

---

# Lazarus: Data Leakage with PGP and Resurrection of the Revoked User

---

Rodrigo Ruiz<sup>1</sup> and Rogério Winter<sup>2</sup>

<sup>1</sup>*CTI Renato Archer, Campinas, Brazil*

<sup>2</sup>*Brazilian Army, Campinas, Brazil*

*E-mail: rodrigoruiz@outlook.com; rogwinter@gmail.com*

Received 8 September 2016; Accepted 10 November 2016;  
Publication 19 November 2016

## Abstract

The cybersecurity is the issue on the international agenda. The abuse of communication and faulty software is a common practice that brings the decade of 70. Invariably technology is the great protagonist of data leakage and loss of privacy. However, issues related to cybersecurity are founded on sociotechnical approach: technology, people, processes and environment, which interact indistinctly in a sensitive relationship. In this intricate sociotechnical environment of cybersecurity, this paper discloses a flaw in Symantec Encryption Desktop (SED), which can allow the leakage of sensitive information from governments, military and research centers around the world. In this context, as an example, the National Aeronautics and Space Administration (NASA) uses the Symantec Pretty Good Privacy (PGP) Encryption Desktop (SED). The Technology is not the main culprit for data leakage. Sometimes, the users are influenced by sophisticated marketing campaigns, which reaffirms the quality of products and services. In practice, this work is focused in the design errors and past vulnerabilities which are still present in recent technological solutions and allow data leakage and loss of privacy in a general way.

**Keywords:** Data Leakage, Privacy, Data Loss, Drive Encryption, Encryption, PGP, Symantec, NASA.

*Journal of Cyber Security, Vol. 5.2, 1–14.*

doi: 10.13052/jcsm2245-1439.521

© 2016 River Publishers. All rights reserved.

## **1 Introduction**

First of all, we would like to explain the name of our article “Lazarus: Data Leakage with PGP and Resurrection of the Revoked User”. We used the biblical metaphor Lazarus history, regarding his return from death after a miracle. By the same token, we can resurrect a user revoked by the system administrator – as a miracle. However, user revoking resurrection have not the same consequence joy, as Lazarus resurrection.

Data leakage and Loss of Privacy are often used interchangeably to refer to a type of security breach that traditionally causes great financial losses and moral damages. The privacy issue and data loss in the digital world are sometimes controversial and difficult to solve because the cause is not so easy to detect. The intricate environment of cyber security is contaminated by issues that go beyond technology, gathering a quaternary structure composed by processes, people, environment, and technology. The reliability of a security system is based on temporally human knowledge concepts which are renewed, ratified or rectified day to day. In this paper, we test Symantec Pretty Good Privacy (PGP) Symantec Encryption Desktop (SED) and identified a vulnerability which permit information leakage. In this way, it is possible to show that the SED does not protect as it should, research laboratories, governments, agency, industry, armed forces etc. The cybersecurity is a complex problem and technology is not always accountable. The guiding principles behind information security are summed up in the acronym CIA, standing for Confidentiality, Integrity and Availability. We want our information to be read by only the right people (confidentiality), only be changed by authorised people or processes (integrity) and, be available to read and use whenever we want (availability).

Everybody needs to keep safety secrets, such as account password, state secrets, trade secrets, weapons project, aerospace projects, and new technologies. As a solution aiming keeping secrets – protection against cybercriminals, the user acquires cybersecurity solutions software & hardware, since any loss or leakage of information may cause serious damages such as reputation, financial losses etc.

Cybercriminals have stolen passwords from internet users... A survey conducted by InsightExpress and Cisco (CISCO, 2008), pointed out what IT professionals perceive about companies’ data loss incidents and answer why we need to protect our secrets:

70% of IT professionals believe the use of unauthorized programs resulted in as many as half of their companies’ data loss incidents.

44% of employees share work devices with others without supervision.

39% of IT professionals said they have dealt with an employee accessing unauthorized parts of a company's network or facility.

46% of employees admitted to transferring files between work and personal computers when working from home.

18% of employees share passwords with co-workers. That rate jumps to 25% in China, India, and Italy.

