Poster: FLUSH+RELOAD Cache Side-Channel Attack on Mail User Agent

Hodong Kim
Korea University
hdkim@isslab.korea.ac.kr

Hyundo Yoon
Korea University
hdyoon@isslab.korea.ac.kr

Youngjoo Shin
Kwangwoon University
yjshin@kw.ac.kr

Junbeom Hur
Korea University
jbhur@isslab.korea.ac.kr

***Abstract*—Many mail user agent (MUA) programs support email encryption functionality to clients using crypto libraries such as GnuPG. In 2013, Yarom and Falkner demonstrated FLUSH+RELOAD cache side-channel attack is used to extract RSA private key in GnuPG 1.4.13. In this study, we propose a novel attack scenario based on FLUSH+RELOAD attack, and demonstrate that a list of MUA programs are still vulnerable to FLUSH+RELOAD attack, even if the vulnerability is resolved in the latest version of GnuPG in practice. Specifically, we evaluated 37 MUAs, and conducted in-depth analysis of 13 ones among them, which are available in Ubuntu 14.04 and 16.04. According to our experiment, we found that about 77% of the MUAs are vulnerable to the FLUSH+RELOAD attack. Our attack could recover 92% of the bits of RSA private key of a victim when he receives and decrypts email contents using the MUA.**

I. Introduction

Mail user agent (MUA) is one of the most widely used email programs, which supports email encryption functionality to clients using a crypto libraries such as GnuPG [1] for prevention of private information breaches [2]. In a virtualized desktop environment, each user can have individual virtual machine (VM) on a hypervisor, operating on the shared hardware resources. Thus, even if individual users access separated desktop environments supported by their own VM with independent applications, they are inherently executed on the same hardware resources managing each VM for the service. Recently, Yarom et al. proposed FLUSH+RELOAD cache side-channel attack and demonstrated the attack is able to restore RSA private key in GnuPG 1.4.13 by exploiting shared resources in the system, such as the Last Level Cache (LLC, or L3) [3].

In this study, we propose a novel MUA attack scenario exploiting FLUSH+RELOAD attack, and demonstrate that a list of MUA programs are still vulnerable to FLUSH+RELOAD attack even if the vulnerability is resolved in the latest version of GnuPG in practice. Our attack leverages the vulnerability of MUAs that allow installation of the old version of GnuPG library without version check, which is vulnerable to FLUSH+RELOAD attack. Specifically, our attack procedures progress as follows.

Network and Distributed Systems Security (NDSS) Symposium 2019
24-27 February 2019, San Diego, CA, USA
ISBN 1-891562-55-X
https://dx.doi.org/10.14722/ndss.2019.23035
www.ndss-symposium.org

First, an attacker performs a FLUSH+RELOAD attack [3] to the L3 cache, when a victim reads an encrypted e-mail in the MUA by utilizing page sharing feature in VM environment. Then, the attacker is allowed to observe victim's execution of decryption and acquire essential information to guess the private key (that is, RSA exponent in the GnuPG in this attack). Second, the adversary restores a private key based on the observed information in the first step. Finally, the adversary is able to decrypt the victim's encrypted email in MUA with restored private key if it matches with the private key of victim.

We evaluated 37 MUAs, and conducted in-depth analysis of 13 ones among them, which are available in Ubuntu 14.04 and 16.04. According to our experiment, we found that about 77% of the MUAs are vulnerable to the FLUSH+RELOAD attack. Our attack could recover 92% of the bits of RSA private key of a victim when he receives and decrypts email contents using the MUA.

II. Preliminary

RSA implementation. CRT-RSA is a modified form of RSA in private key and decryption function. Instead of d, the system uses $d_p = d\,(mod\,(p-1))$, and $d_q = d\,(mod\,(q-1))$ to make $private\ key = (d_p,\, d_q,\, p,\, q)$.

The Square-and-Multiply Algorithm is used to reduce the number of exponent operations required for decryption in CRT-RSA. Specifically, the algorithm solves exponentiation with Square-reduce-Multiply-reduce (S-R-M-R) operation for positive bit of exponent and Square-reduce (S-r) operation for negative bit from next bit of MSB. For example, for a^{13}, the exponent 13 can be denoted as 1101_2. Then, the operation sequence for the exponent would be {S-r-M-r, S-r, S-r-M-r} instead of hardcore calculation such as multiplying 13 times of a. The sequence of Square-reduce and Square-reduce-Multiply-reduce operations exactly corresponds to the sequence of binary represented exponent.

