UNIVERSITY OF ZAGREB

FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

MASTER THESIS No. 326

E-MAIL SECURITY

Vid Mužević

Zagreb, February 2024

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

MASTER THESIS No. 326

E-MAIL SECURITY

Vid Mužević

Zagreb, February 2024

UNIVERSITY OF ZAGREB
FACULTY OF ELECTRICAL ENGINEERING AND COMPUTING

Zagreb, 02 October 2023

MASTER THESIS ASSIGNMENT No. 326

Student:	**Vid Mužević (0036516912)**
Study:	Computing
Profile:	Computer Science
Mentor:	assoc. prof. Miljenko Mikuc

Title: **E-mail security**

Description:

In the business world, e-mail is a fundamental means of communication. The specification of the "Simple Mail Transfer Protocol", SMTP, which is used for the exchange of electronic mail, does not contain any security mechanisms. About 20 years ago, mechanisms were added to enable more secure communication between email servers: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These mechanisms make it possible to verify the identity of the sender. Nowadays, most e-mail servers are hosted by large cloud service providers. Therefore, the security mechanisms mentioned cannot always be used reliably. Your task is to research the email protection mechanisms currently available, both at the user level and at the email server level. Using your own e-mail addresses as an example, show how these security mechanisms work and how they can be used to ensure secure communication.

Submission date: 09 February 2024

SVEUČILIŠTE U ZAGREBU
FAKULTET ELEKTROTEHNIKE I RAČUNARSTVA

Zagreb, 2. listopada 2023.

DIPLOMSKI ZADATAK br. 326

Pristupnik:	**Vid Mužević (0036516912)**
Studij:	Računarstvo
Profil:	Računarska znanost
Mentor:	izv. prof. dr. sc. Miljenko Mikuc

Zadatak: **Sigurnost elektroničke pošte**

Opis zadatka:

Elektronička pošta je u poslovnom svijetu temeljni način komunikacije. Specifikacija protokola "Simple Mail Transfer Protocol", SMTP, koji se koristi za razmjenu elektroničke pošte ne uključuje nikakve sigurnosne mehanizme. Prije 20-tak godina, dodani su mehanizmi koji omogućavaju sigurniju komunikaciju između poslužitelja elektroničke pošte: SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) i DMARC (Domain-based Message Authentication, Reporting, and Conformance). Ovi mehanizmi omogućavaju verifikaciju identiteta pošiljatelja. U današnje vrijeme većina e-mail poslužitelja smještena je kod velikih pružatelja usluga u oblaku. Kao rezultat toga, navedeni sigurnosni mehanizmi ne mogu se uvijek pouzdano koristiti. Vaš zadatak je istražiti trenutačno dostupne mehanizme za zaštitu elektroničke pošte kako na razini korisnika, tako i na razini e-mail poslužitelja. Koristeći vlastite e-mail adrese kao primjere, demonstrirajte kako ovi sigurnosni mehanizmi funkcioniraju i kako se mogu iskoristiti za osiguravanje sigurne komunikacije.

Rok za predaju rada: 9. veljače 2024.

With great thanks to my mentor, Dr. Miljenko Mikuc for his invaluable assistance in the creation of this thesis. With thanks to my friends, for motivating me to make it this far in my academic career. And finally, with thanks to my fiancée, Petra Jović, for helping me retain my sanity during this final year.

Contents

1 Introduction

As the world's technology continues to advance, so too has reliance on the internet. Lately, devices ranging from speakers to washing machines have all become a part of the so-called "Internet of Things" or "IoT", which is defined as "a network of interrelated devices that connect and exchange data with other IoT devices and the cloud." [1] Naturally, almost every device connected to the internet requires a strong security system, as any one vulnerability can be used as a way into the entire network, and as such has become another front line for the constant arms race between attackers and cybersecurity professionals, and so the focus of cybersecurity experts in 2023 was mainly around cloud technologies along with AI and Zero trust [2]. But what about the security of older technologies? E-mail predates the internet, so surely most of the vulnerabilities should be fixed in the 52 years since its conception in 1971, considering it's widespread use even today. Sadly that's not the case.

Ian D. Foster, Jon Larson, Max Masich, Alex C. Snoeren, Stefan Savage and Kirill Levchenko pointed out the importance of e-mail security in their research article by saying: "Email as we use it today makes no guarantees about message integrity, authenticity, or confidentiality. Users must explicitly encrypt and sign message contents using tools like PGP if they wish to protect themselves against message tampering, forgery, or eavesdropping" [3].

E-mails are extremely common in everyday business and private use. In their book, "E-mail Security, A Pocket Guide", Furnell and Dowland say that e-mail offers indisputable benefits but that "such significant use introduces inevitable elements of dependence and exposure" and that "reliance upon e-mail can introduce the first element of risk, especially when the underlying technology does not provide a guaranteed service" [4].

This thesis will focus on E-mail security measures and the shortcomings thereof, as well as the ethics behind such security research, examples of e-mail based attacks and an experiment on spoofing e-mails. Protocols such as SMTPS, SSL and TLS for HTTPS, STARTTLS, SMTP MTA-STS, SPF, DKIM, DMARC will be explained, as well as SSL/TLS, STARTTLS and SPF vulnerabilities. The importance for change in e-mail security will be indicated, by a safely and ethically conducted e-mail spoofing experiment.

2 Security and e-mails

2.1 Security overview

The digital world is both a blessing and a curse. Being connected to the entire world through a device is a blessing when it comes to the availability of information and communication. However it is also a curse, as malicious users will use this worldwide connection to access your device and the information within. The methods of these attacks vary wildly depending on the type of attack.

It cannot be understated how important protection of information is, and as a result, the US government introduced the five pillars of Information Assurance [5], [6], those being:

- Integrity
- Availability
- Authentication
- Confidentiality
- Non-repudiation

Integrity means ensuring that the information system and information within can not be tampered with.
Availability means ensuring that anyone that should have access to the information can have access at all times.
Authentication means ensuring that those who have access to the information are who they say they are. This can be achieved through passwords, two-factor authentication, biometric identification and other methods.

Confidentiality involves the confidentiality of information, meaning that if only a subset of the group using a certain information system are authorized to view a certain file, then that subset and only that subset can view the aforementioned file.
The final pillar is non-repudiation, which ensures that any user that commits to an action within the information system cannot deny having taken said action, such as the modification of a file.

2.2 Ethics of security

There is a lot of public and private data on the internet and on devices connected to the internet. Private data can belong to different sources, from ordinary people, large corporations, government bodies etc. Leaking of that data can lead to big losses, that can impact on a lot of aspects such as money or personal image. Christen, Gordijn and Loi state in their book called "The Ethics of Cybersecurity" [7] that "due to the uptake of information and communication technology (ICT) in the business sector, the value of information has increased" and also that "information is now considered the new oil and as oil brought both prosperity and problems, so too does information" which is in regards to the importance of data security. There are a few regulations around the world on the topic of cybersecurity. One of them is "The Cybersecurity Act (EU 881 / 2019)" which is defined as a "European regulation that introduces a harmonised European system for the cybersecurity certification of ICT products, services and processes" [8].

Different domains of information can have different ethical issue. For example if some information is from the health care system and other is from a social networking company their ethical problems would not be the same. Christen, Gordijn and Loi listed the 15 most important ethical issues in cybersecurity for the business domain. Those are as follows: [7]:

1. Privacy

2. Protection of data

3. Trust

4. Control

5. Accessibility

6. Confidentiality

7. Responsibility on businesses to use ethical codes of conduct

8. Data integrity

9. Consent

10. Transparency

11. Availability

12. Accountability

13. Autonomy

14. Ownership

15. Usability

In regards to the healthcare domain there are some ethical principals and technical aims that can be mapped together to make ethical healthcare cybersecurity. Those ethical principals are [7]:

- Autonomy
- Non-maleficence
- Beneficence
- Justice

On the other hand the technical aims are [7]:

- Efficiency and quality of services
- Privacy of information and confidentiality of communication
- Usability of services

- Safety

An example of the mapping of principals and aims is the mapping of *Autonomy* to *Privacy of information and confidentiality of communication* with the reasoning being "privacy is often seen as a prerequisite of patients' autonomy and therefore privacy maps to the principle of autonomy" [7].

There are also some ethical issues regarding e-mail security. David B. Resnik and Peter R. Finn write about phishing ethics and ethics behind conducting experiments in their article named "Ethics and Phishing Experiments". They say that "phishing experiments that simulate real world conditions can provide cybersecurity experts with valuable knowledge they can use to develop effective countermeasures and prevent people from being duped by phishing emails" [9]. But there are also problems with conducting such experiments and for them to be completely ethical, risks need to be minimized, confidentiality and privacy need to be protected, potential participants need to have an opportunity to decline research before it begins, and participants need to be informed when that experiment is finished [9].