Surveys such as conducted by the DSS Company (Filatovs, 2014) are very common and normally highlight special product features. A Symantec report presents that 10% of employees lost company devices such as computers and flash drives, however, 32% did not report these losses.

The above researches show the existence of an environment which is dark and uncertain. Moreover, manufacturers often exaggerate with promises ensuring highly efficient protection, perhaps beyond real security. Under certain circumstances, this assurance can hide threats. Some faults are difficult to detect, such as enabling revoked users in cryptosystems. In this case, attackers can enable revoked users allowing them to have access to cryptosystem again. Research Institute are attacked by hackers due to the nature of his activity.

“Investigators in the United States and Europe say they have spent almost a year pursuing the case involving attacks on computer systems serving the American military, NASA and research laboratories.” (The New York Times, 2005).

Recent publications on failures in many cryptographic applications systems allow access to private data. According to Security Issue on Cloned TrueCrypt Containers and Backup Headers (Ruiz, Amatte, & Park, 2014) and (Winter & Ruiz, Corrosive Secrecy and Confidence: the Paradox Among Bypassing Cryptographic Software, Loss of Privacy and Information Security, 2016) it is noteworthy how failures can compromise information security and privacy of people.

This paper is organized into the following sections: Introduction, Method, Attack Scenario, Results, and Discussion. In the introduction we contextualize the subject within the cybersecurity. In the Method section is shown in a didactic way the techniques used to explore the SED failure. In the Attack Scenario, we propose a plausible attack scenario due to the form of use indicated by Symantec. In the Results section, we present the results of operations of the SED and in the Discussion section we address some possibilities to fix the problem.

## 2 Method

Basically, we need three things to guarantee a privacy and protect the secrets from people or organizations: cryptography algorithms, application software, and people attitude.

- a. Cryptographic algorithms – This is the strongest resource. The algorithms are based on mathematical proofs which guarantee the maturity and system consistency. We may consider an attacker aiming to break an algorithm, he must expend much effort. The PGP and the Advanced Encryption Standard (AES) are good examples of cryptographic algorithms.
- b. Application Software – Cryptographic algorithms are used in conjunction with software application. Software application facilitates the usability, and allows deploy various algorithms. Examples of software application: Symantec Encryption Desktop (SED), Truecrypt, Veracrypt, Cipher-shed, Microsoft Bitlocker, and Bitdefender Total Security 2015 File Encryption.
- c. People attitude – People need to guarantee principles behind information security, such as: confidentiality, integrity and availability. On the other hand, they must use secure methods to store the information and to reduce the number of people that know a particular information. Moreover, a security policy will determine the rules for people and which features allowed.

An analysis of the items above – a, b, c – we consider that the major weaknesses may be found in application software and people attitude. A sociotechnical approach to cybersecurity seems more appropriate. Thus, the SED (Symantec Corporation, 2015) was chosen in this research the following reasons:

- The SED is based on PGP which is well-known algorithm and it has a high reliability and security.
- The Symantec developed SED as a user-friendly interface to a collaborative multi-user work. According to (CISCO, 2008), the humans are also responsible by exploration of software vulnerabilities. The SED facilitates collaborative work with security, but users need to follow a few security rules;
- The SED creates a protected virtual encrypted drive as a simple logical drive f:\. However, the access control of this PGP drive is assured by means of the management of cryptographic keys.

We highlight in this paper some software application and it is possible to note that all software share the same characteristic as SED. All tested application software use the same principle that is, the header section where it is stored user information and cryptographic keys. In this case, the software application allows the header to be manipulated to insert and revoke users. However, the vulnerability discovered on SED multi-user (Figure 1) permits full access in files even after PGP key was revoked by administrator user.

