Sri Lanka Institute of Information Technology

BSc. Hons in Information Technology specialized in Cyber Security

Department of Information System Engineering

Secure Software Engineering

Assignment

IT17136884 – Prabhathi S.H.U

IT17111034 – U.C.S Bandara

Contents

Table of figures

Table of Table

Mozilla Thunderbird

Domain and Historical Analysis

Product Overview

Thunderbird is a free and open source e-mail client hosted by dreamhost[1]. It is cross platform, allows users running Microsoft Windows, macOS, Linux, and other supported systems to send, receive, and manage their e-mail [1]. Moreover, Mozilla thunderbird is a news client and chat client. This was developed by Mozilla foundation and version 1.0 released on 7th of december 2004 [1]. But this was developed, tested and supported largely by dedicated volunteers and paid staff. This is an independent community driven project and as a result budget and salary of staff totally managed by thunderbird council [2]. With the help of contributors around the world, clients are translated into 50 languages. But email addresses limited to ascii local parts currently [2].

Originally this launched as Minotaur and then it was named as phoenix [1]. But the project could not get the momentum because of the failure. After the success of the project minotaur named as thunderbird and demand gradually increased mail clients to go with it. Then it changed to a new toolkit introduced by Firefox. First three days it got 500 000 downloads. But important and significant work on thunderbird started after the release of version 1.5. Through the new toolkit Mozilla suite created for separate applications [1].

In December 2004, a new feature called project that was lightly integrated about the calendar functionality and it is a full range calendar mechanism and protocol supported by calendar infrastructure.

The Thunderbird development team expected to accomplish many objectives through it. Message management is one of their goals, through that they are expected to manage multiple emails, news feed, chats and newsgroups [1]. Moreover, providing quick search, message groups, virtual folders or saved search folders, advanced message filtering. Thunderbird provides junk filtering or basic spam filtering system [1]. It includes a whitelist based on the provided address book and server based filter called SpamAssaisian [1].

Thunderbird uses industry standards for email as POP basic email retrieval protocol, IMAP, LDAP, OPENPGP and for webfeeds it provides ATOM and RSS. Additionally, extensions allow through installation of XPinstall modules is add-on to the website and update function of it [1]. Apart from that there are downloadable themes available at the add-on website at Mozilla add-ons. Moreover, this grants mailbox using plugins. Mbox, unix mailbox format and maildir are the mailboxes supported in 2014 [1].

Finally, thunderbird provides more security features like TLS/SSL connection to IMAP and SMTP servers and native support for S/MIME secure email means digital signing and message encryption using certificate. Optional security provided by disabling loading of remote images with messages, only enabling specific media types etc. [1].

Product Assets

Asset	Functionality	Intangible property that attacker want to exploit
Emails	Receive, read, compose and send emails.	Through malicious emails like spam,keyloggers, ransomware etc and social engineering techniques.
Chats	Instant messaging using IRC, XMPP, twitter and google talk	Not having a proper encryption mechanism for messages.
Address Book	Add people to profile and maintain the contacts.	Not updated address book file system.
Database	Storing the copy of the e-mails.	Malicious code execution in the global database.
Profile	local mail that copies of the messages that reside on the mail server and stores the changes done when user using thunderbird	Not having a proper access control mechanism.

Add-ons	Resources that add extensions and other additional functions to the thunderbird	Less protected add-ons without proper cryptographic function.
Frameworks	backend programming core languages, debuggers, patching, source control management, collaborations, build automation etc.	Common errors of programming languages and tools.

Table 1 - Assets

Emails

Email is one of the most critical asset of the thunderbird. It is the easiest possible way to attack the system. Because cyber criminals use emails based attacks to spread malware. Mainly attackers send malicious attachments to install keyloggers, ransomwares and other malwares, links to malicious web sites and enticements to perform transactions by social engineering to enter sensitive details like credentials of financial accounts etc. [3]. Finally, proper encryption mechanism and digital signatures is the best protective method for mails [4].

Chats

To use the chat, user have to create a new account or configure the current account with an online instant messaging provider. XMPP, Google talk, Twitter are some examples [5]. Previously there was a OTR (off the record messaging) feature. But currently it is disable according to user expectations it can be activated [6]. So this OTR makes it possible to use end to end encryption for the chats exchanged with the contacts. Then this works only in one to one chats [6].

If you send an unencrypted message to someone, and that person also supports OTR, it can be detected, and both users will automatically initiate a handshake to start an encrypted conversation. User does not know there is a man in the middle attacker active [6]. So user should identify the conversation partner to avoid a man in the middle attack. There are many verification processes established in thunderbird for that. If the users exchange verification information through the internet, that channel can be controlled by man in the middle attackers. So use different channels for verification by using correct keys [6].

.

Address book

One click address book is an easy and fast way to add people to your profile or account [7]. Contacts can be added easily by clicking the star icon of the received email [7]. Address book is also an asset that needs to be backed up [8]. Because the address book file system is not fully immune to attacks that may happen in the user's system. Files stored in the local system get a high opportunity to corrupt and accidental deletion [8]. Additionally, malware like virus and worms can damage MAB file [8]. Due to this condition every user must do the back up to protect their contacts by manually or MAB converter [8].

Database

Database is an essential resource of any software. According to the thunderbird terminology database known as Global database or gloda [9]. This system makes thunderbird more efficient through quick search of emails to users. There is a global-message-db.sqlite file and can be found in thunderbird profile folders. This file contains copies of all the emails.

One flaw of the file is, this can create a large database as it contains all the copies of the messages. But there is a feature to disable the index file. But users can still search the messages in the current folder.

