using a password as a secret key in FTK Imager 2.9. The problem of modification is harder than the previous scenario (both cases), but it is still possible. The underlying security assumption in this case is that an unintended person will not get hold of the secret key. However, a person with sufficient knowledge and tools can steal or guess the secret key. Passwords used as secret keys in FTK Imager 2.9 and possibility of their compromise is further discussed in the section "Attacks on Passwords."
      2.1.2 Asymmetric encryption is used to provide confidentiality to digital evidence including the digital hashes appended with it. This case is more difficult for attackers than the previous one i.e. 2.1.1. The assumption is that digital certificates are stored in a computer via appropriate software. A user must enter a password to unlock and open the features of the software that is safe guarding digital certificates. The implication is that if someone knows the password used to start the software and can eventually get an access to the stored certificates then he can use them. So this case is reduced to the one examined above denoted with 2.1.1. The safekeeping and security of the password and their subversion by an un-wanted person is discussed in the section "Attacks on Passwords".
3. Digital signatures are used for integrity protection as suggested by [8].Since we are using software based techniques for safekeeping digital credentials, so the case reduces to 2.1.2 or the possibility to modify digital evidence without being detected.

3.1 Attacks on Passwords

One can find the passwords used in above scenarios by employing different strategies such as social engineering techniques (Shoulder Surfing, Dumpster Diving) and other more sophisticated techniques such as the analysis of RAM and virtual memory.

As an experiment, we attacked the password used by Nexus Personal 4.10.2 [12]. The clients of Handelsbanken [13] use this software to maintain and utilize

their private and public key certificates securely. The program works with Internet Browsers such as Internet Explorer, Firefox, Google Chrome, and Flock providing online and internet banking benefits to the Handelsbanken customers.

Encase 6 package was used to capture the contents of the RAM and the contents of Flock Process respectively. Then we analyzed the data to find the password used by Nexus Personal, which was in plain text. In similar manner, pagefile.sys is used as a swap area in Windows operating system. Contents analysis of this file can also reveal the password in plain text.

Hyberfil.sys is used to dump the contents of main memory when system goes on hibernation in Windows. Analyzing the contents of this file can also reveal the password in plain text. There are other artifacts of user activity which can hold clues to the passwords used by such secure stores e.g. Registry Hives, NTUSER.dat etc.

By using the enumerated techniques an illegitimate entity can get hold of a password without being noticed and detected by the legitimate user. This undermines the core security assumption in this paradigm which leaves the Digital Evidence vulnerable to integrity losses.

Nexus Personal is one of the softwares which can be employed to maintain and use digital credentials securely while conducting forensic examination. Our experiments demonstrated that it is not always secure to use software based techniques to store and use digital credentials. This is particularly important when one deals with the probative aspects of digital evidence that can cause significant financial losses and even put human life in peril.

4 The Solution Based on the PIDESC Model

The essence of our proposal, and hence the core of the PIDESC model, is the use of smart cards technology for keeping or maintaining and using digital credentials securely while conducting forensic examination.

The fundamental security assumption in the model is that the loss of smart card will not go undetected. First, it is really hard for an adversary to steal digital credentials from a smart card without stealing the card itself. Stealing a physical entity without being noticed is difficult enough. Moreover, if someone succeeds in stealing a card without being noticed then its absence should be felt by its legitimate user soon enough. The legitimate user can then revoke the keys inside the lost card thus rendering the card useless for any future use.

Following guidelines and standards are considered in solving the problem of integrity protection:

1. Quality Assurance section of IOCE's Guidelines [2] suggests that an organization involved in Forensics Examination should outline and enforce "Competence Requirements" and "Proficiency Testing".
2. Section 5.1.E in IOCE's Guidelines [2] suggests that "An individual is responsible for all the actions taken by him on the digital evidence while it was in his procession."

3. Human intervention should be avoided as much as possible to reduce errors and automated tools should be used as much as possible to produce precise results. It is mandatory that reviewers can assess and evaluate the automated tools being used.
4. Sections 4 and 5 of RFC 3227 [1].

4.1 Pre-conditions

1. PKI is up and running.
2. The organization responsible for the forensic investigation, will issue a smart card to the forensic examiner with his digital credentials embedded in it. Validity of these digital certificates depend on examiner's competence, results of proficiency testing as mandated by "Quality Assurance" section outlined in IOCE's guidelines and other attributes such as time etc.
3. Automated evidence collection tools should be enhanced by adding a service for digital signatures in conjunction with a smart card. This implies that the tool should be able to communicate with a smart card for cryptographic services.
4. Automated evidence collection tool would not operate without initially being able to authenticate its user based on the credentials in the smart card.
5. The tool should be able to communicate with the back end authentication server in the organization and various PKI components.

4.2 Procedure

Following steps are recommended in order to establish strong integrity protection relative to the extracted digital evidence.