The method used in this article was the manipulation of the virtual encrypted drive header. The same method was applied to the software applications, such as: TrueCrypt (Ruiz, Amatte, & Park, 2014) and Bitdefender Total

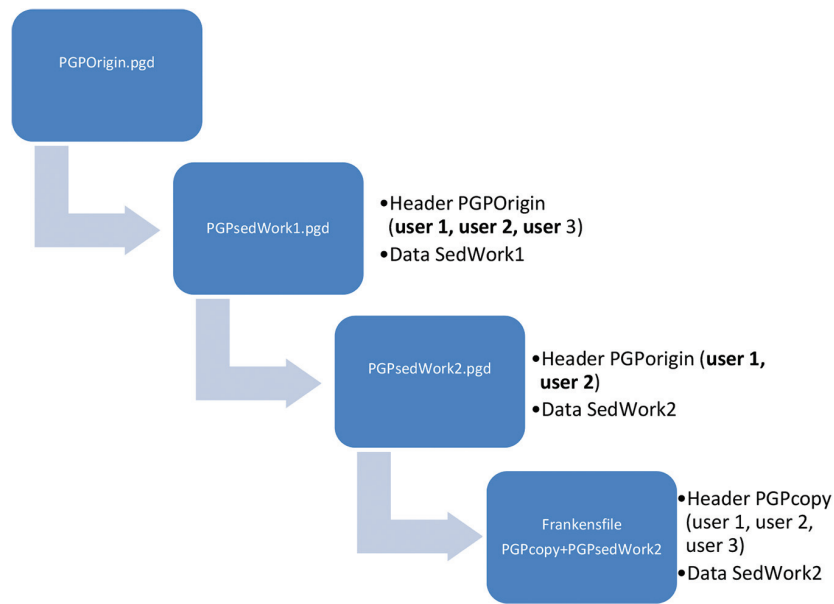
0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
50	47	50	64	55	53	45	52	74	01	00	00	6B	45	C9	2C	PGPdUSERt kEÉ,
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	3C	00	00	00	38	01	00	00	00	00	00	00	< 8
00	00	00	00	00	00	00	00	00	00	00	00	55	53	45	52	USER
53	59	4D	4D	38	01	00	00	00	00	00	00	00	00	00	00	SYMM8
00	00	00	00	00	00	00	00	00	00	00	00	75	73	65	72	user
32	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	90	A9	DD	E3	@ÿä
70	B2	71	4A	B5	D7	45	EB	5F	92	05	54	D9	54	CD	2B	p²qJµ×Eë_` TÚTí+
D5	CF	31	76	37	8C	9B	C7	3B	EF	EC	68	00	00	00	00	Öİlv7  Ç:iih
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	EA	F7	E6	70	ê+øp
21	91	DE	7B	CB	FD	13	44	C9	CÀ	5E	AA	80	3E	00	00	!`b{Ëÿ DÉÉ^â >
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

**Figure 1** SED file with user segment permit the replacement. It is possible to make the revoked user returns.

Encryption 2015 (Winter & Ruiz, Luke 8:17 – Errors that Compromise the Privacy and Information Security, 2015).

In the mentioned article, all cryptographic system use a header to open the encrypted data. Basically, the SED file has two sections: header section and a data section. The header section has serious problems because this enables mixing of different file versions and permit to gain access to new file version. As SED is a multi-user system it needs to save in the same file all users' keys and encrypted data.

In this point, we show how to replace of headers of different versions of SED file. The method used to exploit the vulnerability exists in SED follows operation sequence below. Schematically the method follows as Figure 2 and Table 1:

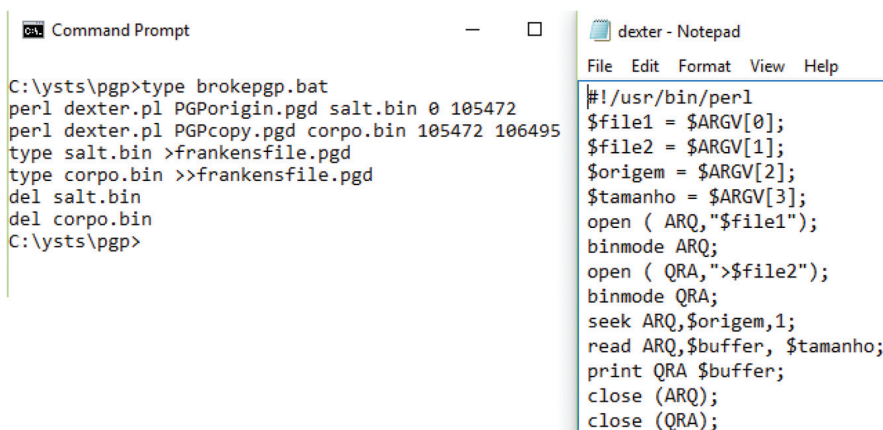


**Figure 2** Process of file handling to create Frankensfile.pgd and information disclosure.

**Table 1** Files, users and data type

File	Users	Data
PGPOrigin.pgd	user1, user2, user3	none
PGPcopy.pgd	user1, user2, user3	none
PGPsedWork1.pgd	user1, user2, user3	Secret text
PGPsedWork2.pgd	user1, user2	Secret text
Frankensfile.pgd	user1, user2, user3	Secret text

- (a) Generate **PGPOrigin.pgd** file and create users (user1, user2 and user3);
- (b) Make a copy of **PGPOrigin.pgd** into **PGPcopy.pgd**.
- (c) Save the information inside the **PGPsedWork1.pgd** file. User1, user2 and user3 have access;
- (d) Delete the user3 according SED user manual (Symantec, s.d.) from **PGPsedWork1.pgd** file. In theory, only user1 and user2 will have access to encrypted data.
- (e) Make the **Frankensfile.pgd** file, which has the header section of **PGPcopy.pgd** and data section from **PGPOrigin.pgd** (Figure 2). Based on Figure 3, it is possible to reproduce the experiment using following file: Perl script dexter.pl and bat script brokepgp.bat.



```
Command Prompt
C:\ysts\pgp>type brokepgp.bat
perl dexter.pl PGPorigin.pgd salt.bin 0 105472
perl dexter.pl PGPcopy.pgd corpo.bin 105472 106495
type salt.bin >frankensfile.pgd
type corpo.bin >>frankensfile.pgd
del salt.bin
del corpo.bin
C:\ysts\pgp>

dexter - Notepad
File Edit Format View Help
#!/usr/bin/perl
$file1 = $ARGV[0];
$file2 = $ARGV[1];
$origem = $ARGV[2];
$tamanho = $ARGV[3];
open ( ARQ, "$file1");
binmode ARQ;
open ( QRA, ">$file2");
binmode QRA;
seek ARQ, $origem, 1;
read ARQ, $buffer, $tamanho;
print QRA $buffer;
close (ARQ);
close (QRA);
```

Figure 3 Perl script dexter.pl and bat script brokepgp.bat description.



```
C:\ysts\pgp>md5sums *.pgd

MD5sums 1.2 freeware for Win9x/ME/NT/2000/XP+
Copyright (C) 2001-2005 Jem Berkes - http://www.pc-tools.net/
Type md5sums -h for help

[Path] / filename                               MD5 sum
-----
[C:\ysts\pgp\]
frankensfile.pgd                                1327c98bb22cb38a8ad097dd3d54a7bf
PGPcopy.pgd                                     9531060b86ef7a925726bca4ac4954a9
PGPorigin.pgd                                  735806aa9de281d48746bd01ed4227b4

C:\ysts\pgp>
```

Figure 4 MD5 hash PGPOrigin.pgd, PGPcopy.pgd and Frankensfile.pgd.

- (f) The script Perl `dexter.pl` is responsible for divide files in two equal parts: header and data. On the other hand, the bat script **`brokepgp.bat`** is responsible for making the junction of header **`PGPcopy.pgd`** with data **`PGPOrigin.pgd`** file. This scripts works in specific SED file conditions of size, file system and Encryption algorithm, but the principle is the same for all file configuration.

### 3 Attack Scenario

When starting an important project security administrators of the fictitious ACME Company configured a SED (**`PGPorigin.pgd`**) for the following users involved with the project: Peter, Tom and Sarah. From then on, they can save on the security of important project information within the SED file.

On the first day of the project, Sarah back up the SED file (`PGPcopy.pgd`) in a flash memory.

The three users (Peter, Tom and Sarah) working for months on the important ACME project saving the files within the SED (**`PGPsedWork1.pgd`**).

