ISSN 2229-5518

A Review Report on Cryptovirology and Cryptography

Shafiqul Abidin, Rajeev Kumar, Varun Tiwari

Abstract— Cryptography has traditionally been used for defensive purposes. Ciphers defend against a passive eavesdropper. Public key infrastructures defend against an active adversary that mounts a man-in-the-middle attack. Digital signature algorithms defend against a forger. E-cash systems defend against a counterfeiter and a double-spender. Pseudorandom bit generators defend against a next-bit predictor, and so on. Crypto virology extends beyond finding protocol failures and design vulnerabilities. It is a forward engineering discipline that can be used for attacking rather than defending.

Index Terms— Cryptography, Cryptovirology, Public Key, Security, Cryptovirus, FIPS, PKCS.

1 INTRODUCTION

Crypto virology is the study of the applications of cryptography to malicious software. It is an investigation into how modern cryptographic paradigms and tools can be used to strengthen, improve, and develop new malicious software (malware) attacks. Crypto virology attacks have been devised to: give malware enhanced privacy and be more Robust against reverse-engineering, give the attacker enhanced anonymity when Communicating with deployed 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 computer security, a crypto 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 may utilize secret sharing to hide information and may communicate by reading posts from public bulletin boards. Cryptotrojans and crypto worms are the same as crypto viruses, except they are Trojan horses and worms, respectively. Note that under this definition, 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.

Fig. 1. Cryptovirus

- *Shafiqul Abidin and Rajeev Kumar are currently associated with GGS I P Universiuty affiliated Institute as HOD (ComputerScience) and Assistant Professor (Computer Science) respectively. E-mail: shafiqulabidin@yahoo.co.in*
- *Varun Tiwari is pursuing his Ph. D. in (Computer Science) from NWMDIU, South Africa.*

2 Comparison of Crypto Virology and Cryptography

Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. Here we present the idea of ``Crypto virology'' which employs a twist on cryptography, showing that it can also be used offensively. By being offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents. In this paper we analyze potential threats and attacks that rogue use of cryptography can cause when combined with rogue software (viruses, Trojan horses), and demonstrate them experimentally by presenting an implementation of a ``crypto virus'' that we have tested (we took careful precautions in the process to insure that the virus remained contained). Public-key cryptography is essential to the attacks that we demonstrate (which we call "cryptovirological attacks"). 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.

2.1 Cryptographic Standards

FIPS: - FIPS stands for "Federal Information Processing Standard." FIPS standards are published in **FIPS PUBS.** These standards and guidelines are issued by NIST for use by the U.S. government. NIST develops FIPS when there are compelling federal government requirements for security and interoperability and there are no acceptable industry standards or solutions to these requirements. Of particular relevance to crypto virology is the FIPS 140- 2 standards entitled, "Security Requirements for Cryptographic Modules" [FIPS140] and its annexes. The annexes employ the FIPS 186-2 standard entitled, "Digital Signature Standard (DSS) These standards are relevant to crypto virology since companies rely heavily on them for information security and privacy.

PKCS: - The Public-Key Cryptography Standards (PKCS) is a set of standards for public-key cryptography, developed by RSA Laboratories in cooperation with an informal consortium, originally including Apple, Microsoft, DEC, Lotus, Sun and MIT. PKCS has been cited by the OIW (OSI Implementers'' Workshop) as a method for implementation of OSI standards.) PKCS includes both algorithm-specific and algorithm-independent implementation standards. Documents detailing the PKCS standards can be obtained at RSA Data Security's FTP server.

3 Advantages of crypto Virology over the cryptography

a. Provides privacy
b. Authentication
c. High security
d. It extends beyond finding protocol failures and design vulnerabilities
e. High speed
f. Requires less human resources

3.1 Disdvantages of Cryptography

Traditional active virus detection, proposed as one countermeasure, would be helpless against such worm, since the updates could be distributed much faster that the system administrators can clean their system. The virus stays afloat by constantly re-infecting the whole Internet using new zero-day vulnerabilities discovered by the worm owner Instances observe schemes of access control to cryptographic tools on the victims' systems and trick them into allowing access to those tools. All attempts to analyze the traffic and track down the worm owner fail, since all traffic is minimized -- most of the times [5].

3.2 Applications of Cryptography

3.2.1 Defensive purposes

Crypto virology extends beyond finding protocol failures and design vulnerabilities. It is a forward-engineering discipline that can be used for *attacking* rather than *defending*.

3.2.2 Security on the internet

Crypto virology attacks have been devised to: give malware enhanced privacy and be more robust against reverse-engineering, give the attacker enhanced anonymity when communicating with deployed malware.