Email clients can be subjected to exploitation by attackers due to several reasons. Thunderbird database is also subject to exploitation like malwares. Malicious codes can be attached to the mails. But those codes did not activate by reading the email. Thunderbird renders those mails by loading please wait message under the main message in the body section. Although part of the attachment rendered script that exploit code does not trigger.

Profile

profile is the place where two main items, as local mail that copies of the messages that reside on the mail server and stores the changes done when user using thunderbird. As an example for the second item, changes done in account settings, changes to toolbars can take. After installing thunderbird, it creates default profile and that profile invokes automatically, if the user does not

invoke profile manager to create a new account [10]. Profile stored in thunderbird program files. Program files are static and do not change.

Add-ons

Add-ons is one of product assets or resources that add extensions and other additional functions to the thunderbird [11]. As a result of open extensible design and program architecture, thunderbird allows create add-ons for it. Those add-ons are mostly created by Mozilla volunteers. Therefore, Mozilla are not responsible for supporting add-ons if a user needs any help he needs to contact the add on author. Most add-ons can be found in thunderbird add-ons site or through itself in thunderbird. Thunderbird update add-ons but users have to check them manually [11]. Some add-ons are enigmail, mail merge, confirm address, check and send, signal spam, password tags etc. [12].

Enigmail adds openPGP message encryption and authentication to thunderbird and it's based on GnuPG for cryptographic function. But there were some forgery attacks against the openPGP implementation. Spoofed valid signatures, ID attacks, UI attacks, GPG API attacks are an example for that [13].

Frameworks

Thunderbird is a cross platform mail client application developed by Mozilla framework. This is a central toolkit framework. C and C++ are the backend programming core languages [14]. MSVC for windows, gdb for linux and Mac OS X are debuggers. Apart from those, there are patching, source control management, collaborations, build automation etc [14].

Example attacks

1. Malicious code execution through spam mails

Distribution of malware like virus, worms, adware, spyware, trojans etc cause for execution of malicious code and compromise [15]. Those codes attached to emails and

sent and those are activated when the victim opens the email, clicks a link on the message or any other interaction with the message. Those malicious code included viruses mostly spread by sending the same mail to contacts in the victim's address book [16].

Ransomware is also a kind of email virus that encrypts the victim's data like emails and shared documents and demands a value to give them back. As a result, confidentiality of the data is reduced. Mainly those attacks are done by hacking groups. This can be considered as spam too.

2. Phishing attacks

Again phishing is another possible attack on thunderbird. Because it tricks users to enter their credentials or other sensitive data [16]. As a result, confidentiality and sometimes integrity of the data violate. Individual or group wise cybercriminals do these attacks [17].

3. Spoofing

Lack of efficient mechanism of email protocols for authenticating emails address cause for this. As a result, hackers can use addresses and domains to act like legitimate ones. Therefore, victims tricked by fraudulent mails like actual ones. As well as confidentiality breaks [18].

4. Man in the Middle attacks

Similarly, clicking the attachments sent by attackers cause access to the user's web browser. Therefore, attackers can direct the users to fake websites that look like actual one. When the user logs those fake websites, attackers gain the credentials. So confidentiality and integrity of the data violates [19].

Vulnerability History

Vulnerability 1

CVE number - CVE-2019-11752 [20]

CVE- 2019-11752 vulnerability announced on 3rd of september 2019 and reported by Zhanjia Song. It is a critical vulnerability that affects Firefox products including thunderbird. According to the CVE details, the severity level of the vulnerability is 9.3 [20]. This vulnerability affected 155 versions in thunderbird. MITRE CVE dictionary stated that, this vulnerability can delete an indexdb key value and try to extract when conversion happening [20].

As a result, after free and potentially exploitable crash may happen. Vulnerability can be exploitable with network access; it implies vulnerable software is bound with network stack. As a result, attackers do not need local network access or local access for exploitation [21]. According to the exploitability complexity, the attackers are limited to the group of systems or users at some level of authorization. The vulnerability is not affected for non-default configurations or common configurations. As an example when a server performs user account configuration through specific scheme vulnerability can be presented. But not presented in another authentication schema. The attack requires a social engineering part like phishing to modify the web browser's status bar to show a false link [21].

According to CVE details confidentiality impact is completed [20]. Because there is total information disclosure by revealing all system files. Similarly, there is integrity violation happening because of the loss of system protection. That might lead to editing system files by the attacker. Moreover, this complete shutdown of the resources causes violation of availability. Finally, authentication is not needed to exploit the vulnerability.

The patches are available for the vulnerability and installing updates from the vendor's website is the mitigation [22].

Vulnerability 2

CVE number - CVE-2017-7826 [23]

CVE-2017-7826 was announced by Mozilla developers and community members Christial Holler, David Keeler, John Coppeard, Jan de Mooij, Jason Kratzer, Philipp, Nicholas Nethercote, Oriol Brufau, André Bargull, Bob Clary, Jet Villegas, Randell Jesup, Tyson Smith, Gary Kwong, and Ryan VanderMeulen. This was published on 11th of june 2018 in CVE [24].

According to the NVD unwanted vetting of parameters and passed with prompt: Open IPC message between child and parent processes can cause opening of parent process with non-sandboxed that the web content chosen by compromised child process. As a result, those can be combined with additional vulnerabilities and execute arbitrary code on the user's computer. MITRE stated that this is a memory safety bug that was reported in Firefox 56 and Firefox ESR 52.4 [24]. There is some evidence of memory corruption. More over vulnerability may lead to dos attacks and spoofing of the sender's email address.

CVSS score is 10. 205 versions of thunderbird affected by the vulnerability. Confidentiality and integrity impact is completed. As a result, there is a complete information disclosure and compromise of the system. Access control is very low and authentication is not requirement to exploit the relevant vulnerability [25].