Kevin Macnish and Jeroen van der Ham pointed out in their article that there needs to be "a greater appreciation of the risks of cybersecurity development in academic ethical review committees and clear (and enforceable) codes of conduct for, or at least active discourse within, the professional community which cover development and practice" [10].

2.3 E-mail security

E-mails and e-mail systems are not exempt from the Information Assurance pillars, as they are used to transmit information, and e-mails are often stored in a cloud. In order to cover the requirements of said pillars, e-mails use both standard internet security protocols as well as protocols designed specifically for emails.

2.3.1 SMTPS

Simple Mail Transport Protocol Secure (SMTPS) is and extension of Simple Mail Transport Protocol (SMTP). SMTP is used to transmit e-mails between servers. SMTPS adds security to SMTP by establishing a secure connection between servers using SSL/TLS.

2.3.2 SSL and TLS

Secure Sockets Layer (SSL) and its successor Transport Layer Security (TLS) are cryptographic protocols. SSL and TLS are primarily used to create a secure HTTP connection, more commonly known as a HTTPS connection. They are designed to provide secure communication in a network by using encryption algorithms to secure data transmitted between a client and a server. In the context of e-mail security, SSL and TLS can be used to secure the connection between the e-mail client and e-mail server. This fulfills the requirement for confidentiality, protecting against man-in-the-middle attacks and eavesdropping. The communication channel is created through a process known as a "handshake" which is performed as follows [11]:

- Client Hello message - Client sends a "Hello" message to the server along with the TLS version, supported cipher suites and some random bytes
- Server Hello message - Server replies to clients hello message with the server's SSL certificate, the chosen cipher suite and the "server random" string
- Authentication - Client confirms SSL certificate with the issuing authority
- Premaster secret - Client sends random string of bytes to server using public key infrastructure
- Private key - server decrypts premaster secret
- Session keys - client and slave use the client random, server random and premaster secret to generate session keys
- Client ready - client sends a "finished" message encrypted with the session key
- Server ready - server sends a "finished" message encrypted with the session key
- Secure symmetric encryption achieved

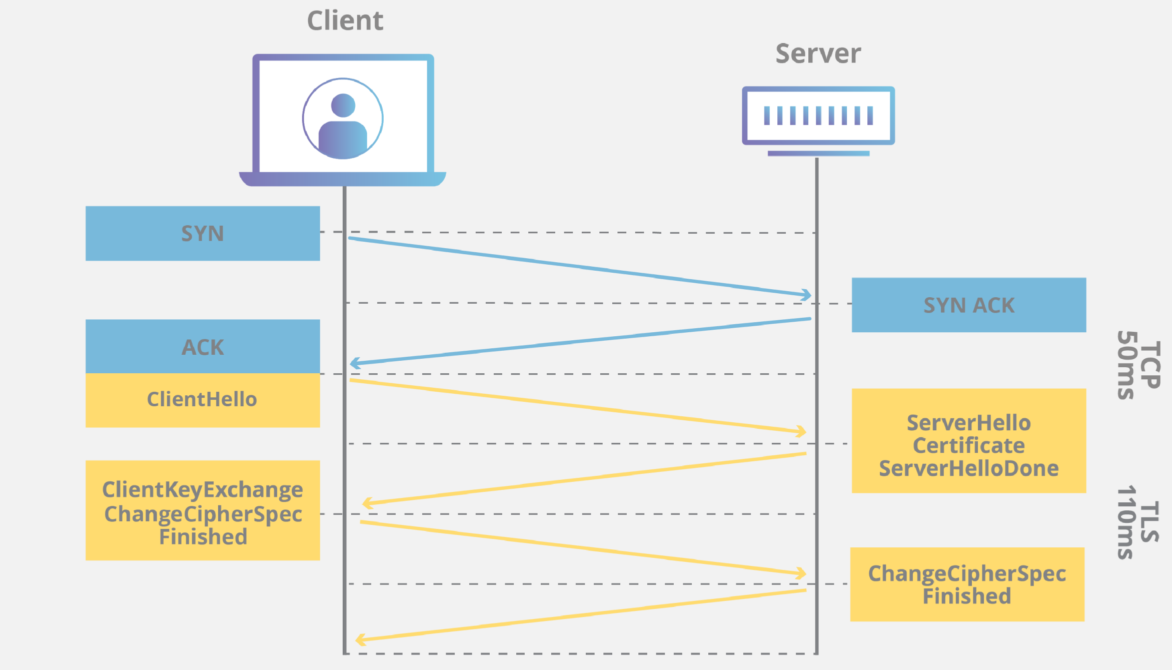


Figure 2.1: A graphical representation of the SSL/TLS handshake
Source: https://www.cloudflare.com/learning/ssl/what-happens-in-a-tls-handshake/

2.3.3 STARTTLS

STARTTLS is an extension to SMTP, IMAP and POP3 protocols which upgrades the plaintext connection to an encrytped SSL/TLS connection. The connection is established as follows [12]:

- TCP handshake between e-mail client and server for identification
- Server replies with "220 Ready" to notify client that it can continue with the communication
- Client send "EHLO" message to inform the server that it would like to use Extended SMTP (Advanced SMTP that allows images, attachments, etc.)
- Client sends "250-STARTTLS" to the mail server to check if StartTLS is accepted
- If the server responds with "go ahead", the StartTLS connection can be created
- The client restarts the connection and encryption is established

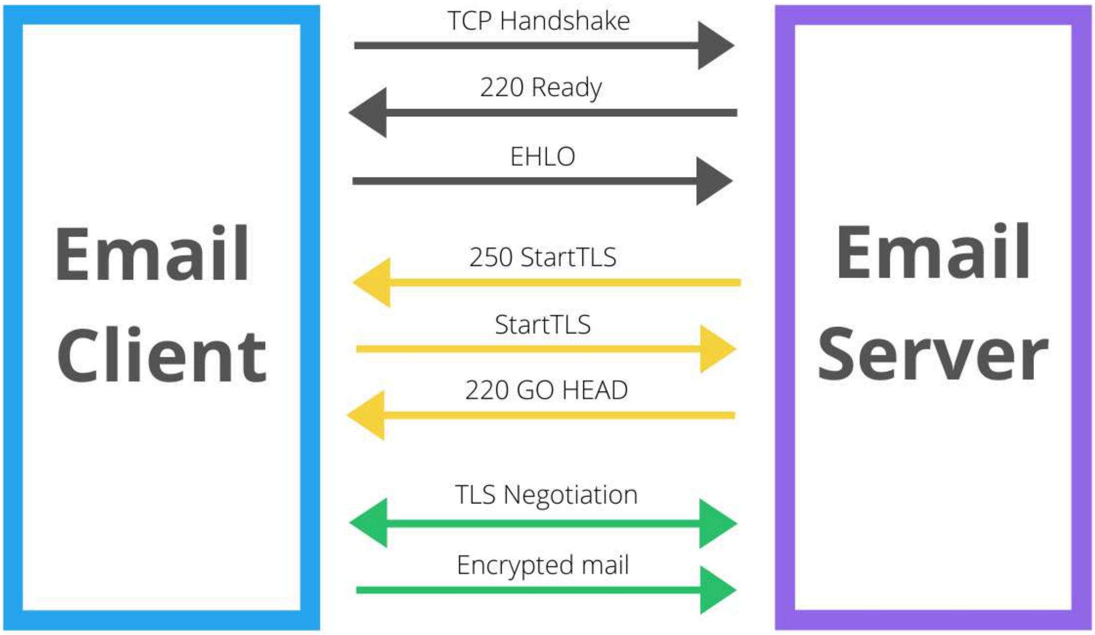


Figure 2.2: A graphical representation of the StartTLS connection
Source: https://sendgrid.com/en-us/blog/what-is-starttls

2.3.4 SMTP MTA-STS

SMTP Mail Transfer Agent Strict Transport Security (SMTP MTA-STS) is a security protocol that enforces the use of SSL/TLS for e-mail transmission. It defines a policy that e-mail servers can publish which specifies required encryption levels and authentication for e-mail communication. When a client connects to the server it checks for the presence of the MTA-STS policy, and if present ensures that the connection meets the specified requirements. Otherwise the e-mail is refused.

2.3.5 SPF

Sender Policy Framework (SPF) is an e-mail authentication protocol that helps prevent e-mail spoofing and phishing attacks. This is achieved by allowing domain owners to define a list of authorized e-mail servers with permission to send e-mails on behalf of their domain.

