IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-7, July 2018 E-ISSN: 2347-2693

Novel Insights Into Cryptovirology : A Comprehensive Study

Manas Kumar Yogi[1] , S. Lakshmi Aparna[2]

[1]Department Of CSE,Pragati Engineering College(A)
[2]Department Of CSE,Pragati Engineering College(A) Surampalem, East Godavari, A.P., India

*Corresponding Author: manas.yogi@gmail.com, Tel.: +91 9966979279

Available online at: www.ijcseonline.org

Accepted: 19/Jul/2018, Published: 31/Jul/2018

Abstract—Cryptography is presently used for defensive purposes. Ciphers are used against passive attackers. Public key algorithms are used against an active attacker in man-in-the-middle attack. Digital signature is used for defending against a forger. E-cash systems are used against a counterfeiter and a double-spender. Pseudorandom bit generators are used against a next-bit predictor. Crypto virology is used for locating failures of protocols and vulnerabilities in design. For defending purpose Forward engineering is used.

Keywords— Cryptography, Cryptovirology, Public Key, Security, Cryptovirus, FIPS, PKCS

I. INTRODUCTION

Cryptovirology is the study of the applications of cryptography to malicious software. It is an inspection on working of modern cryptographic structures that can be used to strengthen, improve, and develop new dangerous malware attacks. The attack of Crypto virology are used for assurance of advancement in privacy and more strong against reverse-engineering, gives the attacker an enhanced anonymity when Communicating with located malware (e.g., over public bulletin boards and Usenet Newsgroups), improve the ability to steal data, improve the ability to carry out extortion, Enable new types of denial-of-service; enable fault-tolerance in distributed crypto viral attacks, and so on. Also, recent work shows how a worm can install a back door on each infected system that opens only when the worm is presented with a system-specific ticket that is generated by the worm's author. This is called an access-for-sale worm [1].

1.1 Cryptovirus

In security of a computer, a virus is defined as a computer virus that contains and uses a public key. Usually the public key belongs to the author of the virus, though there are other possibilities as well. For instance, a virus or worm may generate and use its own Key pair at run-time. Crypto viruses use secret sharing to hide information and communicate by reading posts from public bulletin boards. Cryptotrojans and crypto worms are the same as crypto viruses, but they are Trojan horses and worms. A virus that uses a symmetric key and not a public key is not a Crypto virus (this is particularly relevant in the case of polymorphic viruses).

There are several rules that all viruses seem to obey.

- By virtue of being programs they all consume CPU time and occupy space.
- Since viruses need to gain control of the program counter in order to execute, they must (directly or indirectly) modify code in the host system in order to do so.
- Their inherent vulnerability to user scrutiny is the last and perhaps most interesting rule of viruses

Viruses can always be frozen and analyzed by the user. They can be backed up (or a backed up copy can be found) and later scrutinized in detail using a low level debugger. In what follows we show that this vulnerability can be effectively bypassed if strong cryptographic techniques are employed and if the virus acts fast enough, i.e. before detection. We also suggest countermeasures and mechanisms to cope with and prevent such attacks[2]. These attacks have implications on how the use of cryptographic tools should be managed and audited in general purpose computing environments, and imply that access to cryptographic tools should be well controlled. The experimental virus demonstrates how cryptographic packages can be condensed into a small space, which may have independent applications (e.g., cryptographic module design in small mobile devices). Hackers have uncovered the dark side of cryptography—that device developed to defeat Trojan horses, viruses, password theft, and other cyber-crime. It's called crypto virology, the art of turning the very methods designed to protect your data into a means of subverting it. In this fascinating,

disturbing volume, the experts who first identified crypto virology show you exactly what you're up against and how to fight back

II. RELATED WORK

Ted Bridis, wrote an Associated Press article entitled Hackers Holding Computer Files 'Hostage' dated Tuesday. May 24, 2005[5]. This article describes that researchers at Websense Inc. identified the malware infection in which peoples' files are encrypted and held for ransom by the virus author. Symantec has named that malware as Trojan.Pgpcoder. F-Secure analyzed an Trojan (F-Secure Corporation, Technical Details: Alexey Podrezov, May 27-28, 2005) and they referred it as Gpcode. The analysis by F-Secure indicates that this Trojan uses a breakable encryption method. They state that F-Secure Anti-Virus detects that Trojan and repairs the files that it encodes. This is in line with the article, that states that the victim's files were repaired without paying any ransom. Ted Bridis referred this as the "latest threat to computer users" and that it was "unusual extortion plot," overlooking the previous malware that attempted this and the discovered that asymmetric cryptography is needed for carrying the attack correctly.