Vulnerability 3

CVE number - CVE-2019-11708

This vulnerability was found by Google's Project Zero's Samuel Groß and the Coinbase Security team in the mid of April of 2019[26]. Severity of this vulnerability marked as 10 because all confidentiality, integrity, and availability can be compromised by this vulnerability. Not only Thunderbird but also Mozilla Firefox and Mozilla Firefox ESR are affected by this vulnerability.

By this vulnerability, attackers can bypass the sandbox by using Prompt:Open IPC message and create a parent process outside the sandbox [28]. And this will allow remote access to the victims account.

To overcome this vulnerability Mozilla has released patch updates. All the versions below the Thunderbird 60.7.2 are vulnerable to this vulnerability [27]. In Thunderbird 60.7.2 it is fixed and it has disabled the scripting when reading the mail.

Vulnerability 4

CVE number - CVE-2017-7845

Severity of this vulnerability is marked as 9.3. This vulnerability is only affected on the windows operating system [4]. Omair, Sabri Haddouche, and cure53 are the reporters who reported the issue [30].

It has an impact on all confidentiality, integrity, and availability because when drawing and validating elements using Direct 3D 9 with the ANGLE graphics library, used for WebGL content a buffer overflow occurs [29].

To this vulnerability, the vendor has released patch updates. All products after Thunderbird 52.5.2 are free of this vulnerability.

Design Analysis

Architectural Overview

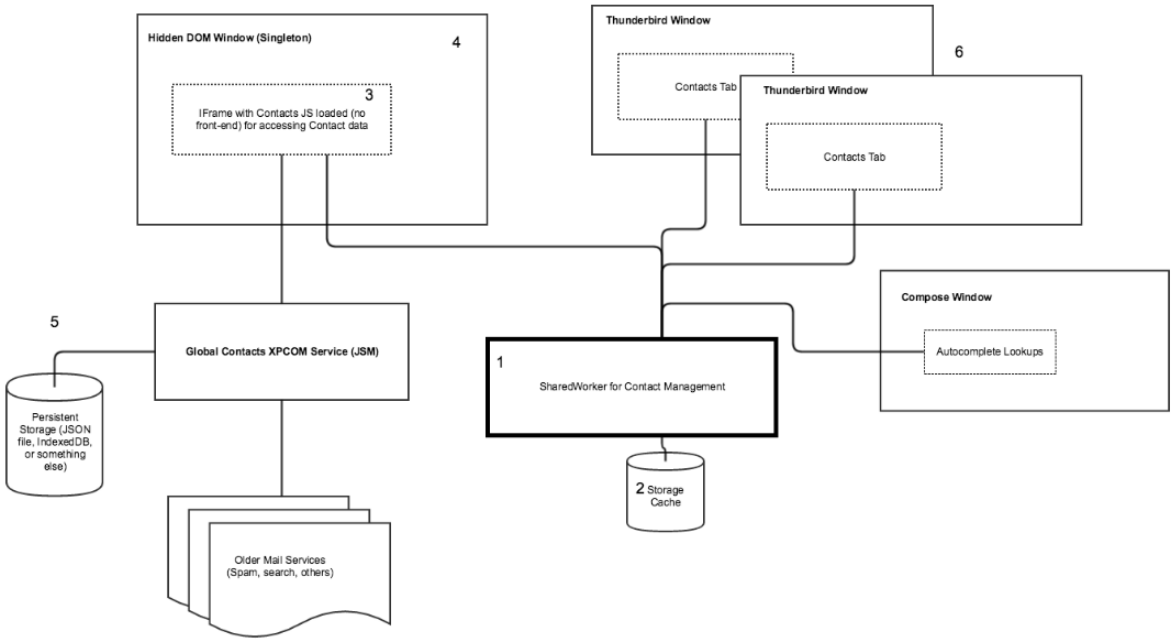


Figure 0-1 Architectural overview

Main function

Main functionality of this product is to work as a mail client. Not like a common mail client it uses POP, IMAP, LDAP, S/MIME, and OpenPGP standards to control the emails [31]. This product supports Linux, Windows, and macOS. When setting the mail client, we can use asymmetric authentication and signature-based authentication.

Sub functions

· 1. Tabbed email

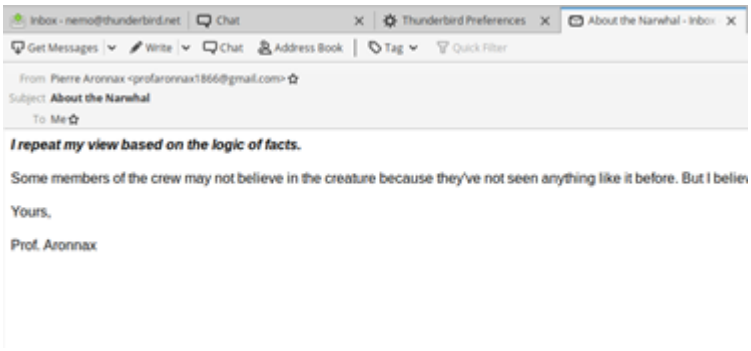


Figure 0-2 - Tabbed mail

By this function it allows user to use multiple emails in different tabs. When quitting Thunderbird, visible tabs will be saved and will be restored when you open Thunderbird the next time [32].