When an e-mail server receives an e-mail message, it checks the SPF record for the sender's domain to determine if the message originated from an authorized e-mail server. If authorized, the e-mail is is accepted; otherwise, the message is rejected. This helps prevent unauthorized parties sending e-mail messages which appear to be from a legitimate domain. Here is an example of an SPF record with explanations[13]:

```
TXT @ “v=spf1 a include: spf.google.com ~all”
```

- TXT - Specifies that the SPF record is stored in the DNS in text format
- @ - Placeholder that represents the current domain
- v=spf1 - represents and SPF record version of 1
- a - Authorizes systems in "domain A" record to send e-mails on behalf of the organization
- include - Authorizes a third-party to send e-mails on behalf of the domain, in this case Google
- all - Means that all e-mails will be allowed to pass through. Does not prevent suspicious e-mails from being flagged.

2.3.6 DKIM

DomainKeys Identified Mail (DKIM) is an e-mail authentication protocol that helps ensure the integrity of e-mail messages by allowing the sender to digitally sign their messages. This ensures the message has not been tampered with (Integrity).
When an e-mail server sends a message it generates a digital signature using the sender's private key, which is then included in the message header. When the receiver's e-mail server receives the message, it uses the sender's public key available in the sender's DNS records to check if the signature is valid. If valid, the message is accepted; otherwise the message is rejected. Here's an example with flag explanations[14]:

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=asuswebstorage.com;
s=default; t=1572282571; bh=NFzBvJ/pEmf+yUHDd/Y7dYNH9pE+Bx6o95KcxhwFL78=;
h=From:To:Subject:From; b=QwgINKqwcBu3GbeWm2Be81qXks6Pq9yMmDZl9C6mT8moX...
```

- v - the version

- a - signing algorithm used for the creation of a DKIM record
- c - canonicalization algorithm for the header and body
- d - domain where the DKIM is signed
- s - DKIM selector
- t - timestap of when the e-mail was signed
- bh - hashed e-mail body
- h - list of headers
- b - the digital signature

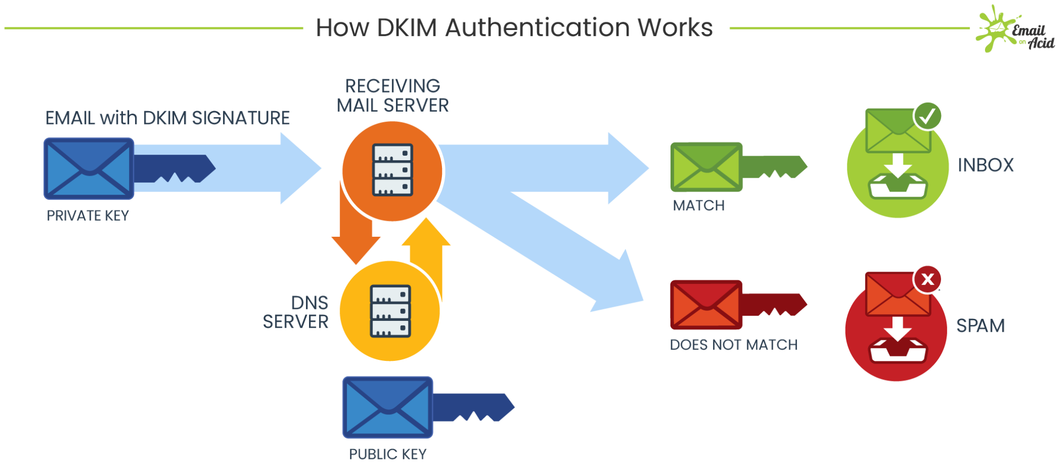


Figure 2.3: A graphical representation of DKIM protocol
Source: https://media.emailonacid.com/wp-content/uploads/2021/07/DKIM-Authentication-Process.png

2.3.7 DMARC

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an e-mail authentication protocol that improves upon SPF and DKIM to provide a better countermeasure to e-mail spoofing and phishing. DMARC works by allowing domain owners to define a policy that specifies how e-mail servers should react when confranted with a message that fails SPR or DKIM checks.

When an e-mail server receives an e-mail message it performs an SPF and DKIM check to determine the authenticity of the message. If either or both of these checks fail, then the server checks the DMARC policy for the sender's domain in order to determine how to handle the message. The policy could state:

- Reject the message
- Quarantine the message
- Accept the message
- Do nothing

An example DMARC record in the DNS[15]:

```
"v=DMARC1; p=none; rua=mailto:dmarc@yourdomain.com"
```

This is the full list of flags that can be added to a DMARC record[15]:

- v - Version
- p - policy
- pct - Percentage of e-mails subject to filtering
- rua - For reporting URI's (Uniform Resource Identifier) for aggregate data
- ruf - designates to which addresses forensic information is to be reported
- fo - defines how forensic reports are created and presented
- aspf - alignment mode for SPF
- adkim - alignment mode for DKIM
- rf - reporting format
- ri - reporting interval
- sp - handling policy for subdomains

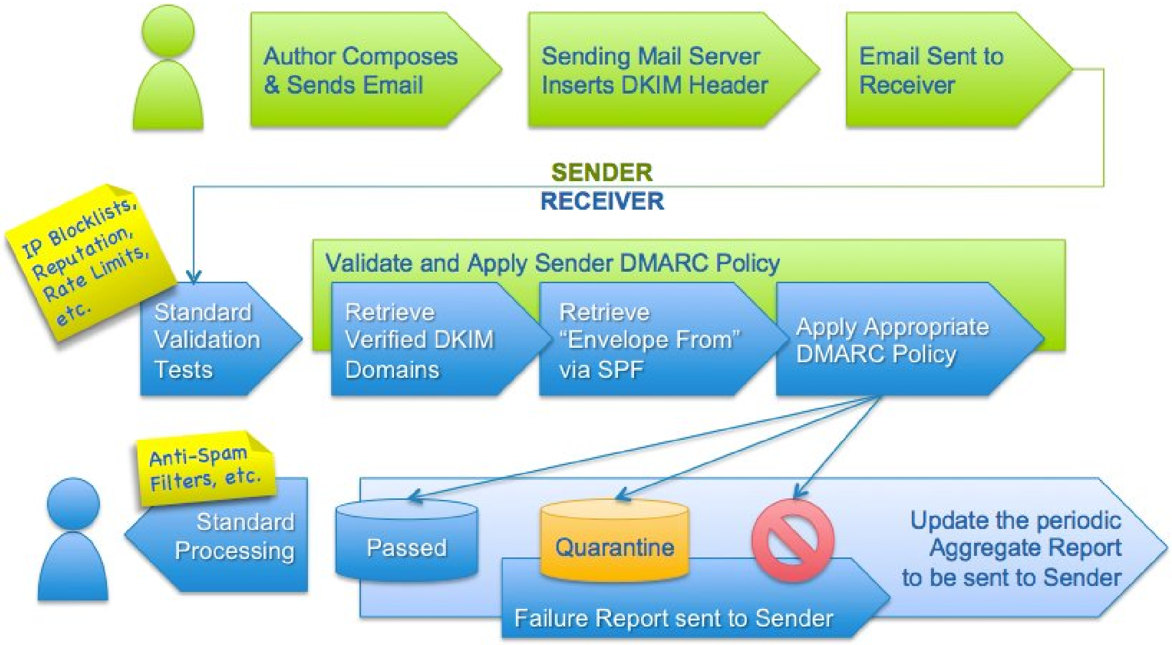

Author Composes & Sends Email
Sending Mail Server Inserts DKIM Header
Email Sent to Receiver
SENDER
RECEIVER
IP Blocklists, Reputation, Rate Limits, etc.
Standard Validation Tests
Validate and Apply Sender DMARC Policy
Retrieve Verified DKIM Domains
Retrieve "Envelope From" via SPF
Apply Appropriate DMARC Policy
Anti-Spam Filters, etc.
Standard Processing
Passed
Quarantine
Update the periodic Aggregate Report to be sent to Sender
Failure Report sent to Sender

Figure 2.4: A graphical representation of DMARC protocol
Source: https://dmarc.org/wp-content/uploads/2015/02/DMARC_author-to-recipient_flow.jpg

2.4 E-mail security vulnerabilities

Despite all of the aforementioned security implementations, e-mails are still a common vector of attacks, with multitudes of ways to exploit vulnerabilities in e-mail systems worldwide. Not all of the listed vulnerabilities are fully associated with e-mail's, however this section is dedicated to giving insight into just how vulnerable modern system's are, and putting the frequency of discovery of said vulnerabilities into context.

2.4.1 SSL/TLS Vulnerabilities

SSL/TLS comes in many versions, the most recent of which is TLS 1.3. Some servers or devices have not been updated to 1.3, and prior versions have known vulnerabilities. In fact, in 2021 a majority of US Healthcare sites were still using TLS 1.2, despite TLS 1.3 having been released in August of 2018. Following are a few example of vulnerabilities in earlier versions of SSL/TLS [16]:

- Beast Attack - TLS 1.0 - allowed attackers to capture and decrypt HTTPS client-server sessions. It combined a Man-in-the-Middle attack, record splitting and chosen boundary attack [17].

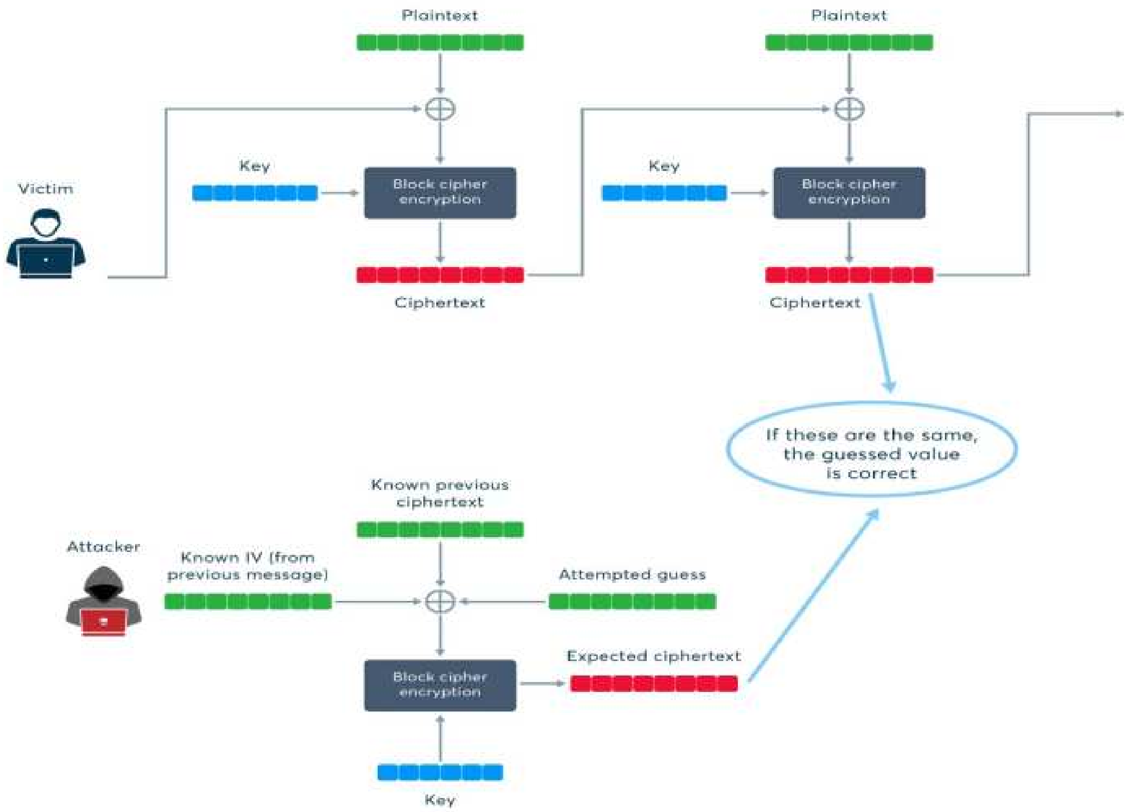


Figure 2.5: A graphical representation of beast attack
Source: https://www.invicti.com/blog/web-security/how-the-beast-attack-works/

- Raccoon Attack - TLS 1.2 and prior - Attacks the Diffie-Hellman key exchange process and uses the premaster secret to complete the handshake.

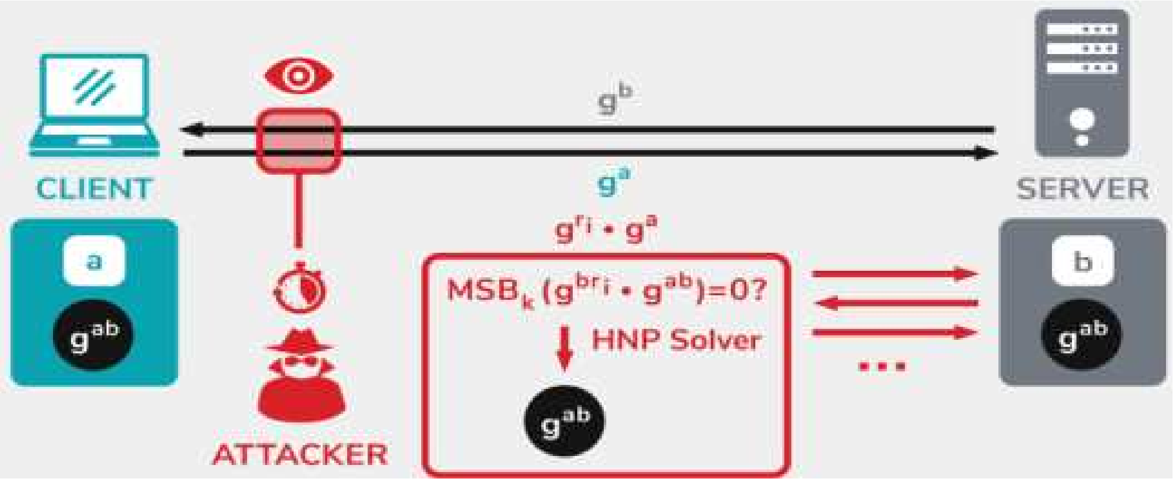


Figure 2.6: A graphical representation of raccoon attack
Source: https://raccoon-attack.com

- C.R.I.M.E (Compression Ratio Info-Leak Made Easy) - HTTPS using TLS 1.2 and below - C.R.I.M.E works by leveraging a property of compression functions. By noting how the length of compressed data changes, a Man-in-the-Middle attack is able to obtain plaintext HTTP headers using a series of guesses in which a string in a HTTP request may correspond to an unknown string.

The U.S Department of Health and Human services Cybersecurity program claimed that upgrading to TLS 1.3 would eliminate all known vulnerabilities including those above. However TLS 1.3 is not perfect and known vulnerabilities are published often on the National Vulnerability Database (NVD), a U.S government repository of standards based vulnerability data, held by the National Institute of Standards and Technology (NIST). Searching for TLS 1.3 in the NVD results in some of the following:

- "An issue was discovered in Mbed TLS 3.5.1. There is persistent handshake denial if a client sends a TLS 1.3 ClientHello without extensions" - January 21, 2024
- "The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences." - January 09, 2024
- "Matrix SSL 4.x through 4.6.0 and Rambus TLS Toolkit have a length-subtraction integer overflow for Client Hello Pre-Shared Key extension parsing in the TLS 1.3 server. An attacked device calculates an SHA-2 hash over at least 65 KB (in RAM). With a large number of crafted TLS messages, the CPU becomes heavily loaded." - December 21, 2023
- "A vulnerability in the TLS 1.3 implementation of the Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to cause the Snort 3 detection engine to unexpectedly restart." - November 01, 2023

2.4.2 STARTTLS Vulnerabilities

As established before, STARTTLS upgrades SMTP, IMAP and POP3 connections to use SSL/TLS, so naturally these connections are vulnerable to everything that SSL/TLS is vulnerable to. On top of that, STARTTLS itself has additional vulnerabilities:

- "A meddler-in-the-middle attacker can fixate their own session during the cleartext phase before a STARTTLS command (a violation of "The STARTTLS command is only valid in non-authenticated state." in RFC2595). This potentially allows an attacker to cause a victim's e-mail messages to be stored into an attacker's IMAP mailbox, but depends on details of the victim's client behavior." - May 29, 2023

- "Meddler-in-the-middle attackers can pipeline commands after POP3 STLS, IMAP STARTTLS, or SMTP STARTTLS commands, injecting cleartext commands into an encrypted user session. This can lead to credential disclosure." - May 29, 2023

- "The myMail app through 14.30 for iOS sends cleartext credentials in a situation where STARTTLS is expected by a server." - May 06, 2023

- "During the plaintext phase of the STARTTLS connection setup, protocol commands could have been injected and evaluated within the encrypted session. This vulnerability affects Thunderbird < 78.7." - December 22, 2022

The above vulnerability reports highlight another key factor in cybersecurity - developers must understand that just using a secure protocol makes their application secure. They must understand how the security protocol functions, and they must pay attention to what information their application puts out in the open when making a client-server application. The "iOS sends cleartext credentials" case is an unforgivable mistake, and is likely a result of developer over-reliance on copy-pasted code or gross incompetence in the field of security.

2.4.3 SPF Vulnerabilities

- "Exim before 4.97.1 allows SMTP smuggling in certain PIPELINING/CHUNKING configurations. Remote attackers can use a published exploitation technique to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This occurs because Exim supports <LF>.<CR><LF> but some other popular e-mail servers do not." - December 24, 2023

- "sendmail through 8.17.2 allows SMTP smuggling in certain configurations. Re-

> mote attackers can use a published exploitation technique to inject e-mail messages with a spoofed MAIL FROM address, allowing bypass of an SPF protection mechanism. This occurs because sendmail supports <LF>.<CR><LF> but some other popular e-mail servers do not. This is resolved in 8.18 and later versions with 'o' in srv_features." December 24, 2023

These 2 vulnerabilities were reported on the same day and are largely similar. The vulnerability states "This occurs because X supports <LF>,<CR><LF>". These are control characters, specifically for line breaks. Using these line breaks, headers can be edited. This can be categorized as a problem with sanitisation of inputs, which is as important in e-mails as in any other online input field.

3 E-mail Attacks

E-mail attacks can be broadly categorized into categories and subcategories. Here are some examples:

3.1 Phishing

Phishing is the act of sending a fraudulent e-mail with intent to trick a recipient into relinquishing information or clicking and/or installing a malicious program to achieve a similar goal. Many variants of phishing exist including the following:

- Spearphishing - Essentially the same as regular phishing, but highly specialized for a certain group or individual. ex. Sending a phishing e-mail such that it looks like a person's boss, wife or other significant individual sent the e-mail.

- Vishing - Vishing is phishing using voice communication technology. Usually performed over telephone, with modern AI technology are able to clone someones voice and send a recording through e-mail [18]

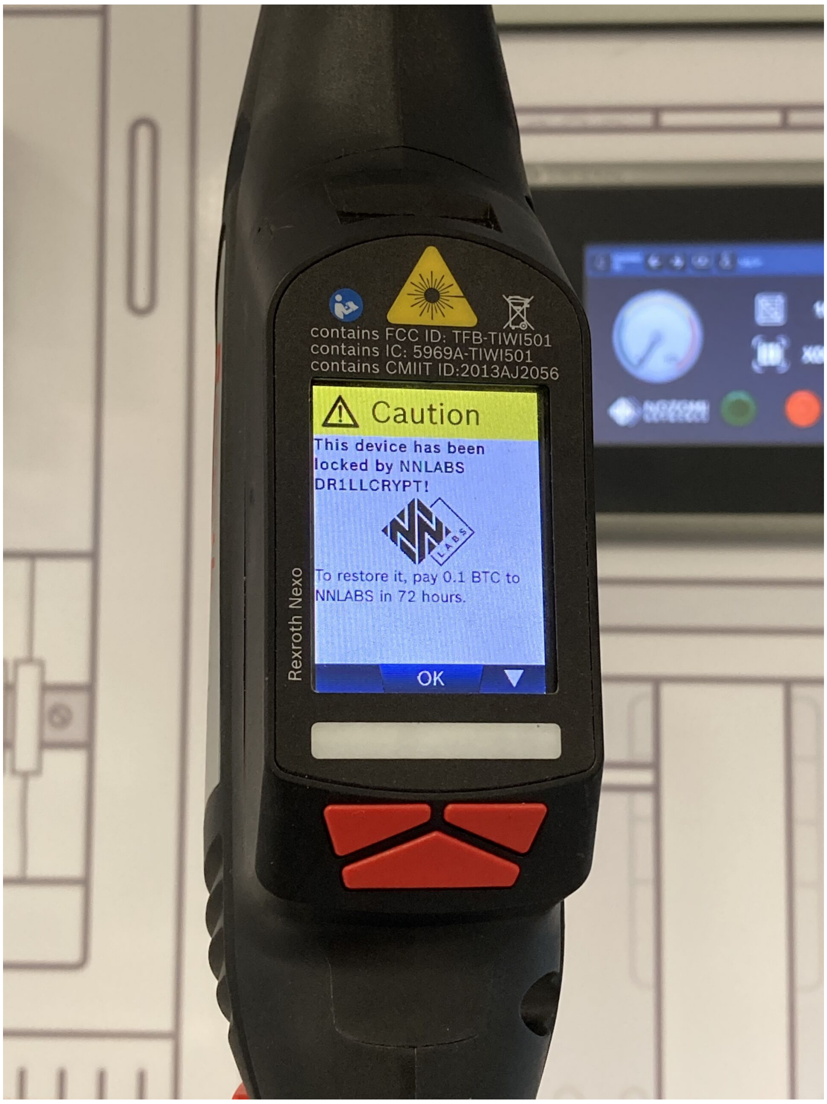
- Whaling - Phishing targeting high-profile targets such as executives within an organization, politicians or celebrities. Achieved by impersonating another high-profile individual such as a senior executive.