It also used in Development of Security Products and ATM Centre.

4 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 [Den86]. The paper by White, Chess, and Kuo entitled "Coping with Computer Viruses and Related Problems" is another good source regarding the virus threat.

4.1 Access control to cryptographic tools

More specifically, we suggest auditing access to cryptographic tools - This is perhaps the major issue that needs to be learned. This will help system administrators identify suspicious cryptographic usage.

Note that if strong 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 cryptographic 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[10]. Furthermore, with such tools 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.

4.2 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[6]. 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. Specification-based IDS.s that allow detection of unknown attack and automated response techniques are now being developed [8].

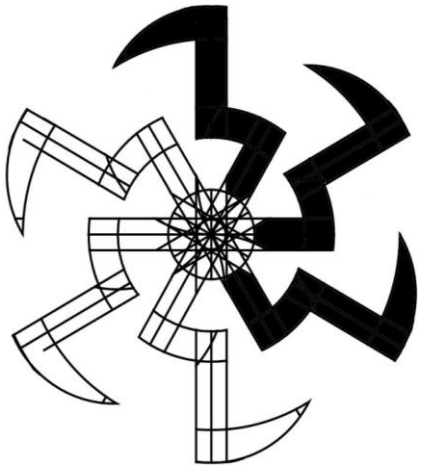

Fig. 2. Skeletal of Crypto Virus

5 Future Scope

Imagining what the nature of future viral attacks might look like is the key to successfully protecting against them. This description discusses how cryptography and key management techniques may definitively checkmate antiviral analysis and mechanisms[9] Traditionally, cryptography and its applications are defensive in nature, and provide privacy, authentication, and security to users. In this paper we present the idea of *Crypto virology* which employs a twist on cryptography, showing that it can also be used offensively. By being offensive we mean that it can be used to mount extortion based attacks that cause loss of access to information, loss of confidentiality, and information leakage, tasks which cryptography typically prevents. In this paper we analyze potential threats and attacks that rogue use of cryptography can cause when combined with rogue software (viruses, Trojan horses), and demonstrate them experimentally by presenting an implementation of a *crypto virus* that we have tested (we took careful precautions in the process to insure that the virus remained contained). Public-key cryptography is essential to the attacks that we demonstrate (which we call "crypto virological attacks"). We also suggest countermeasures and mechanisms to cope with and prevent such attacks. 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).

6 Conclusion

We have shown how Cryptography can be used to implement viruses that are able to mount extortion-based attacks on their hosts. Public-key cryptography is essential in enabling the writer to get an advantage over the victim. We also presented an experimental crypto virus that accomplishes this (it demonstrates cryptographic implementations requiring small

space). A model based on a distributed network was then formulated and an algorithm was provided for how to write a virus that is able to gain discretionary access control over its host. We also suggested a set of measures that can be taken to minimize the possibility of and the risks posed by the crypto virological attacks.

REFERENCES

[1] Adam Young and Moti Yung, Deniable password snatching: On the possibility of Evasive Electronic Espionage, the 1997 IEEE Symposium on Security and Privacy.

[2] Cryptovirology.com FAQ. Available: http://www.cryptovirology.com/

[3] LURHQ Threat Intelligence Group, Cryzip Ransomware Trojan Analysis.Available: http://www.lurhq.com/cryzip.html

[4] Weaver, N., Potential Strategies for High Speed Active Worms: A Worst Case Analysis, http://www.cs.berkeley.edu/~nweaver/worms.pdf, last accessed on December 4, 2002.

[5] Wiley, B., Curious Yellow: The First Coordinated Worm Design,http://blanu.net/curious_yellow.html, last accessed on December 4, 2002

[6] CERT Coordination Center, CERT® Advisory CA-2002-27 Apache/mod_ssl Worm, http://www.cert.org/advisories/CA-2002-27.html, last accessed on December 4, 2002

[7] Slashdot.org, Malicious Distributed Computing,http://slashdot.org/article.pl?sid=02/10/25/1413220&mode=thread&tid=172, last accessed on December 4, 2002

[8] Netcraft, Netcraft Web Server Survey,http://www.netcraft.com/survey, last accessed on December 4, 2002

[9] Dabek F., Brunskill E., Frans Kaashoek M.,et. al. Building Peer-to-Peer Systems with Chord, a Distributed Lookup Service, IEEE Eighth Workshop on Hot Topics in Operating Systems p. 81, Elmau, Germany, May 20 - 22, 2001.