· 2. Filter and search Toolbar

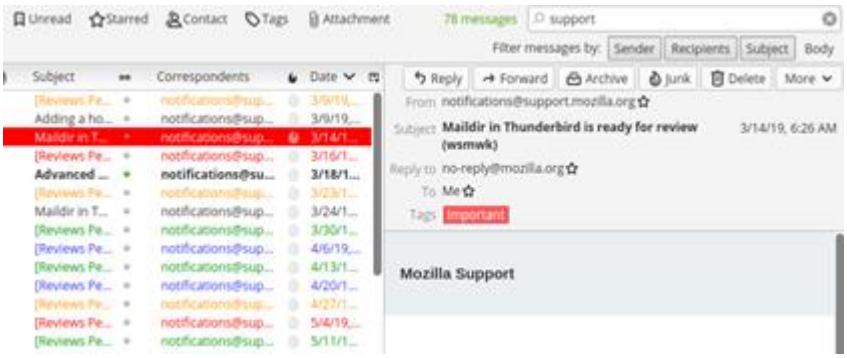


Figure 0-3 - Filtering

Thunderbird allows users to add filters to sort the emails quickly. Users can filter your email by New Messages, Tags, and people in users Address Book.

Figure 0-4 - Searching mails

In Thunderbird users allows to search massages and emails according to the time and sender.

· 3. Cutting Out the Junk

In thunderbird there is a tool which can identify the spam mails. It will identify how user mark spams and automatically identify the spams.

· 4. Customize your email experience

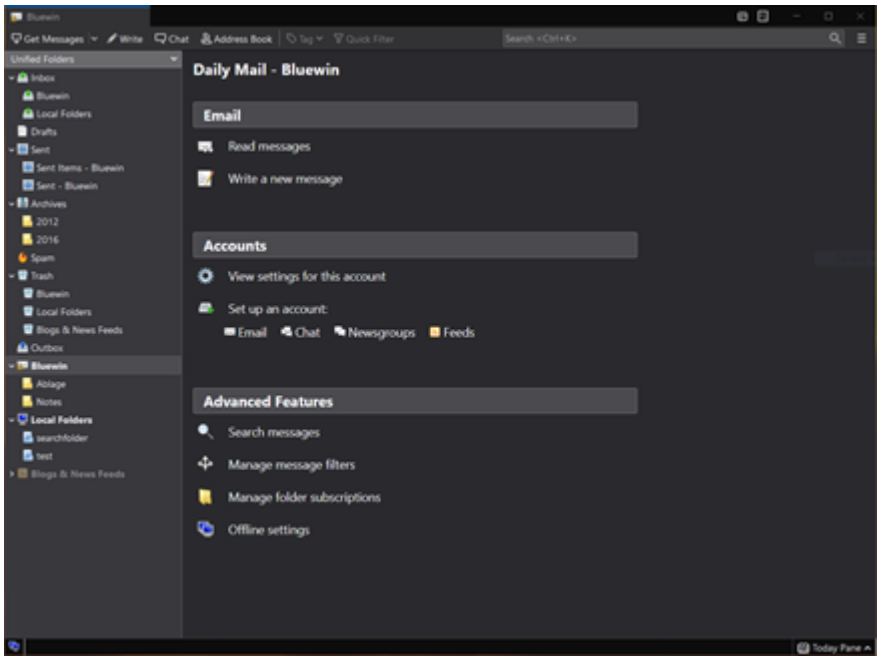
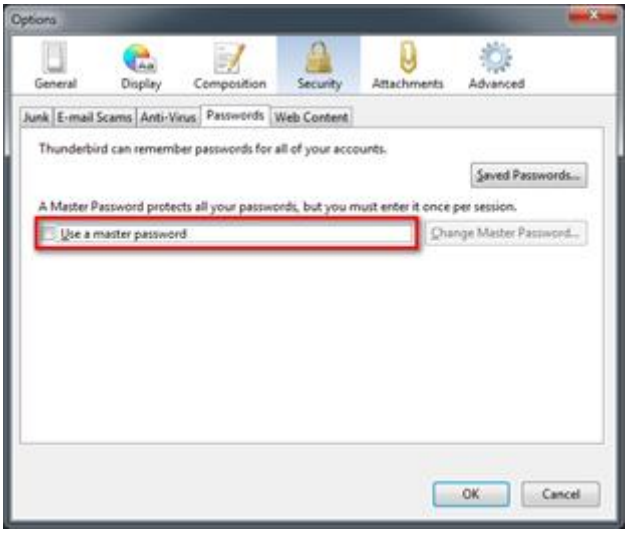


Figure 0-5 - Themes

As a user of thunderbird there are many themes that users can use.

Basic level security.

· 1. Protect your Thunderbird passwords with a Master Password



When we log in to a mail client anyone who is login to the machine can be seen all the mails and chat. To prevent that thunderbird has implement master password. If someone log in to the PC also should enter the mater key to read the mail [33].

Design security principals [34]

- Least Privilege
    - Do not expose unnecessary services

      In here they do not give the access to services which user don't want to access.
    - Do not grant or retain permissions that are no longer needed

      In here they remove the services from expired user.
- Defense in Depth
    - Do not allow lateral movement

      Make attacker difficult to access the other hosts on the network from the current host.
    - Isolate environments

      Use different infrastructures for different services to limit the impact of a security breach.
    - Patch Systems

      Make sure that there are no any known vulnerabilities to exploit.
    - Guarantee data integrity and confidentiality

Use proper actions to ensure that integrity and confidentiality are protected.

- Know Thy System
    - Fraud detection and forensics

      Monitor the system to detect all the suspicious behavior.
    - Are you at risk?

      Asses the risk and take the necessary actions.
    - Inventory the Landscape

      Maintain proper system records for all assets.
    - KISS - Keep It Simple and thus Secure

      Keep the system simple and it is easy to secure the system.
- Authentication and authorization
    - Require two-factor authentication

      Use 2FA when log in to the system or services.
    - Use central identity management (Single Sign-On)

      Use one pair of credentials to access the all services of the organization.
    - Require strong authentication

      Use sessions to manage the user logins and use strong credentials to log in.