1. The forensic examiner should:
   (a) First authenticate himself to the automated forensic tool by using smart card.
   (b) Indicate the tool from where to extract the digital evidence by providing complete description of the corresponding configuration settings.
2. From here automated tool should take control and extract the digital evidence, then
   (a) It should create a digital hash of the contents of digital evidence.
   (b) Tool should communicate with Smart Card to digitally sign the hash obtained from the step above. This Digital Signature Process should also consider information about where, when and by whom the evidence was discovered and extracted thus satisfying a part of requirement outlined in section 4.1 of RFC 3227 (this part requires more research for standardization of format and procedure to incorporate this information into digital signature). Smart card should take this required information from the Digital Credentials saved in it thus reducing examiner's intervention.
   (c) Tool should append this digital signature to the extracted digital evidence.

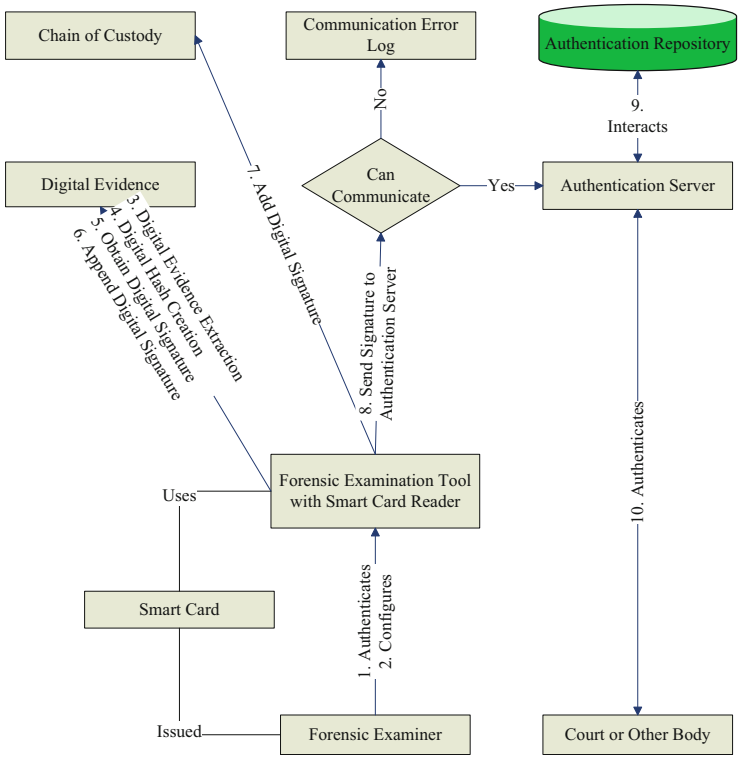

Fig. 2. The PIDESC model and the way it works

(d) Tool should also add this signature to the chain of custody document.
(e) Tool should send the digital signature to organization's authentication server using a secured channel.
(f) If the tool is not able to communicate with the back end server (for instance due to non availability of any communication medium) then it should log the executed processes and list all the reasons for not being able to communicate along with the corresponding time stamps.

3. Authentication server should add a timestamp indicating reception time of digital signature and then store it to the repository of signatures.
4. The organization, institution or any other body which may require verifying integrity of the digital evidence should contact the organization's authentication server of the investigation organization and proceed with the verification.

5 Analysis of Proposed Solution with the PIDESC Model

Results of the analysis of our proposed solution, namely the application of the PIDESC model while considering current practices and other solutions are

provided in Table 1. We have used following criteria: upfront cost, operational cost, time, integrity protection, and non-repudiation. The attribution of "+" indicates presence and "-" absence of the criteria under discussion, while the number of "+" indicates the degree of presence. Obviously, a higher the number of "+" signs corresponds to a better performance of the model with respect to the specific criteria.

Table 1. Analysis of current practices and PIDESC model

	Digital Hash Only	Digital Hash with Symmetric Encryption	Digital Hash with Asymmetric Encryption	Digital Signature with Smart Card
Upfront Cost	+	+	+++	+++
Operational Cost	+	+	+++	+++
Time	+	+	++	++
Integrity Protection	+	++	+++	++++
Non-Repudiation	-	-	-	++++

One can clearly notice from the evaluation table that the PIDESC model:

1. Provides better integrity protection as compared with digital hashes or digital signatures (where digital certificates are in the provenance of software based techniques). This is because of the fact that smart cards utilize all across the board secure environment for digital credentials. Hence it is rather difficult for an adversary to manipulate with the integrity of digital evidence.
2. Renowned tools in the industry such as FTK and EnCase use digital hashes alone or encrypted with a secret key to protect integrity of extracted digital evidence. Time required to generate[1] SHA1 Digital Hash on 8 GB USB drive was $1.21 * 10^5$ milliseconds. As depicted in Figure 3, time required to generate[2] a digital signature on SHA1 output is only 0.5 milliseconds which is negligible when compared with the time required to generate a hash. Simply, there is almost no increase in time complexity of the computational requirements compared to current practices.