FLUSH+RELOAD attack. The memory de-duplication allows processors to share a single copy instead of storing multiple copies of the same data. Many current hypervisors support the feature to improve memory utilization, especially in the cross-VM environment. Yarom et al. described how the attacker exploits a pinhole from the feature to make side-channel attack successful, which is called FLUSH+RELOAD [3].

The FLUSH+RELOAD attack begins with loading up data to the memory that the adversary wants to observe. Then he evicts the data from the memory with CLFLUSH instruction,

TABLE I. VULNERABILITY ANALYSIS OF MUAS

	Ubuntu	14.04	Ubuntu	16.04
MUA	**Version**	**GnuPG 1.4.13**	**Version**	**GnuPG 1.4.13**
Alpine	2.10	Allowed	2.20	Allowed
Balsa	-	-	2.5.6	Allowed
Claws Mail	3.9.3	Allowed	3.13.2	Allowed
Cone	0.89	Allowed	1.0	Allowed
Evolution	3.10.4	Allowed	3.18.5.2	Allowed
GNUmail	-	-	1.2.2	Allowed
i.Scribe	-	-	2.2	Allowed
KMail	4.13.3	Allowed	5.1.3	Allowed
Thunderbird	52.9.1	Prevented	60.2.1	Prevented
Seamonkey Mail	-	-	2.49.4	Prevented
Sylpheed	-	-	3.5	Prevented
Trojit	0.7	Allowed	-	-
Zimbra	7.3.1	Allowed	-	-

which is used to empty the memory location where the data is loaded. Then he reloads the same data and measures the elapsed access time. In the moment between flushing and reloading the data, if the victim loads exactly the same data of the attacker's interest (which will be reloaded later), it will cause cache hit in the reload phase by the attacker, which takes shorter execution time compared to cache miss case. By careful observation of the time difference several times, the adversary would be able to figure out what data or function the victim accessed in what order.

III. ATTACKS ON MAIL USER AGENT

The GnuPG 1.4.13 (or previous version) performs Square-and-Multiply algorithm in CRT-RSA decryption. Since the decryption in CRT-RSA involves two exponents, tracing the execution flow of Square-and-Multiply implementation when victim performs a decryption results in restoring two elements d_p and d_q. Yarom et al. describes the details of how to use FLUSH+RELOAD attack to process an execution flow of Square-and-Multiply implementation into a RSA private key on GnuPG 1.4.13 in [3]. We designed our attack based on the technique, then conducted our attack on an Intel Xeon E5 2620 v4 (16 cores), 256GB RAM, QEMU-KVM 1:2.5+dfsg-5ubuntu10.5 hypervisor, and a pair of VMs for each version of Ubuntu OS (14.04 and 16.04).

A. Analyzing MUA

In our experiment, we first evaluated 37 MUAs, and finally installed 13 ones among them on each VM, which are available in Ubuntu 14.04 and 16.04. Then, we tested whether they allow installation of GnuPG 1.4.13, which is vulnerable to FLUSH+RELOAD attack. Table I shows the result. 10 MUAs among them allowed the installation without checking crypto library version, making our attack feasible. However, the other 3 MUAs (Thunderbird, Seamonkey Mail, and Sylpheed) prevented the installation of it since it is not the latest (or secure) version of crypto library.

B. Attacking MUA

Based on the analysis result in Table I, we delivered our attack on vulnerable MUAs. An attacker runs spy process for a FLUSH+RELOAD attack, then sends an encrypted email to a victim. In this moment, adversary's MUA encrypts email contents with public key of the victim. The victim reads the encrypted email, then MUA exploits GnuPG 1.4.13 to decrypt contents. The left side of Fig. 1 shows the attacker's view

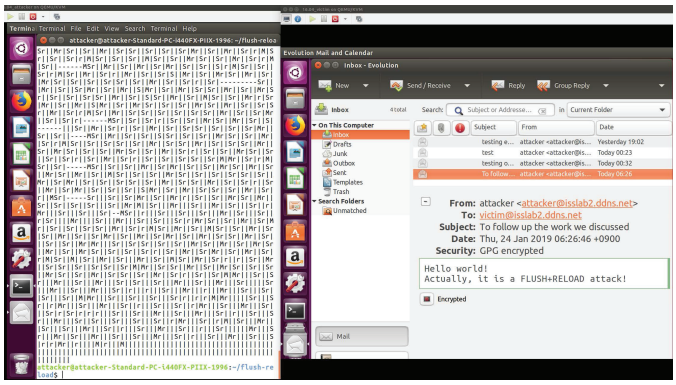

Fig. 1. Attacking Evolution 3.18.5.2 in Ubuntu 16.04

when launching FLUSH+RELOAD attack on Evolution which is one of the vulnerable MUAs we found, and the right side shows the victim's. In the attacker's view, S and M represent Square and Multiply operation, respectively, and r means the reduce operation preparing next input, that is next execution of Square and Multiply operation. The terminal window shows the attacker obtained an execution flow of Square-and-Multiply operations during the victim's decryption. After converting the obtained sequence of operations into bit representation by using a converter we implemented, the adversary could restore 92% of the victim's RSA secret key in this attack.