Threat Model

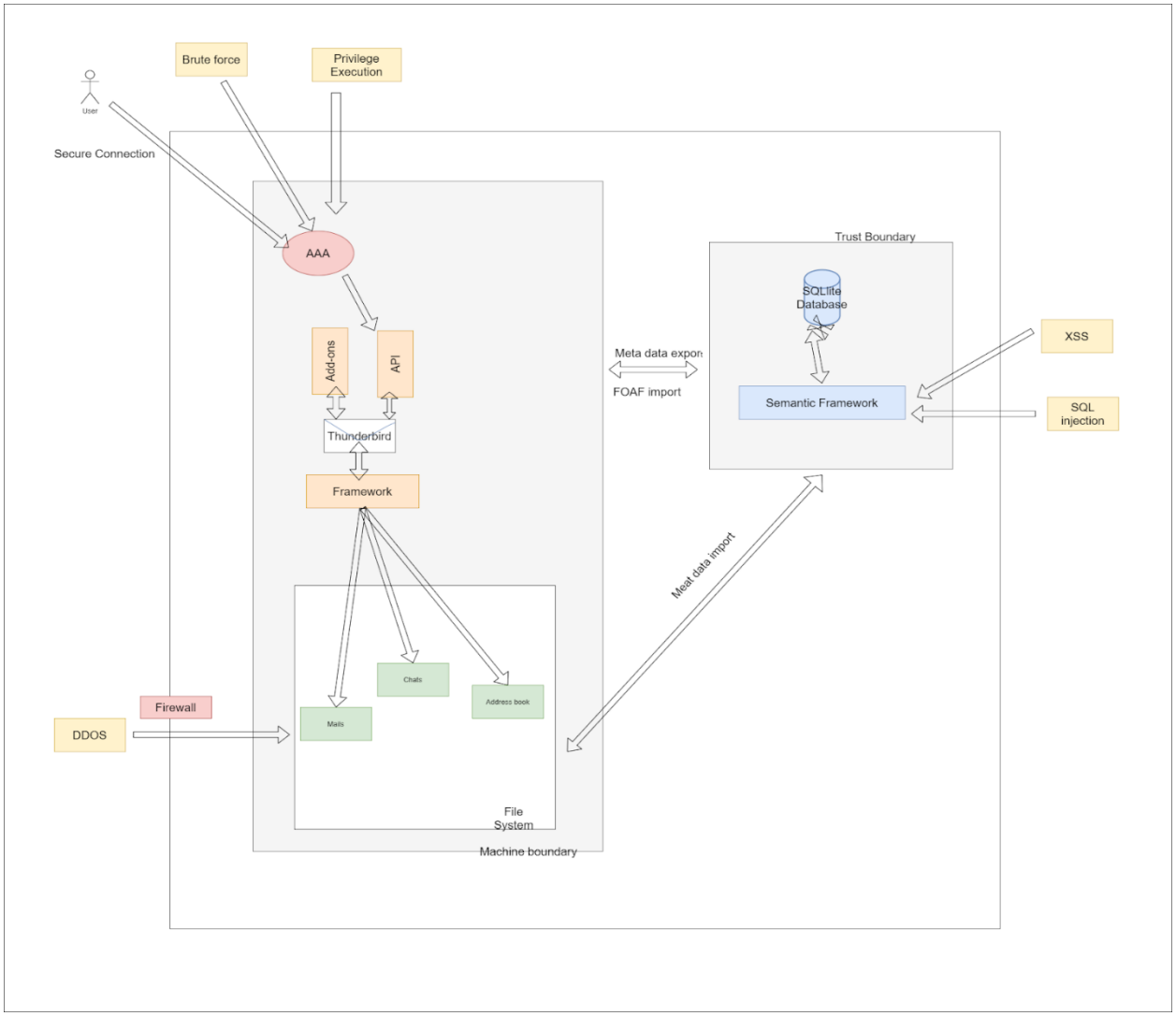


Figure 0-7 - Threat model

Assets to threat model tracing

1. E-mails
2. Chats
3. Address book
4. Database
5. Profile

6. Add-ons
7. Framework

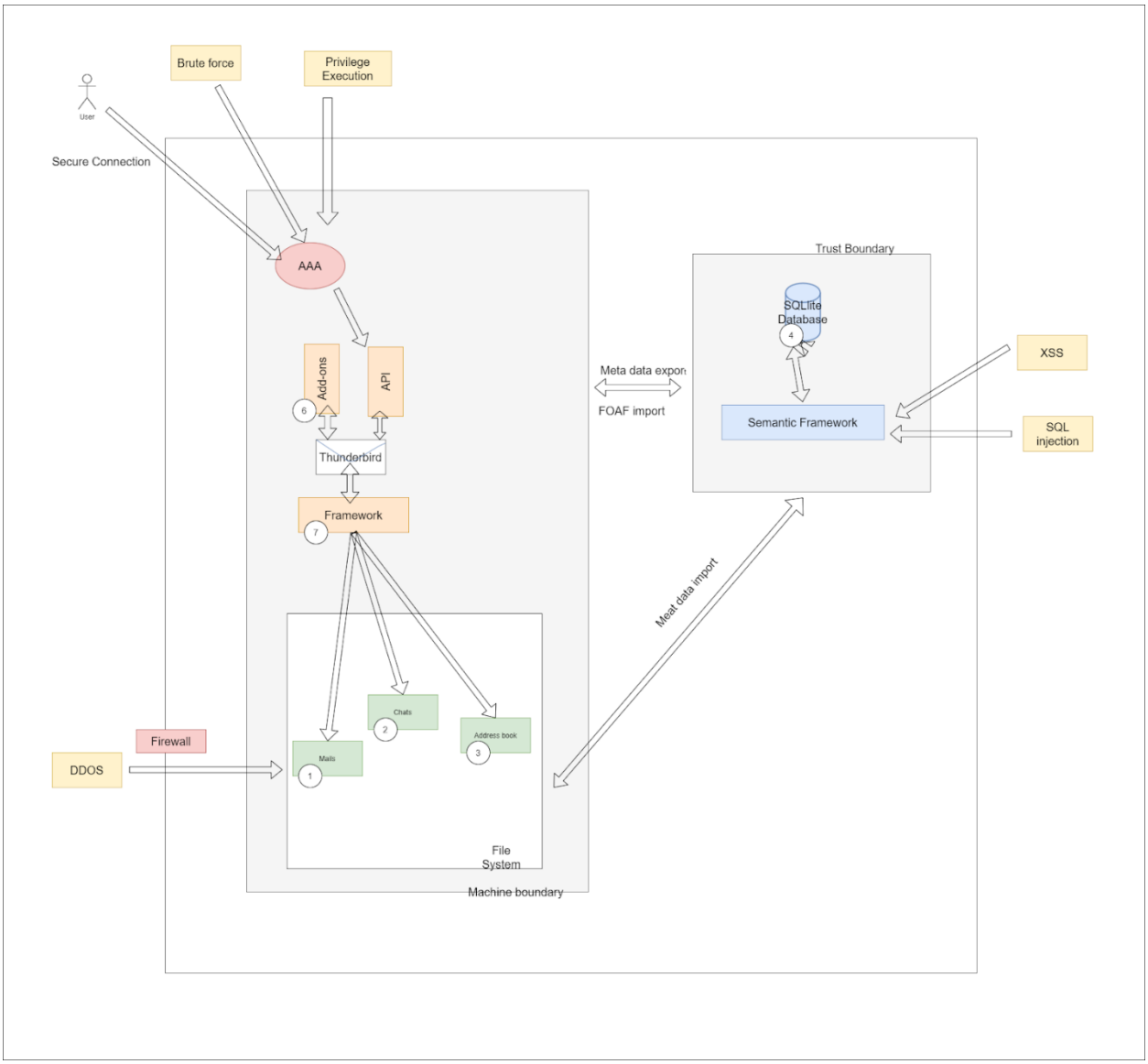


Figure 0-8 - Asset to threat model

According to the architecture there are 2 boundaries as Machine boundary and Trust boundary. Inside the machine boundary there is a location called file system. File system is the base location for most of the assets. But there is a risk because if there is a backdoor on the host all the assets can be affected. When we drawing the treat model asset called profile cannot be placed inside it because prolife is combination of all the other assets and it is the outcome of the product.

Code Inspection Assessment

Code review and inspection

File name -: imAccounts.jsm

Link of the file -: https://searchfox.org/comm-central/source/chat/components/src/imAccounts.jsm

Basic function -: setting up a thunderbird account for the email.

function	
UnknownProtocol()	This function stands for finding the protocol when setting the thunderbird account.
UnkownAccount()	This function stands for checking of inserted known account.
imAccount()	This function stands for setting up thunderbird account for the email. There only 3 parameters call here as aKey, aName, aPrplID. Inside this function protocol plugin to unknown instance is called. Apart from that check whether account is stored in SQLite db, getting prplIAccount from protocol plugin are called here. And most important part of the account is password creation. It is called inside this function by service.logins.initializationPromise.then. Again there are getters and setters for the password and master password exception handled. connect(), autologin(), remove() also called inside.
AccountService()	Here, get _accountList(), processAutoLogin(), creatAccount(, deleteAccount() can see. There is code if user cancel master password prompt to convert old password. Through AccountService function big focus given to autologin process. So developers implement disable auto login if they running safe mode, check if they crash the startup during auto login, locate last crash file etc.

Table 2 - imAccounts