   Figure 3 represents time in milliseconds required to generate digital signature on 128 bits of SHA1 output, compared with the time required to generate digital hash for 8 and 2 GB USB drives.
3. The model requires PKI. Establishing and operating a PKI is financially demanding. So one could think that PIDESC will require higher upfront costs. But, FTK Imager 2.9 can optionally use digital certificate to provide confidentiality services which mean the prevailing solutions are already moving towards asymmetric cryptography (AC). AC requires PKI at its back end. So, at the present there are situations (and a lot more expected) where people are making serious financial commitments to establish and operate PKI.

[1] Using FSUM 2.52, `http://www.slavasoft.com/fsum`

[2] Using FIPS 201 Standard, Precise Biometric Card Reader with its APIs and Gemalto Smart Card.

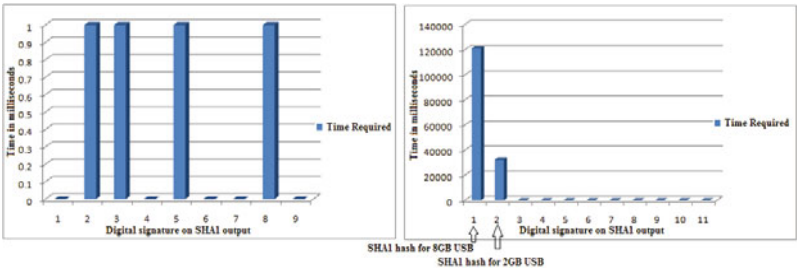

Fig. 3. Time in Milliseconds Required to Generate Signature for 128 bits of SHA1 Output and Time Required to Generate Digital Hash for 8GB and 2 GB USB Drive

4. All the operations such as extraction of digital evidence, generation of digital signature, appending it to the digital evidence, adding it to the chain of custody and communicating it with the backend authentication server, are transparent to the forensic examiner so there is minimal human intervention during most of the phases when the model is running. This indicates that it is:
   (a) Easy for an examiner to operate the tool because of automation.
   (b) Less prone to human errors.
   (c) Provides precise results.
   (d) Fairly open to reviews for consistency, precision and accuracy, which will result in trustworthy digital evidences.
5. There are also additional benefits, or some extra information while generating digital signature such as when, where and who interacted with the digital evidence. This makes repudiation harder and attribution easier.

6 Conclusion

Our work and the paper address and investigate current practices employed to ensure integrity of extracted digital evidence. In order to improve on these practices we have explored and outlined the associated vulnerabilities present in them. Several experiments were conducted to exploit these vulnerabilities which showed that an adversary is able to modify the contents of digital evidence without being detected.

Consequently, we proposed a new model for strong integrity protection of digital evidence using smart cards termed as PIDESC. We proceeded with the critical analysis of the new model in terms of improvements achieved and cost incurred. We found that with a very modest additional cost, the PIDESC model can provide better protection to the integrity of digital evidence along with an additional non-repudiation service, and thus better conformity to the RFC 3227 and IOCE's guidelines.

It is to expect that future work will focus upon the format and data structures needed to communicate information to and from the smart card, such as digital hash, where, when and who interacted with the digital evidence. Indeed, proper

and well defined communications and the corresponding environment between the main factors in the secure and with the strong integrity protected digital evidence extraction and collection such as the forensic tool, authentication server, the legal and other bodies that require this evidence is another direction for our research.

References

1. Brezinski, D., Killalea, T.: RFC3227: Guidelines for Evidence Collection and Archiving. RFC Editor United States (2002)
2. International Organization on Computer Evidence (IOCE), Guidelines for best practice in the forensic examination of digital technology, Orlando (2002)
3. Aoki, K., Guo, J., Matusiewicz, K., Sasaki, Y., Wang, L.: Preimages for Step-Reduced SHA-2. In: Matsui, M. (ed.) ASIACRYPT 2009. LNCS, vol. 5912, pp. 578–597. Springer, Heidelberg (2009)
4. Robshaw, M.: On recent results for MD2, MD4 and MD5. RSA Laboratories Bulletin 4 (1996)
5. Stevens, M.: Fast collision attack on MD5. IACR ePrint archive Report 104, 17 (2006)
6. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full SHA-1. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 17–36. Springer, Heidelberg (2005)
7. Wang, X., Yu, H.: How to break MD5 and other hash functions. In: Cramer, R. (ed.) EUROCRYPT 2005. LNCS, vol. 3494, pp. 19–35. Springer, Heidelberg (2005)
8. Lee, S., Kim, H., Lee, S., Lim, J.: Digital evidence collection process in integrity and memory information gathering. In: First International Workshop on Systematic Approaches to Digital Forensic Engineering, Systematic Approaches to Digital Forensic Engineering, Taipei, Taiwan, pp. 236–247. IEEE, Los Alamitos (2005)
9. Smart card: Introduction: Primer (March 2010), `http://www.smartcardalliance.org/pages/smart-cards-intro-primer`
10. Product downloads (April 2010), `http://www.accessdata.com/downloads.html`
11. Encase forensic (March 2010), `http://www.guidancesoftware.com/default.aspx`
12. Nexus personal security client (April 2010), `http://www.nexussafe.com/en/Products/Nexus-Personal/`
13. Handelsbanken (April 2010), `http://www.handelsbanken.se`