An article also reported that a malware extortion attack has occurred in Europe. The description of that attack is vague. It was not mentioned of public keys, nor asymmetric encryption, nor hybrid encryption. Prior to Trojan. Pgpcoder there were small number of malware attacks that encrypt the host data that were reported by researchers. They all based on symmetric cryptography and hence they were not cryptoviruses/cryptotrojans. Their encryption techniques were therefore reversible and antivirus fixes the problem and decrypted the data they encrypted.Many reports and on-line discussions confuse secure cryptoviral extortion that utilizes asymmetric cryptography with attacks that depend on symmetric encryption alone.

III. METHODOLOGY

Attacking Methodology of A Cryptovirological Attack

I. Cryptoviral Extortion : Cryptoviral extortion is mechanism for the encrypted viruses which uses public key cryptography, in a denial of resources(DoR) attack which can be introduced by the cryptovirus. It is a three-round protocol which is carried out by an attacker against the victim. The attack is generally carried out via a cryptovirus that uses a hybrid cryptosystem to encrypt data while deleting or overwriting the original data in the infecting process. The protocol is as : An asymmetric key pair is generated by the virus designer on a smartcard and the public key is placed in the virus. The private key is especially designated as "non-exportable" so that even the virus author cannot obtain it's bit representation and the private key is generated, stored, and used on the smartcard. Ideally, the smartcard implements two-factor security. Also, the card will ideally be immune against differential power analysis, timing attacks, etc. to prevent the virus author from ever learning those bits of the private key. The virus author then deploys the cryptovirus. After that the virus activates tens or even hundreds of thousands of computer systems. The remainder of this description will cover the protocol for just single such machine.

When the virus get activated, it uses a true random bit generator (TRBG) to generate a symmetric key and initialization vector uniformly at random way. It is essential that the TRBG should produce truly random bits to prevent the symmetric key and the initialization vector from being guessed by the analyst or otherwise will get determined by the victim at a later date. The virus then encrypts host system data with this random symmetric key and the initialization vector. The virus then concatenates the initialization vector with the symmetric key and later encrypts the International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.4, July 2011 37 resulting string by using the public key of the virus author. The encrypted plaintext is then held for ransom. The virus notifies its victim that the attack has occurred and states that the asymmetric cipher-text will be needed to restore the original data. If the victim ready to pay the ransom and transmitting the asymmetric cipher-text to the virus author then the virus author decrypts the cipher-text using the private key that only the virus author has. The virus author sends that symmetric key and corresponding initialization vector to the victim. These are then used to restore the data that was held ransom.

3.1 . The Secret Sharing Virus

This section shows how to implement a virus that is a very close approximation to the highly servile virus. Whereas in the above attack the virus author managed the keys and owned the private key and the virus itself will manage its private key. Since a virus holding a public key and managing its private key can be get analyzed by antivirus analyst and could lose its power. However, this can be accomplished by changing our notion of a system S to be a network of computers, and to regard the host as being the part of entire network. We utilize the distributed environment to hide the key in that virus copies themselves previously. This can be describe in some detail. It is shown that how Public Key

Table 1: Virus size

The Main Attack routine	432	ANSI
C Global data	560	
TEA encryption routine	88	ASM
Modified GNU MP lib	4372	ANSI
C		
MISC attack code	804	ANSI C
Main virus routine	614	ASM
Entire attack routine	6372	ANSI

Cryptography can be used in a virus to encrypt information in such way that the user cannot retrieve it.
In order to be able to decrypt held data to get original, the private key must be storied somewhere, since otherwise held or encrypted data cannot be decrypted.