After six months, the user Sarah is fired from ACME Company and your login is deleted from the SED file (`PGPsedWork2`). However, it should be emphasized that Sarah still has the SED file (**`PGPcopy.pgd`**) which it was back up on the first day of the project and she can access the information. The logins of other users (Tom and Peter) are changed. In this case, the security issues are in compliance with the guidelines of the manufacturer, because the Saha user credentials do not allow access to the SED file (**`PGPsedWork2`**).

After his resignation, Sara is hired by a competing company ACME which it has interests in the same area of ACME project. As mentioned above, the cybersecurity has an engagement areas that extend beyond technological issues of software solution. In the Cisco Report (CISCO, 2008), 39% of companies surveyed had problems with employees who had access to unauthorized parties network or other service company. In addition, the same survey showed that 44% of employees share work devices with others without supervision.

In this way, it is reasonable to imagine that the file from ACME Company can be obtained by an unauthorized person. In this case, the SED file (**`PGPsedWork2`**), in which Sarah user does not have access credentials, but based on the information in the section Method, Sarah again get access to SED file.



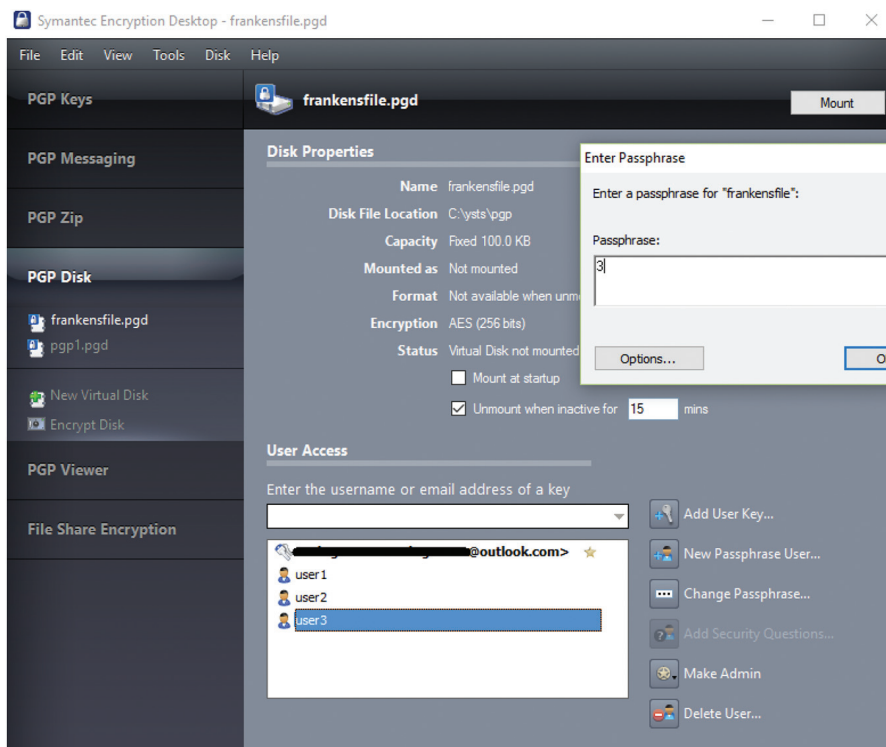


Figure 5 Frankensfile can open PGP1 file secrets with user3 revoked in pgp1.pgd.

## 4 Results

After of the steps method (Figure 2), user3 gained to the encrypted file **Frankensfile.pgd** Remembering that the user3 had their rights revoked earlier. The delete operation represented the resignation or termination of an employee from a project. In this case, a former employee (user3) who not had access to **PGPsedWork2.pgd** file now can read the encrypted information (**Frankenstyle.pgd**) with a simple file operation mixing.

## 5 Discussion

The cybersecurity is often weakened by beliefs, marketing advertisements or human behavior.

According to the article published in the CIO Magazine (Corbin, 2016), mentions that compliance is not the only way to ensure the security of

systems. Today's attacks are extremely sophisticated and exploit the weak protection systems, which was designed for more than a decade. The goal of software testing is highlighted defects if they exist. However, the results can be subject to modification, which depends on the method and the way that tests are performed. According to Forbes (Greenberg, 2010), Symantec paid \$300Million for PGP technology. Since then, Symantec has been using the algorithm in their security products. The fame of PGP has been used to give a reliability of cryptographic systems. However, as described above it is possible to access the contents of the files encrypted with PGP, regardless of the date of creation. We discovered the flaw in the SED, it is a flaw in the application software that uses PGP to encrypt the files. Probably the failure reported in this article is related a bug SED project, in the same way as in other systems mentioned above.