Reason to select that file -: in thunderbird Account is the basic function. So I select this file to check whether how the developers implement account wizard and what are the mechanisms they use to create password when creating account. According to my opinion, if there is no any proper code for master password creation and other password process this code may be vulnerable.

File name -: ExtensionToolbarButtions.jsm

Link of the file -: https://searchfox.org/comm-central/source/mail/components/extensions/ExtensionToolbarButtons.jsm

Basic function -: buttons of adding and removing extensions to the thunderbird.

function	
onMainfestEntry()	Inside this function makebutton(), paint(), unpaint(), are called.
triggerAction()	Getpopup() function that returns pre-loaded url in given window, updateButton() for update toolbar, getIconData() to update UI are done by this code part.
update Window()	This function is written for button that update when the toolbar extension icon, title, url etc.
getTargetfromwindow()	Through this can get active tab of the passed window if the window has tabs or window itself.
getAPI()	Get API files

Table 3 - ExtensionToolbarButtions

Reason to select -: I select this file because this code for buttons of extension toolbar and this extends the extensionAPI. Extensions are very important when using thunderbird. So adding them removing them through button is controlled by here. Additionally, there is a code segment for getting API files also.

File name: imContacts.jsm

Searchfox link: https://searchfox.org/comm-central/source/chat/components/src/imContacts.jsm

Basic Function: manage the contacts of chats.

Functions Inside this code and their process:

	Function	Process
01	executeAsyncThenFinalize(statement)	Sync and finalize the contacts
02	getDBConnection()	Establishing the database connection
03	TagsService()	Checking and creating tags for chats
04	Contact(aId, aAlias)	Creating the contacts
05	ContactsService()	Manage creating editing and deleting of contacts

Table 4 - imContacts

Reason to choose this file: In Thunderbird, chat option is a sub function. In chat it is very important to consider how the contacts are added to the chat menu. This can be led to a vulnerability if there are any mistakes. Because of that inspecting of this code file should be done.