IV. CONCLUSION AND DISCUSSION

In this study, we proposed a novel MUA attack scenario based on FLUSH+RELOAD attack, and demonstrated that a list of practical MUAs are still vulnerable to the attack. In our attack, we could exploit the extinct vulnerability of old crypto library because of implementation flaws in MUA applications, that is lack of simple version control of library on which they rely. Besides MUAs we investigated, any other applications can be exposed to the same threat if there are similar implementation flaws. As we demonstrated in this study, disallowing any vulnerable crypto library would be the first line of defense to protect users' private information.

ACKNOWLEDGMENT

This work was supported by the research fund of Signal Intelligence Research Center supervised by the Defense Acquisition Program Administration and Agency for Defense Development of Korea.

REFERENCES

[1] D. Poddebniak, C. Dresen, J. Müller, F. Ising, S. Schinzel, S. Friedberger, J. Somorovsky, and J. Schwenk, "Efail: breaking s/mime and openpgp email encryption using exfiltration channels," in *USENIX Security Symposium*, 2018, pp. 549–566.

[2] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov, O. Comanescu, V. Eranti, A. Moscicki *et al.*, "Data breaches, phishing, or malware?: Understanding the risks of stolen credentials," in *ACM SIGSAC Conference on Computer and Communications Security*, 2017, pp. 1421–1434.

[3] Y. Yarom and K. Falkner, "Flush+ reload: A high resolution, low noise, l3 cache side-channel attack." in *USENIX Security Symposium*, vol. 1, 2014, pp. 22–25.

NDSS Symposium 2019

FLUSH+RELOAD Cache Side-Channel Attack on Mail User Agent

Hodong Kim
Dept. of Computer Science and Engineering
Korea University, South Korea
hdkim@isslab.korea.ac.kr

Hyundo Yoon
Dept. of Computer Science and Engineering
Korea University, South Korea
hdyoon@isslab.korea.ac.kr

Youngjoo Shin
Dept. of Computer and Information Engineering
Kwangwoon University, South Korea
yjshin@kw.ac.kr

Junbeom Hur
Dept. of Computer Science and Engineering
Korea University, South Korea
jbhur@isslab.korea.ac.kr

Abstract

Many mail user agent (MUA) programs support email encryption functionality to clients using crypto libraries such as GnuPG. In 2013, Yarom and Falkner demonstrated FLUSH+RELOAD cache side-channel attack is used to extract RSA private key in GnuPG 1.4.13. In this study, we propose a novel attack scenario based on FLUSH+RELOAD attack, and demonstrate that a list of MUA programs are still vulnerable to FLUSH+RELOAD attack, even if the vulnerability is resolved in the latest version of GnuPG in practice. Specifically, we evaluated 37 MUAs, and conducted in-depth analysis of 13 ones among them, which are available in Ubuntu 14.04 and 16.04. According to our experiment, we found that about 77% of the MUAs are vulnerable to the FLUSH+RELOAD attack. Our attack could recover 92% of the bits of RSA private key of a victim when he receives and decrypts email contents using the MUA.

Background

Mail User Agent (MUA)

- MUA is a program providing integrated interface for e-mail service.
- **Encrypted email:** Many MUAs support email encryption for providing confidentiality of the email contents as fallow.
  1. A MUA encrypts email contents with public key of recipient exploiting a crypto library such as GnuPG.
  2. Receiver can use own private key to decrypt the received email with exploiting corresponding crypto library (GnuPG in this case).

FLUSH+RELOAD cache side-channel attack

- Yarom and Falkner proposed FLUSH+RELOAD attack and demonstrated the attack is able to restore RSA private key on GnuPG 1.4.13.
  1. FLUSH: Load the target data to memory and use CLFLUSH instruction to flush the memory line.
  2. RELOAD: Reload the same data and measure the elapsed access time.
- Short access time: The victim accessed memory before the reload phase.

Analyzing MUA

- We tested whether MUAs allow installation of GnuPG 1.4.13, which is vulnerable to FLUSH+RELOAD attack.