3.2 . Deniable Password Snatching

In the DPS attack, the attacker first seeks to install a cryptotrojan into a target computer. Already it seems possible that the attacker is at the high risk of getting caught and most probably if he has installs the cryptotrojan manually. The attack is generally carried out by using a custom cryptovirus designed by the attacker [6]. The attacker(virus author) distributes the virus preferably using the passive virus distribution channel. Once the virus get installed a Trojan horse that it carries with it activated. The purpose of this whole is to allow the attacker to indirectly run code of his own Trojan without being blamed for installing it.

IV. RESULTS AND DISCUSSION

To successfully implement a cryptovirus, a study of the various cryptographic approaches such as random number generators(TRBG), proper recommended cipher text chaining modes such as CRC etc. are necessary. Wrong choices can lead to poor cryptographic attack and increase chances of getting caught. So, use of previously existing cryptographic routines would seems to be ideal such as Microsoft's Cryptographic API (CAPI). It has been shown that using just eight different calls API calls, a crypto virus can satisfy all its encryption requirements.
Performance: The following table is a summary about the performance of the Cryptovirus related to the time in the infection.

Table 2: Running time

System boot(normally)	<	16.7msec
Generation of 384 random bits	=	6.4sec
Infect a system file	=	4sec
RSA Encryption	=	66.7msec
System boot	=	11.92sec
Infect a program	=	1 sec
True Encr Algorithm Rate(1 round)	=	47kbyte/sec
TEA Rate(3 rounds)	=	15.7kbytes/sec

Note that about ten minutes of CPU time was spent on the above pre-computations. The approximate running time are given because they can vary program to program. Factors such as disk response time can make the variations. The critical file and desired files used for this benchmark were each 30 kb approximately in the length. There are no disk writes needed in the system boot phase of the virus, however disk writes are needed in infection operation. And because of that the system boot phase takes significant less time in second case. The random number generation takes up 53.7 percent of the total attack time.
It can be inferred from above table 1 that the attacking routine could be made much small if they were written in machine language. The outcomes of research was that we found that it is possible to write code for RSA, true_rand(), and True Encryption Algorithm, such that code s not exceed 7kb in size. Optimizing the size of code was a challenging since many viruses are considerably small in size. Optimizations allowed to omit exponentiation, multi-precision and a division routines. This optimizations were used in areas like smart card technology.

V. COUNTERMEASURES TO CRYPTO VIRUS

There are several measures that can be taken to significantly reduce the risk of being infected by a crypto virus, and there are also measures that can insure a quick recovery in the event of an attack. Fortunately, many of the attacks described in this paper can be avoided using existing antiviral mechanisms, since crypto viruses propagate in the same way as traditional viruses. The first step in this direction is implementing mechanisms to detect viruses prior to or immediately following system infiltration. One of the pioneering works in the area was "An Intrusion-Detection Model", by Dorothy Denning. The paper entitled "Coping with Computer Viruses and Related Problems" is another good source regarding the virus threat.

a) Access control to cryptographic tools

In particular, we will give idea of auditing access to cryptographic tools - This is perhaps the major issue that needs to be learned. This may support system administrators identify suspicious cryptographic usage.
If complex cryptographic ciphers and random number generators are made available to user processes, then they will also be made available to crypto viruses. Such viruses would be smaller than our crypto virus since they would not contain as much code, and they would also run faster since such tools are usually optimized for speed. Incorporating strong crypto-graphic tools into the operating system services layer may seem like it would increase system security, but in fact, it may significantly lower the security of the system if the system is vulnerable to infection[7]. In

addition with the tools which are readily available, virus writers would not even have to understand cryptography to create crypto viruses. Note that this rule should not apply only to export control (as it is now) but also to protection of an installation by its own administration