File name: logger.jsm

Searchfox link: https://searchfox.org/comm-central/source/chat/components/src/logger.jsm

Basic Function: log all the chat activities.

Functions Inside this code and their process:

	Function	Process
01	queueFileOperation(aPath, aOperation)	Identify the operating system and queue the operations to execute
02	appendToFile(aPath, aEncodedString, aCreate)	Adding required parent files to the operating system
03	encodeName(aName)	Encode the name of the device
04	getNewLogFileName(aFormat, aStartTime)	Create new log file for new accounts
05	LogWriter(aConversation)	Log all the details of the account activities
06	getLogWriter(aConversation)	Get the log files
07	Logger()	Log all the details to existing file otherwise creates one

Table 5 - logger

Reason to choose this file: when we consider about any system it is very important to keep a log record. In this code it demonstrates how log file is created and updated. Because of this it is essential to inspect code like this.

Project specific checklist and Domain specific concerns

Project specific checklist [34]

According to the LGTM details,

1. Incomplete url substring sanitization.
2. Unnecessary “pass” statement.
3. Unreachable code.
4. Multiple calls to __init__ during object initialization.
5. Variable defined multiple times.
6. Import of deprecated module.
7. Unguarded next n generator.
8. Unused named argument in formatting call.
9. Use of ‘global’ at module level.
10. Deprecated slice method.
11. Duplication in regular express character class.
12. Signature mismatched in overriding method.
13. __init__ method call overriding.
14. __eq__ not overridden when adding attributes.
15. Use of the return value of the procedure.
16. Nested loops with the same variables.
17. Module is imported with ‘import’ and ‘import from’.
18. Except block handle ‘Baseexcepion’
19. Unused local variables.
20. Unused import.

Coding Mistakes

Changed server not reflected in the saved password list is a bug reported in Bugzilla about thunderbird security that severity is normal and priority is not set. Platform is x86_64 windows 10 [35].

Can’t send S/MIME encrypted between two identities on the same account is another bug reported in thunderbird security domain that type is defective. The severity level is normal and the priority is also not set [36].

Another security domain bug is a warning window appears spontaneously ‘add security exception’. Similarly, severity level is normal. It appears in x86 windows xp platform [37].

Design Errors

- In 2018, January it is announced that Thunderbird starts working on improving it’s interface to enhance user retention and make it more user friendly [38].

Summary

Mozilla Thunderbird is free and open source email client software that relies on various operating systems like Mac os, windows and linux. It provides many features like sharing emails, instant messaging, newsgroups and feeds etc. So the ultimate goal of this prose is to look around what are assets of thunderbird like emails, chats, address book, add-ons, database etc, what are possible attacks on it, how to minimize those attacks, what are the vulnerabilities reported in the first chapter. Then this comes across the design phase of thunderbird and architectural overview takes part in it. Then the threat model with four functions and how assets mapped with the threat model is discussed. Finally, the code inspection phase takes place. The source code taken by serachfox website and four files of it inspected according to the reasons of the selection. Additionally, project specific checklist created with reference to LGTM and few design concerns and coding mistakes added.

References

[1] Mozilla Thunderbird [Internet]. En.wikipedia.org. 2020 [cited 29 April 2020]. Available from: https://en.wikipedia.org/wiki/Mozilla_Thunderbird

[2] Thunderbird FAQ | Thunderbird Help [Internet]. Support.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://support.mozilla.org/en-US/kb/thunderbird-faq

[3] Love J. Top 10 Malicious Email Threats [Internet]. Lastline. 2020 [cited 29 April 2020]. Available from: https://www.lastline.com/blog/top-10-malicious-email-threats/

[4] Thunderbird:OpenPGP:2020 - MozillaWiki [Internet]. Wiki.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://wiki.mozilla.org/Thunderbird:OpenPGP:2020

[5] Instant Messaging and Chat | Thunderbird Help [Internet]. Support.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://support.mozilla.org/en-US/kb/instant-messaging-and-chat

[6] Thunderbird:OTR - MozillaWiki [Internet]. Wiki.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://wiki.mozilla.org/Thunderbird:OTR

[7] Thunderbird Features [Internet]. Thunderbird. 2020 [cited 29 April 2020]. Available from: https://www.thunderbird.net/en-US/features/

[8] How to Backup Mozilla Thunderbird Address Book [Internet]. Systoolsgroup.com. 2020 [cited 29 April 2020]. Available from: https://www.systoolsgroup.com/updates/how-to-backup-thunderbird-address-book/

[9] [Internet]. 2020 [cited 29 April 2020]. Available from: https://www.uslsoftware.com/global-database-in-thunderbird/

[10] Profiles - Where Thunderbird stores your messages and other user data | Thunderbird Help [Internet]. Support.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://support.mozilla.org/en-US/kb/profiles-where-thunderbird-stores-user-data

[11] Thunderbird add-ons - frequently asked questions | Thunderbird Help [Internet]. Support.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://support.mozilla.org/en-US/kb/thunderbird-add-ons-frequently-asked-questions#w_what-is-an-add-on

[12] Privacy and Security: Add-ons for Thunderbird [Internet]. Addons.thunderbird.net. 2020 [cited 29 April 2020]. Available from: https://addons.thunderbird.net/en-US/thunderbird/extensions/privacy-and-security/

[13] [Internet]. Usenix.org. 2020 [cited 29 April 2020]. Available from: https://www.usenix.org/system/files/sec19-muller.pdf

[14] Thunderbird:Backend Hacking Guide For Newbies - MozillaWiki [Internet]. Wiki.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://wiki.mozilla.org/Thunderbird:Backend_Hacking_Guide_For_Newbies