- Pharming - Pharming involves sending a link to a fake website that appears to be official, then storing any personal information the victims enter.

3.2 Distribution of Malware

E-mails can convey attachments as well as text, which open another vector for attack through e-mails. E-mails are a common way of distributing malicious programs which can be categorized as follows [19]:

- Spyware - Software that allows the attacker to obtain information about activities performed on the affected device.
- Ransomware - Software that disables the victim's access to data or device until a ransom is paid.



Caution

This device has been locked by NNLABS DR1LLCRYPT!

To restore it, pay 0.1 BTC to NNLABS in 72 hours.

contains FCC ID: TFB-TIWI501
contains IC: 5969A-TIWI501
contains CMIIT ID:2013AJ2056
LABS
OK
Rexroth Nexo

Figure 3.1: A network-connected Bosch Rexroth torque wrench, infected with ransomware while testing vulnerabilities
Source: https://arstechnica.com/security/2024/01/network-connected-wrenches-used-in-factories-can-be-hacked-for-sabotage-or-ransomware/

- Trojan - Named after the Trojan Horse, a trojan is a malicious program disguised as a desirable piece of software. Often embedded in attachments in e-mails, or in illegally downloaded programs.

- Virus - Similar to a trojan, a virus injects itself into and application or code and runs when the application is run to perform malicious actions.
- Rootkits - Gives malicious actors remote control of a victims device with full privileges.
- Bots and Botnets - Adds the users device to a botnet, wherein the device becomes slaved to a master device, from which it can be activated and used to launch remote-controlled flood attacks.

3.3 E-mail spoofing

E-mail spoofing is the act of tricking a victim into thinking an e-mail came from a trusted source instead of the attacker by modifying the e-mail headers to show a different sender address than the attackers own. This is commonly done alongside a phishing or malware distribution attack to increase the effectiveness of said attack, however spoofing can be used irrespective of malware distribution and credential theft such as with Business E-mail Compromise (BEC), which is the act of impersonating a high-ranking member or trusted partner of a business, usually in an attempt to trick employees into transferring money or revealing confidential business information.

4 Spoofing Emails

E-mail spoofing is defined as the creation of e-mails with a forged sender address [20]. In other words, an email sent by "badGuy@suspiciousSite.com" can be forged to appear in the inbox as having been sent by "goodGuy@trustedSite.com". E-mail spoofing opens the gateways for myriad e-mail based scams and crimes, including phishing, spearphishing, spreading of hoaxes among others. The bad news is that spoofing e-mails is surprisingly easy, however the good news is that most of the time, a spoofed email can be easily detected by most e-mail servers and clients.

4.1 Why is e-mail spoofing possible

There are multiple reasons e-mail spoofing is possible even to this day. The primary reason is how e-mail systems are designed. The client application sets the sender address for outgoing messages, therefore spoofing is done client-side and the outgoing e-mail servers cannot identify whether the address is legitimate or spoofed. Another reason is in the way SMTP was designed. SMTP was designed to be simple and easy to use, and as a result also easily manipulated. SMTP contains multiple header fields, FROM, TO, REPLY-FROM and so on, and to spoof an e-mail in the simplest form requires modification of the FROM field[21].

4.2 Dangers of e-mail spoofing

Hopefully the dangers of spoofed e-mails are already apparent but if not here are some possible cases that could arise out of a spoofed e-mail:

- Slander and impersonation through spoofing an individuals or business e-mail
- Malware distribution - Sending malware links by spoofing a trusted e-mail

- Misinformation - Impersonating government or other authorities
- Phishing - Links to false websites used to intercept login credentials or trick users into revealing sensitive information
- disguising the origin of spam

4.3 Spoofing and Phishing

It is important to distinguish between spoofing and phishing. Spoofing is the act of forging the address of the sender. Phishing is the act of stealing information, through various tricks designed to trick a person into giving up their information willingly. While spoofing is used to increase the effectiveness of a phishing attack, phishing attacks do not necessarily come from a spoofed e-mail. Legally, spoofing is not considered fraud, as the e-mail is not stolen but rather imitated. Phishing is considered fraud as it is considered information theft [22].

4.4 E-mail spoofing history and incidents

E-mail spoofing has been an issue since 1970. From 1970 to the year 2000 there were not robust authentication mechanisms in place, and SMTP lacked any security protocols, so spammers spoofed their e-mails to get around e-mail filters[21]. In the year 2000, SPF (sender policy framework) was introduced[23], which allowed domain owners to specify which mail servers were authorized to send e-mails on behalf of their domain. This reduced the effectiveness of e-mail forgery by allowing the receiving e-mail server to check the authenticity of the senders domain.

In 2004, DomainKeys was introduced by Yahoo! as an e-mail authentication method that verified the sending domain and body of an e-mail using a public and private key. Identified Internet Mail by CISCO was created to offer a means of applying cryptographic signatures to e-mail messages for verification purposes, first draft published in 2005. In 2007 Yahoo! and CISCO decided to merge these two technologies into a single security protocol, which was later published in 2011 under the name of DKIM (DomainKeys Identified Mail) which allowed senders to digitally sign an e-mail. This allowed the receiving mail server to verify the signature using the public key available in the sender's

DNS records.[24]
DMARC was introduced in 2012. DMARC built off of SPF and DKIM to provide a more comprehensive e-mail authentication solution. It enabled domain owners to specify how their e-mail should be handled in the case of a failed SPF or DKIM inspection. This provided another barrier for e-mail spoofing while also providing another way for legitimate senders to authenticate their e-mails.[25]
To this day spoofing is still an issue, and as with all aspects of cybersecurity, organizations and e-mail service providers continually update their security measures to keep up with evolving spoofing techniques as attackers continue to find ways to bypass the existing security measures.

4.4.1 Famous examples of e-mail attacks

- The Nordea Bank Incident (2007) - In 2007 Sweden's Nordea Bank lost $1.1 million to a trojan that was distributed by e-mail to their customers. The trojan "was masquerading as anti-virus software and was downloaded by Nordea's customers on the recommendation of emails that claimed to come from the bank." [26]

- Operation "Phish Phry" (2009) - In 2009 the FBI caught around 100 American and Egyptian individuals and charged them with "crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identify theft" [27]. after stealing $1.5 million from various banks by transferring using stolen credentials.

- The Sony Pictures Leak (2014) - In 2014 over 100 terrabytes of confidential company information was leaked from Sony resulting in $100 million in damages. The attackers pretended to be colleagues of top-level Sony employees who opened malicious attachments causing the leak[28].

These are but a few examples of famous attempts which succeeded. There are many scams and attacks which go unreported on a daily basis, and the attacks are not limited to banks and major companies.

5 Example of spoofing

This is an example of using Kali Linux "sendemail" function to spoof an e-mail. For this experiment three e-mails were used:

- thesissendertest@outlook.com - the original sender of the e-mails, referred to from this point onwards as "the sender"
- thesisreceivertest@outlook.com - the primary receiver of e-mails from the sender, henceforth referred to as "the receiver"
- a private Gmail account used for testing various cases such as forwarding, referred to as "V.M."

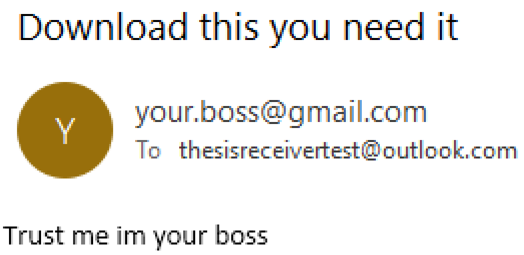
The following command was used to send e-mails from the Kali Linux terminal:

```
sendemail -xu thesissendertest@outlook.com -xp pass
-s smtp-relay.brevo.com:587
-f "your.boss@gmail.com"
-t "thesisreceivertest@outlook.com"
-u "Download this you need it"
-m "Trust me im your boss" -o tls=no
```

the flags mean the following:

- -xu - USERNAME for SMTP authentication
- -xp - PASSWORD for authentication
- -s - server and port for mail relay

- -f - sets the FROM header
- -t - TO address
- -u - message subject
- -m - message body
- -o - advanced option, in this case disabling TLS



Download this you need it

Y

your.boss@gmail.com

To thesisreceivertest@outlook.com

Trust me im your boss

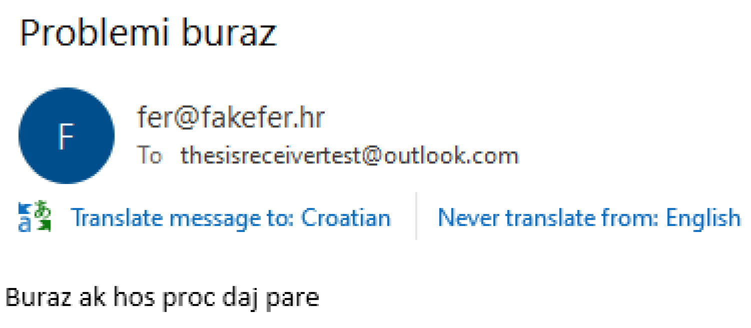
Figure 5.1: How the "yourboss" e-mail is shown in outlook

As demonstrated, the e-mail from the sender showed up in the receiver's inbox as being sent from "yourboss@gmail.com", albeit in the spam folder. Digging through the internet headers for this e-mail gives the following results:

```
From: <your.boss@gmail.com>
To: <thesisreceivertest@outlook.com>
Subject: Download this you need it
Authentication-Results: spf=pass (sender IP is 77.32.148.22)
smtp.mailfrom=gu.d.sender-sib.com; dkim=pass (signature was verified)
header.d=gu.d.sender-sib.com;dmarc=fail action=none
header.from=gmail.com;compauth=fail reason=001
Received-SPF: Pass (protection.outlook.com: domain of gu.d.sender-sib.com
designates 77.32.148.22 as permitted sender) receiver=protection.outlook.com;
client-ip=77.32.148.22; helo=gu.d.sender-sib.com; pr=C
```

Interestingly, the spoofed e-mail passed both SPF and DKIM checks, but failed the DMARC check with "reason=001". Reason "001" means a failed implicit authentication step of the composite authentication process[29], which is defined as "an extension of regular email authentication policies. These extensions include: sender reputation, sender history, recipient history, behavioral analysis, and other advanced techniques."[30]

Another example:



Problemi buraz

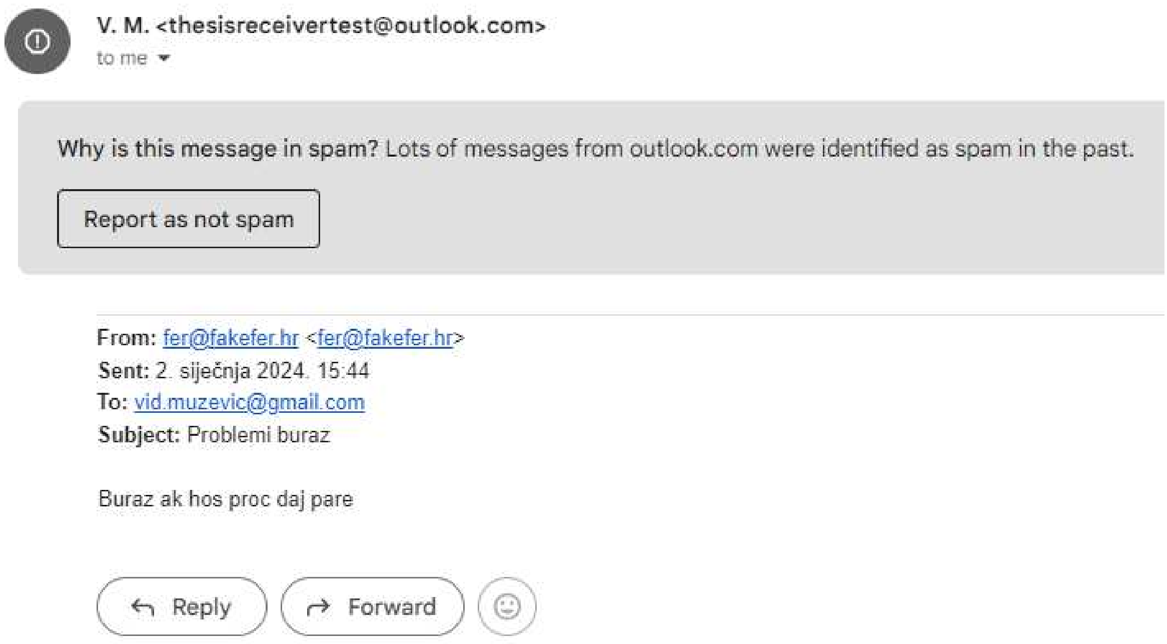
fer@fakefer.hr

To thesisreceivertest@outlook.com

Buraz ak hos proc daj pare

Figure 5.2: How the "fakefer" e-mail is shown in outlook

The headers of this e-mail are practically identical to those from the "your.boss" e-mail shown above so will not be repeated. These are very banal and obviously false spoofed e-mails. A rule was set where the receiver would automatically forward any e-mails to V.M.:



V. M. <thesisreceivertest@outlook.com>

to me

Why is this message in spam? Lots of messages from outlook.com were identified as spam in the past.

From: fer@fakefer.hr <fer@fakefer.hr>
Sent: 2. siječnja 2024. 15:44
To: vid.muzevic@gmail.com
Subject: Problemi buraz

Buraz ak hos proc daj pare

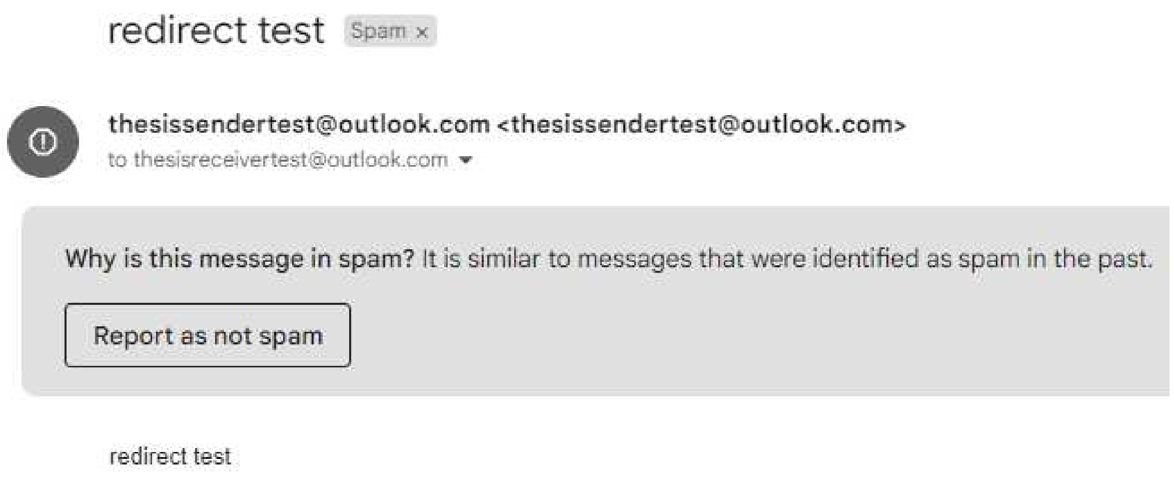
Figure 5.3: How the "fakefer" e-mail is shown in gmail

Resulting in the following headers as seen through the Gmail web application:

```
From: "V. M." <thesisreceivertest@outlook.com>
To: "vid.muzevic@gmail.com" <vid.muzevic@gmail.com>
Subject: FW: Problemi buraz
ARC-Authentication-Results: i=2; mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1 header.b=BVvKJFPs;
arc=pass (i=1);
spf=pass (google.com: domain of thesisreceivertest@outlook.com designates
2a01:111:f400:fe0c::813 as permitted sender)
smtp.mailfrom=thesisreceivertest@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
```

As is shown, the forwarded message is shown as having come from the receiver. However, the message body does not include the senders original address, rather it shows the spoofed address. In this case all authentication checks pass, which is to be expected as this e-mail has been sent from the receiver e-mail which was not spoofed. Curiously, searching for the message body yielded no results. Another important thing to note is the subdomain policy "sp=QUARANTINE". This will be referred to in the next example.

When the rule was changed from "forward" to "redirect" the following occurred:



redirect test

thesissendertest@outlook.com <thesissendertest@outlook.com>
to thesisreceivertest@outlook.com

Why is this message in spam? It is similar to messages that were identified as spam in the past.

redirect test

Figure 5.4: How a redirected e-mail is shown in gmail

```
From: "thesissendertest@outlook.com" <thesissendertest@outlook.com>
To: "thesisreceivertest@outlook.com" <thesisreceivertest@outlook.com>
Subject: redirect test
ARC-Authentication-Results: i=2; mx.google.com;
dkim=pass header.i=@outlook.com header.s=selector1 header.b=MpAvK15l;
dkim=neutral (body hash did not verify) header.i=@gv.d.sender-sib.com
header.s=mail header.b=1L7BOByo;
arc=pass (i=1);
spf=pass (google.com: domain of thesisreceivertest@outlook.com designates
2a01:111:f403:2e0f::801 as permitted sender)
smtp.mailfrom=thesisreceivertest@outlook.com;
dmarc=pass (p=NONE sp=QUARANTINE dis=NONE) header.from=outlook.com
```

In this case the e-mail is shown as having been sent from the sender's address as this e-mail was not spoofed, and all checks passed without issue. However it does not show as having been intended for V.M., rather that it was sent to the receiver.

When attempting to send a spoofed e-mail to receiver and have the receiver's redirect rule send it to V.M., the e-mail was not delivered. It can only be assumed that the e-mail failed the DMARC check and was quarantined before reaching the inbox.

6 Mitigating Risks and Conclusion

E-mail being so widespread in its use means that large overhauls to the way e-mail works is a gargantuan task to accomplish. When DMARC was published in 2012 it was adopted incredibly slowly, only attaining widespread use around 2015/2016 when Google and Yahoo! adopted strict DMARC policies, warning businesses that did not follow the DMARC trend that their business would suffer for it [31]. In fact Google plans to force domain owners who send bulk messages to Gmail addresses to authenticate their e-mails with DMARC in February, 2024 [32], a full 12 years after the creation of DMARC. Some businesses use e-mail hosting services for their business e-mail needs, but some businesses also host their own, which is why e-mail security protocols are so slow to adopt. Those that host their own servers also have to manually implement security protocols, which become more technical as security systems become more complex. In the case of DMARC, organizations had to implement SPF and DKIM before they could even begin implementing DMARC, which requires a lot of technical knowledge to implement [25].

6.1 Mitigating risks on personal e-mail accounts

Most of this work has been centered around the use of e-mail in business, as businesses are the large targets which stand to be most profitable to would-be attackers. This doesn't mean the average person is safe from similar attacks through their personal e-mail account. On a more personal level, the following can be done to alleviate the chances of falling victim to such attacks:

- Use a secure e-mail service provider - It is difficult to accurately define which e-mail service provider is most secure and least invasive in terms of privacy due to the nature of advertising, it is preferable to choose an e-mail service provider that has implemented most if not all of the security protocols mentioned in this thesis.

Thoroughly researching alternative e-mail service providers is recommended.

- Limit the amount of sensitive information sent via e-mail - sometimes situations arise where it's necessary to send sensitive information via e-mail as in the case of emergencies. However, as with all things, one must be mindful of what they are sending through any method of communication, not only because of possible attackers, but also because some e-mail service providers actively collect information about their users, and in the case of Gmail, their systems collect information from non-Gmail users when they send e-mails to Gmail users, quoting that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[33]" as per the United States legal doctrine named the Third-Party Doctrine[34].
- Minimise human error - always ensure that the contents of an e-mail are being sent to a person to whom it concerns. According to Tessian's 2022 Email Security Report "92% of organizations have dealt with a data breach caused by an end-user error on e-mail"[35]. As businesses protect their secrets and data, so too should one protect ones own data and secrets, ensuring they are being shared with those who are trustworthy or to whom the information is of concern.
- two-factor authentication and passwords - all the security protocols in existence will not be of help in the case of a compromised account. It is paramount that one protects their account from access by unwanted parties, most reliably done through an authentication method known as two-factor authentication.
- antivirus programs - if all else fails and a harmful e-mail does get past all security protocols and tricks a user into opening its malicious attachment, an antivirus program could potentially stop and quarantine the attachment before it is able to do damage.

6.2 Mitigating risks on business e-mails

A lot of what has been said about private e-mails can also be said for business e-mail security. Here is some additional advice:

- Employee training - it is imperative that all employees are aware of the risks of e-mails. Ensure all employee business-related devices are running an antivirus and are using two-factor authentication. Remind employees to double and triple-check each e-mail they send out and that they will be held responsible for data leaks even if by accident.

- backups - backup files to an external hard drive regularly. In the case of a ransomware attack or other attack involving the deletion of files, the backup will help recover most if not all of the lost files.

- gateway e-mail content filters - gateway e-mail content filters intercept incoming messages, check them for malicious or suspicious content, and then decides whether to quarantine or deliver the e-mail. This blocks spam and malware before it reaches the users' inboxes.

Training employees in the basics of cybersecurity is the most important factor in mitigating risk, but in the end, all it takes is one gullible employee to click on a link for millions of dollars in damages. As such it is preferable if such employees never see the e-mail containing said link to begin with. Having a security team send out a "safe" phishing e-mail to employees which logs who clicks on the link could be a valid strategy in determining which employees are a risk and need further training in the field of e-mail security.

References

[1] A. S. Gillis, *Internet of things (IoT)*, [last accessed: 2024-01-28]. [Online]. Available: https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT

[2] E. Sayegh, *Reflecting On The Evolution Of Cybersecurity In 2023*, 2023, [last accessed: 2024-01-28]. [Online]. Available: https://www.forbes.com/sites/emilsayegh/2023/12/12/reflecting-on-the-evolution-of-cybersecurity-in-2023/?sh=1f0dd0ba47e7

[3] I. D. Foster, J. Larson, M. Masich, A. C. Snoeren, S. Savage, and K. Levchenko, "Security by any other name: On the effectiveness of provider based email security," in *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security*, 2015, pp. 450–464.

[4] S. Furnell and P. Dowland, *E-mail Security*. It Governance Pub, 2010.

[5] *Information Assurance(IA): definition explanation*, [last accessed: 2024-01-28]. [Online]. Available: https://www.itgovernanceusa.com/information/information-assurance

[6] *The 5 Pillars Of Information Security And How To Manage Them*, 2018, [last accessed: 2024-01-28]. [Online]. Available: https://resourcecenter.infinit-o.com/blog/the-5-pillars-of-information-security-and-how-to-manage-them/

[7] M. Christen, B. Gordijn, and M. Loi, *The ethics of cybersecurity*. Springer Nature, 2020.

[8] (2019) The cybersecurity act. [Last accessed: 2024-02-05]. [Online]. Available: https://www.dutchncca.nl/the-cybersecurityact

[9] D. B. Resnik and P. R. Finn, “Ethics and phishing experiments,” *Science and engineering ethics*, vol. 24, pp. 1241–1252, 2018.

[10] K. Macnish and J. Van der Ham, “Ethics in cybersecurity research and practice,” *Technology in society*, vol. 63, p. 101382, 2020.

[11] A. Rudra, *What is a TLS Handshake?*, 2023, [last accessed: 2024-01-29]. [Online]. Available: https://powerdmarc.com/what-is-a-tls-handshake/

[12] J. Griffin, *What is StartTLS?*, 2023, [last accessed: 2024-01-29]. [Online]. Available: https://sendgrid.com/en-us/blog/what-is-starttls

[13] An spf record example to help you understand the working of sender policy framework. [Last accessed:2024-02-09]. [Online]. Available: https://www.duocircle.com/content/spf-records/spf-record-example

[14] Your guide to safe emails: Create and implement a dkim record. [Last accessed:2024-02-09]. [Online]. Available: https://mailtrap.io/blog/create-dkim-tutorial/

[15] What is a dmarc dns record? [Last accessed:2024-02-09]. [Online]. Available: https://mxtoolbox.com/dmarc/details/what-is-a-dmarc-record

[16] O. o. i. s. Leadership for IT security privacy across HHS, HHS Cybersecurity program, *SSL/TLS Vulnerabilities*, 2021, [last accessed: 2024-01-29]. [Online]. Available: https://www.hhs.gov/sites/default/files/securing-ssl-tls-in-healthcare-tlpwhite.pdf

[17] B. Kiprin, *What Is the SSL BEAST Attack and How Does It Work*, 2021, [last accessed: 2024-01-29]. [Online]. Available: https://crashtest-security.com/ssl-beast-attack-tls/

[18] *WHAT IS VISHING?*, [last accessed: 2024-01-30]. [Online]. Available: https://terranovasecurity.com/what-is-vishing/

[19] K. Baker, *THE 12 MOST COMMON TYPES OF MALWARE*, 2023, [last accessed: 2024-01-30]. [Online]. Available: https://www.crowdstrike.com/cybersecurity-

101/malware/types-of-malware/

[20] G. Varshney, M. Misra, and P. K. Atrey, “A survey and classification of web phishing detection schemes,” *Security and Communication Networks*, vol. 9, no. 18, pp. 6266–6284, 2016. https://doi.org/https://doi.org/10.1002/sec.1674

[21] *What Is Email Spoofing?*, [last accessed: 2024-01-31]. [Online]. Available: https://www.proofpoint.com/us/threat-reference/email-spoofing#:~:text=Email%20spoofing%20is%20possible%20due,detect%20and%20filter%20spoofed%20messages

[22] B. Lenaerts-Bergmans, *UNDERSTANDING THE DIFFERENCE BETWEEN SPOOFING VS PHISHING*, 2023, [last accessed: 2024-01-31]. [Online]. Available: https://www.crowdstrike.com/cybersecurity-101/attack-types/spoofing-vs-phishing/

[23] (2023) What is spf email? [Last accessed: 2024-02-06]. [Online]. Available: https://powerdmarc.com/what-is-spf/#:~:text=SPF%20stands%20for%20Sender%20Policy,which%20is%3A%20Sender%20Policy%20Framework.

[24] (2022) What is dkim? - a bit of history. [Last accessed: 2024-02-06]. [Online]. Available: https://easydmarc.com/blog/what-is-dkim-a-bit-of-history/

[25] (2022) What is dkarc? - a bit of history. [Last accessed: 2024-02-06]. [Online]. Available: https://easydmarc.com/blog/what-is-dmarc-a-bit-of-history/

[26] (2007) Nordea loses $1.1 million to online fraud. [Last accessed: 2024-01-31]. [Online]. Available: https://www.nsbanking.com/news/nordea_loses_1_1_million_to_online_fraud1639300460/

[27] (2009) Operation phish phry, major cyber fraud takedown. [Last accessed: 2024-02-01]. [Online]. Available: https://archives.fbi.gov/archives/news/stories/2009/october/phishphry_100709

[28] Famous phishing incidents from history. [Last accessed: 2024-02-06]. [Online]. Available: https://www.hempsteadny.gov/635/Famous-Phishing-Incidents-from-History

[29] (2023) Anti-spoofing protection in eop. [Last accessed:2024-02-07]. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-spoofing-about?view=o365-worldwide

[30] (2023) Email authentication in eop. [Last accessed:2024-02-07]. [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/email-authentication-about?view=o365-worldwide

[31] (2015) Global mailbox providers deploying dmarc to protect users. [Last accessed: 2024-02-06]. [Online]. Available: https://dmarc.org/2015/10/global-mailbox-providers-deploying-dmarc-to-protect-users/

[32] (2023) New gmail protections for a safer, less spammy inbox. [Last accessed: 2024-02-06]. [Online]. Available: https://blog.google/products/gmail/gmail-security-authentication-spam-protection/

[33] (1979) Smith v. maryland, 442 u.s. 735 (1979). [Last accessed: 2024-02-06]. [Online]. Available: https://supreme.justia.com/cases/federal/us/442/735/

[34] R. M. T. II, *The Fourth Amendment Third-Party Doctrine*, 2014, [last accessed: 2024-02-06]. [Online]. Available: https://sgp.fas.org/crs/misc/R43586.pdf

[35] (2022) State of email security 2022. [Last accessed: 2024-02-06]. [Online]. Available: https://www.tessian.com/resources/state-of-email-security-2022/

Abstract

E-mail security

Vid Mužević

Despite the fact that e-mail has existed for more than 50 years and the fact that many security protocols have been invented in that time, they are still prone to attacks. Some of the most popular attacks are spoofing and phishing and this thesis makes an attempt to prove how easy it is to conduct such attacks in order to show why it is important to improve e-mail security. This thesis lists protocols used for e-mail security, famous attacks, e-mail vulnerabilities and many more. Considering the complications involved in changing the entire infrastructure of e-mails for improved security, there are some precautions that can be taken, primarily the education of people and employees.

Keywords: E-mail;security;spoofing;phishing;

Sažetak

Sigurnost elektroničke pošte

Vid Mužević

Unatoč tome što elektronička pošta postoji preko pedeset godina i razni protokoli što su bili osmišljeni, elektronička pošta i dalje je sklona napadima. Najpopularniji napadi su *spoofing* i *phishing* te ovaj rad ukazuje na to kako ih je jednostavno provesti. Upravo time se dokazuje kako je bitno poboljšati sigurnost elektroničke pošte. Ovaj rad nabraja razne protokole korištene u svrhu sigurnosti elektroniče pošte, neke od poznatih napada, ranjivosti i mnoge druge stavke. S obzirom na komplikacije koje bi bile tijekom izmjene cijele infrastrukture elektroničke pošte u svrhu sigurnosti, postoje neke predostrožnosti koje se mogu poduzeti do tada, a to je prvenstveno edukacija ljudi i edukacija zaposlje-nika u kompanijama.

Ključne riječi: Elektronička pošta;sigurnost;lažiranje;phishing;