As a proposal to resolve this failure would be an encryption operation of the SED data file, when the user is deleted. In this way, it is possible to prevent the Header manipulation, as shown in the section Method.

The cybersecurity is based on people, technology, process and environment and the SED is basically a system that is subject to interference from 4 dimensions. Denning (E. Denning, 1987) observes that the major part of existing systems have vulnerabilities which make them susceptible to attacks, invasions and other kinds of abuse; moreover, the maintenance to avoid all such deficiencies is not viable technically nor economically.

After we discover this vulnerability, the Symantec Company was notified by protocol SSG15-044. In addition, we have identified that the National Aeronautics and Space Administration (NASA, 2012) uses the encryption system of Symantec PGP (Figure 6). Immediately, the NASA was informed by email about this vulnerability.

## **6 Conclusion**

In this article our main goal is to alert scientists, governments and businesses around the world, just as we have done for Symantec and NASA on the risks of this type of security breach. According to TechNavio (Ellacott, 2014), the Symantec Company appears as a world leader in cybersecurity market and certainly the systems are used in thousands of government agencies, businesses and military.

Although Symantec video (Symantec Corporation, 2014) share the SED security premises, unfortunately we need to review the practice of information security. People, Companies and Research Labs around the world are feeling

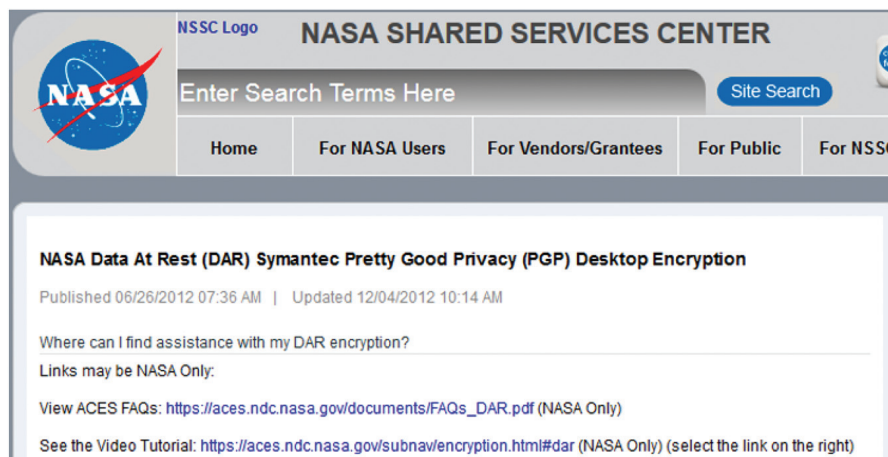


Figure 6 NASA screenshot with instructions about use PGP file encryption.

more secure when deploy cryptographic software to protect their information. The cybersecurity is more complex than the simple use of a cryptographic software. Scientists, governments and public institutions are living with a false sense of security using a vulnerable systems.

It is recommended that vendor require the SED to redo encryption whenever a user is deleted. This simple measure would prevent parts of an old file was used as a key to opening new files.

## References

- [1] CISCO. (2008). *Data Leakage Worldwide: Common Risks and Mistakes Employees Make*. Available at: Data Loss Prevention: [http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white\\_paper\\_c11-499060.html](http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html) (Retrieved: February 24, 2014).
- [2] Corbin, K. (2016). *Cybersecurity much more than a compliance exercise*. Available at CIO: <http://www.cio.com/article/3025452/cyber-attacks-espionage/cybersecurity-much-more-than-a-compliance-exercise.html> (Retrieved February 24).
- [3] Denning, D. E. (1987). "An Intrusion-Detection Model," in IEEE (Ed.) *IEEE Transactions on Software Engineering – Special Issue on Computer*, Vol. 13, (Piscataway, NJ, USA: IEEE Press), 222–232. doi:10.1109/TSE.1987.232894