[15] How to Protect Yourself Against Vulnerabilities in Email Clients [Internet]. Spamlaws.com. 2020 [cited 29 April 2020]. Available from: https://www.spamlaws.com/email-client-vulnerability.html

[16] Cluley G. Does spammed out malware attack exploit Mozilla Thunderbird ‘feature’? [Internet]. Naked Security. 2020 [cited 29 April 2020]. Available from: https://nakedsecurity.sophos.com/2012/02/02/malware-attack-exploit-thunderbird

[17] Stine K, Scholl M. E-mail Security: An Overview of Threats and Safeguards [Internet]. Library.ahima.org. 2020 [cited 29 April 2020]. Available from: http://library.ahima.org/doc?oid=99319#.XqSJp2gzaUn

[18] EI-ISAC Cybersecurity Spotlight - Spoofing - CIS [Internet]. CIS. 2020 [cited 29 April 2020]. Available from: https://www.cisecurity.org/spotlight/cybersecurity-spotlight-spoofing/

[19] [Internet]. 2020 [cited 29 April 2020]. Available from: https://secureswissdata.com/man-in-the-middle-attack-email

[20] CVE-2019-11752 : It is possible to delete an IndexedDB key value and subsequently try to extract it during conversion. This results in a [Internet]. Cvedetails.com. 2020 [cited 29 April 2020]. Available from: https://www.cvedetails.com/cve/CVE-2019-11752/

[21] CVE-2019-11752 - Mageni [Internet]. Mageni.net. 2020 [cited 29 April 2020]. Available from: https://www.mageni.net/cve/CVE-2019-11752

[22] Multiple vulnerabilities in Mozilla Firefox [Internet]. Cybersecurity-help.cz. 2020 [cited 29 April 2020]. Available from: https://www.cybersecurity-help.cz/vdb/SB2019090305

[23] CVE-2017-7826 : Memory safety bugs were reported in Firefox 56 and Firefox ESR 52.4. Some of these bugs showed evidence of memory corrup [Internet]. Cvedetails.com. 2020 [cited 29 April 2020]. Available from: https://www.cvedetails.com/cve/CVE-2017-7826/

[24] Security vulnerabilities fixed in Firefox 57 [Internet]. Mozilla. 2020 [cited 29 April 2020]. Available from: https://www.mozilla.org/en-US/security/advisories/mfsa2017-24/

[25] CVE-2017-7826 - Red Hat Customer Portal [Internet]. Red Hat Customer Portal. 2020 [cited 29 April 2020]. Available from: https://access.redhat.com/node/3241651

[26] Second Firefox Zero-Day Announced - CVE-2019-11708 [Internet]. eSentire. 2020 [cited 23 April 2020]. Available from: https://www.esentire.com/security-advisories/second-firefox-zero-day-announced-cve-2019-11708

[27] Security vulnerabilities fixed in Thunderbird 60.7.2 [Internet]. Mozilla. 2020 [cited 23 April 2020]. Available from: https://www.mozilla.org/en-US/security/advisories/mfsa2019-20/

[28] CVE-2019-11707, CVE-2019-11708: Multiple Zero-Day Vulnerabilities in Mozilla Firefox Exploited in the Wild [Internet]. Tenable®. 2020 [cited 23 April 2020]. Available from: https://www.tenable.com/blog/cve-2019-11707-cve-2019-11708-multiple-zero-day-vulnerabilities-in-mozilla-firefox-exploited-in

[29] NVD - CVE-2017-7845 [Internet]. Nvd.nist.gov. 2020 [cited 24 April 2020]. Available from: https://nvd.nist.gov/vuln/detail/CVE-2017-7845#vulnCurrentDescriptionTitle

[30] Mozilla Thunderbird Multiple Flaws Let Remote Users Spoof Email Addresses, Obtain Potentially Sensitive Information, and Execute Arbitrary Code - SecurityTracker [Internet]. Securitytracker.com. 2020 [cited 24 April 2020]. Available from: https://www.securitytracker.com/id/1040123

[31] Mozilla Thunderbird [Internet]. En.wikipedia.org. 2020 [cited 25 April 2020]. Available from: https://en.wikipedia.org/wiki/Mozilla_Thunderbird

[32] Thunderbird Features [Internet]. Thunderbird. 2020 [cited 25 April 2020]. Available from: https://www.thunderbird.net/en-US/features/

[33] Protect your Thunderbird passwords with a Master Password | Thunderbird Help [Internet]. Support.mozilla.org. 2020 [cited 25 April 2020]. Available from: https://support.mozilla.org/en-US/kb/protect-your-thunderbird-passwords-master-password

[34] Security Principles [Internet]. Infosec.mozilla.org. 2020 [cited 25 April 2020]. Available from: https://infosec.mozilla.org/fundamentals/security_principles.html

[35] LGTM [Internet]. Lgtm.com. 2020 [cited 29 April 2020]. Available from: https://lgtm.com/projects/g/JosiahOne/thunderbird-clone/?mode=list

[36] 1288988 - Changed server not reflected in Saved password list [Internet]. Bugzilla.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://bugzilla.mozilla.org/show_bug.cgi?id=1288988

[37] 570748 - Can't send S/MIME encrypted between 2 identities on the same account [Internet]. Bugzilla.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://bugzilla.mozilla.org/show_bug.cgi?id=570748

[38] 639374 - A warning window appears spontaneously; "Add Security Exception" [Internet]. Bugzilla.mozilla.org. 2020 [cited 29 April 2020]. Available from: https://bugzilla.mozilla.org/show_bug.cgi?id=639374

[39] Thunderbird Starts Working on Improving Its Interface—Take Part In the Survey [Internet]. Monterail.com. 2020 [cited 29 April 2020]. Available from: https://www.monterail.com/blog/thunderbird-new-interface-redesign-survey