b) On-line proactive anti-viral measures Apart from vague advice to perform the backups and patch the systems on the regular basis, there are a few things that we can suggest. Specifically for certificates and e-cash schemes, we can suggest storing them in encrypted form, so that even in case of an infection, the worm would not be able to tell that encrypted data from regular files which present no interest to it[8]. However, that appears to be a non-trivial implementation problem, since the victim needs to somehow obtain these, and the very request for them might lead the worm to the encrypted versions of certificates and ecash. Even though they cannot be stolen in encrypted form, they still can be subverted once the worm finds out about the nature of that One effective tool to combat the cryptovirologic super worm that we envision are automated response-enabled Intrusion Detection Systems (IDS). Although state-of-the-art is not at that point yet, a fruitful direction for research would be trying to develop coordinated response-enabled IDS's that quickly generate signatures of unknown attacks and communicate them to their peers before the worm[9]. Specification-based IDS.s that allow detection of unknown attack and automated response techniques are now being developed.

VI. CONCLUSION AND FUTURE SCOPE

From past incidents we have found continuous disinclination by security firms to narrate the cryptoviral fraud invasion in detail and explain antidotes. We view this as being fundamentally flawed; it is the classic phenomenon of "reactive security" (acting after the attack) as opposed to the preventative "proactive security." We trust ransomware is the tip of the iceberg. Most Cryptovirology attacks are hidden in disposition, granting the rival to securely pilfer data entirely unheeded. These attacks would infiltrate or stall the vast majority of computer incident response teams. It took over 25 years for cryptoviral extortion to gain worldwide recognition, and it appears that the bulk of these other attacks, which are fully described in the scientific lore, are heading in the same direction: fated to be ignored until a large-scale real world attack is publicized. Santayana's adage: "those who cannot remember the past are condemned to repeat it" seems to anoint fairly well to malicious cryptography.

REFERENCES

[1]Barth, B. California ransomware bill supported by Hollywood hospital passes committee. SC Magazine (Apr. 13, 2016).
[2] Christensen, C. The Innovator's Solution: Creating and Sustaining Successful Growth. Harvard Business School Press, 2003.
[3] Eisler, B. Fault Line. Ballantine Books, 2009.
[4] Santayana, G. Reason in Common Sense, (1905), p. 284, volume 1 of The Life of Reason.
[5] Scott, R. Alien. 20 th Century Fox, 1979.
[6] U.S. Dept. of Health and Human Services. FACT SHEET: Ransomware and HIPAA; http://bit.ly/29zm57B
[7] Volz, D. and Auchard, E. More disruptions feared from cyber attack; Microsoft slams government secrecy. Reuters (May 15, 2017).
[8] Young, A. and Yung, M. Cryptovirology: Extortion- based security threats and countermeasures. In Proceedings of the IEEE Symposium on Security and Privacy, (1996), 129–140.
[9] Young, A. and Yung, M. Malicious cryptography— Exposing cryptovirology. Wiley, 2004.

Authors Profile

Mr. Manas Kumar Yogi pursued Bachelor of Technology from VR Siddhartha Engineering College,Vijayawada,A.P. in 2006 and Master of Technology From Malla Reddy College Of Engineering And Technology in year 2012. He is currently working as Assistant Professor in Department of Computer Science Engineering , Pragati Engineering College (Autonomous), Surampalem, East Godavari District, since 2014. He is a member of IEEE & ACM since 2014. He has published more than 60 review,research papers in reputed international journals ,conferences including IETE sponsered conferences. His main research work focuses on Software Engineering, Distributed Computing, Cloud Security and Privacy, Big Data Analytics, , IoT and Computational Intelligence based optimisations. He has 8 years of teaching experience and 2 years of software industry Experience.

Ms.S.Lakshmi Aparna pursued Bachelor of Technology from Kakinada Institute of Engineering and Technology in the stream of CSE at Kakinada in 2013 and Master of Technology from Jawaharlal Nehru Technological University Kakinada in 2015. She is currently working as Assistant Professor in Department of Computer Science Engineering , Pragati Engineering College (Autonomous), Surampalem, East Godavari District.Her main areas of interest includes Network Security, Web Technologies and Hadoop.