- [4] Ellacott, J. (2014). *Leading Email Encryption Vendors Respond to Heartbleed Bug Threat*. (Infiniti Research Limited). Available at: TechNavio: <http://www.technavio.com/report/global-email-encryption-market-2014-2018> (Retrieved February 22, 2015).
- [5] Filatovs, A. (2014). *Data Security Solutions*. Available at: Slide Share: <http://pt.slideshare.net/AndSor/dss-symantec-pgp-encryption-fortress-2014-arrowecs-roadshow-baltics> (Retrieved February 25, 2015).
- [6] Greenberg, A. (2010). *Symantec Acquires Encryption Provider PGP For \$300 Million*. (Forbes) Retrieved February 24, 2015, from Forbes Magazine: <http://www.forbes.com/sites/firewall/2010/04/29/symantec-acquires-encryption-provider-pgp-for-300-million/>
- [7] NASA. (2012). *NASA Data At Rest (DAR) Symantec Pretty Good Privacy (PGP) Desktop Encryption*. (NASA). Available at: NASA SHARED SERVICES CENTER: [https://answers.nssc.nasa.gov/app/answers/detail/a\\_id/6235/~nasa-data-at-rest-%28dar%29-symantec-pretty-good-privacy-%28pgp%29-desktop-encryption](https://answers.nssc.nasa.gov/app/answers/detail/a_id/6235/~nasa-data-at-rest-%28dar%29-symantec-pretty-good-privacy-%28pgp%29-desktop-encryption) (Retrieved April 24, 2015).
- [8] Ruiz, R., Amatte, F. P., and Park, K. J. (2014). *Security Issue on Cloned TrueCrypt Containers and Backup Headers*. Kuala Lumpur, Malaysia: SDIWC. Available at: <https://www.researchgate.net/publication/271498536>
- [9] Symantec Corporation. (2014). *Symantec Endpoint Encryption – Protect Your Data*. (Google Inc.) Available at: You Tube: <https://www.youtube.com/watch?v=NtGSX3pYkLQ> (Retrieved February 24, 2015).
- [10] Symantec Corporation. (2015). *How Endpoint Encryption Works*. Available at: from Symantec Enterprise: [http://www.symantec.com/content/en/us/enterprise/white\\_papers/how-endpoint-encryption-works\\_WP\\_21275920.pdf](http://www.symantec.com/content/en/us/enterprise/white_papers/how-endpoint-encryption-works_WP_21275920.pdf) (Retrieved February 24, 2015).
- [11] The New York Times. (2005). *Nytimes*. Available at: [http://www.nytimes.com/2005/05/10/technology/internet-attack-called-broad-and-long-lasting-by-investigators.html?\\_r=0](http://www.nytimes.com/2005/05/10/technology/internet-attack-called-broad-and-long-lasting-by-investigators.html?_r=0) (Retrieved 01 05, 2016).
- [12] Winter, R., and Ruiz, R. (2015). Luke 8:17 – Errors that Compromise the Privacy and Information Security. *Def.camp*. Bucharest.
- [13] Winter, R., and Ruiz, R. (2016). Corrosive secrecy and confidence: the paradox among bypassing cryptographic software, loss of privacy and information security. *Cyber Secur. Rev.* 66–74.

## Biographies



**R. Ruiz** is researcher of CTI – Information Technology Center – Renato Archer, Campinas, Brazil, also he is a member of the SDIWC (The Society of Digital Information and Wireless Communications) have some papers about privacy and he is co-author of *Apoc@lypse: The End of Antivirus* and he is author of papers about privacy and security.

[https://www.researchgate.net/profile/Rodrigo\\_Ruiz3](https://www.researchgate.net/profile/Rodrigo_Ruiz3)



**R. Winter** is colonel at the Brazilian Army with more than 25 years of experience in military operations and cybersecurity. He is master degree in Electronic Engineering and Computation by Aeronautics Technological Institute-ITA, also he is a member of the SDIWC (The Society of Digital Information and Wireless Communications) and at present, one dedicates to the warfare issues, cybernetics, command and control, and decision-making process and he is co-author of *Apoc@lypse: The End of Antivirus*.