TABLE I. VULNERABILITY ANALYSIS OF MUAS

	Ubuntu 14.04		Ubuntu 16.04	
MUA	**Version**	**GnuPG 1.4.13**	**Version**	**GnuPG 1.4.13**
Alpine	2.10	Allowed	2.20	Allowed
Balsa	-	-	2.5.6	Allowed
Claws Mail	3.9.3	Allowed	3.13.2	Allowed
Cone	0.89	Allowed	1.0	Allowed
Evolution	3.10.4	Allowed	3.18.5.2	Allowed
GNUmail	-	-	1.2.2	Allowed
i.Scribe	-	-	2.2	Allowed
KMail	4.13.3	Allowed	5.1.3	Allowed
Thunderbird	52.9.1	Prevented	60.2.1	Prevented
Seamonkey Mail	-	-	2.49.4	Prevented
Sylpheed	-	-	3.5	Prevented
Trojit	0.7	Allowed	-	-
Zimbra	7.3.1	Allowed	-	-

Acknowledgement: This work was supported by the research fund of Signal Intelligence Research Center supervised by the Defense Acquisition Program Administration and Agency for Defense Development of Korea.

Attacking MUA

Our attack scenario

1. An attacker runs spy process fora FLUSH+RELOAD attack, then sends an encrypted email to a victim.
2. A victim reads the encrypted email, then MUA exploits GnuPG 1.4.13 to decrypt contents.
3. The attacker obtains an execution flow of Square-and-Multiply operations during the victim's decryption (Fig. 1).
4. The attacker converts the obtained sequence of operations into bit representation by using a converter we implemented.

- Result: The adversary could restore 92% of the victim's RSA secret key in this attack (Fig. 2).

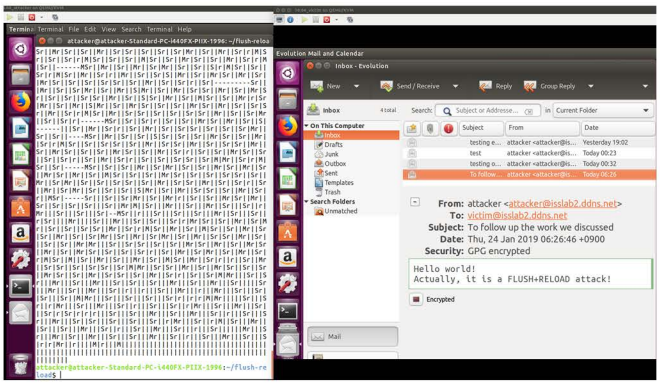

Fig. 1. Attacking Evolution 3.18.5.2 in Ubuntu 16.04

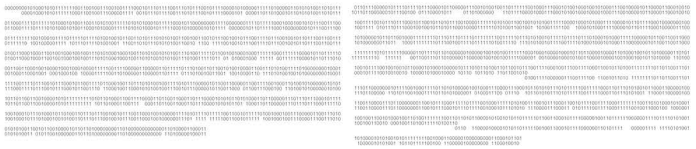

Fig. 2. Restored RSA private key of victim

Conclusion and discussion

In this study, we proposed a novel MUA attack scenario based on FLUSH+RELOAD attack, and demonstrated that a list of practical MUAs are still vulnerable to the attack. In our attack, we could exploit the extinct vulnerability of old crypto library because of implementation flaws in MUA applications, that is lack of simple version control of library on which they rely. Besides MUAs we investigated, any other applications can be exposed to the same threat if there are similar implementation flaws. As we demonstrated in this study, disallowing any vulnerable crypto library would be the first line of defense to protect users' private information.

References

[1] D. Poddebniak, C. Dresen, J. M'uller, F. Ising, S. Schinzel, S. Friedberger,J. Somorovsky, and J. Schwenk, "Efail: breaking s/mime and openpgp email encryption using exfiltration channels," in USENIX Security Sym-posium, 2018, pp. 549–566.

[2] K. Thomas, F. Li, A. Zand, J. Barrett, J. Ranieri, L. Invernizzi, Y. Markov,O. Comanescu, V. Eranti, A. Moscicki et al., "Data breaches, phishing,or malware?: Understanding the risks of stolen credentials," in ACM SIGSAC Conference on Computer and Communications Security, 2017,pp. 1421–1434.

[3] Y. Yarom and K. Falkner, "Flush+ reload: A high resolution, low noise, l3 cache side-channel attack." in USENIX Security Symposium, vol. 1, 2014, pp. 22–25.

KOREA UNIVERSITY · ISSLAB Information System Security Laboratory · KWANGWOON UNIVERSITY