European Commission

JRC TECHNICAL REPORTS

My Email Communications Security Assessment (MECSA): 2018 Results

Draper-Gil, Gerard

Sanchez, Ignacio

2019

Joint Research Centre

EUR 29674 EN

This publication is a Technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The scientific output expressed does not imply a policy position of the European Commission. Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use that might be made of this publication.

EU Science Hub
https://ec.europa.eu/jrc

JRC115217

EUR 29674 EN

PDF	ISBN 978-92-76-00256-7	ISSN 1831-9424	doi:10.2760/166203

Luxembourg: Publications Office of the European Union, 2019

How to cite this report: Sanchez Martin, J. and Draper Gil, G., My Email Communications Security Assessment (MECSA): 2018 Results, EUR 29674 EN, Publications Office of the European Union, Luxembourg, 2019, ISBN 978-92-76-00256-7 (online), doi:10.2760/166203 (online), JRC115217.

Executive Summary

This JRC technical report presents the results obtained by the My Email Communications Security Assessment (MECSA) tool. MECSA is an online[1] tool developed by the Joint Research Centre to assess the security of email communications between email providers; Simple Mail Transfer Protocol [18] (SMTP) servers.

Email communications continue to be one of the most widespread forms of digital communications with thousands of millions of emails exchanged on a daily basis. It is estimated that 72% of the European population use email either in mobile phones, tablets or computers. It is the means of digital communication used by most Europeans on a daily basis[2].

The importance of the protection of these new forms of digital communications over Internet, including email, has been further highlighted in the latest policy initiatives of the Commission [31, 30]. Moreover, when personal data is exchanged over email, the General Data Protection Regulation [32] requires that appropriate technical and organisational measures are put in place to ensure the confidentiality and integrity of the relevant processing systems and services.

MECSA is the outcome of our research on the security of email communications. It servers a triple purpose. Firstly, it allows us to monitor the adoption of modern email security standards in the current ecosystem of email providers, assessing their capability to protect the confidentiality, integrity and authenticity of the email exchange amongst them. Secondly, MECSA aims to become a one-stop shop for email users to receive an indication of the capability of their email providers to protect their email exchange in the communication with other providers of the ecosystem. Finally, MECSA aims to become a reference tool for professionals and a mean to promote the adoption of modern email security standards in Europe.

In 2018, MECSA carried out over 15.000 assessments, analysing a total of 4836[3] unique email providers. In this report, we present the methodology followed, statistics about the results obtained and a set of highlights and recommendations based on the research carried out on this topic.

The main highlights of this report are the following ones:

There are important gaps in the adoption of modern email communications security standards.

Only 25.66% of the email providers analysed by MECSA were found to have properly adopted the minimum set of modern email security standards recommended to ensure the confidentiality, integrity and authenticity of the communications. Out of this 25.66%, only 19.02% adopted all recommended email security standards.

26.72% of email providers did not adopt any email security standard to fight email spoofing and identity theft. Moreover, 12.30% of email providers did not employ any security standard to protect the confidentiality of the email exchange between email providers.

Furthermore, we found that in many cases email providers attempted to adopt security standards but failed to deploy them correctly. In particular, more than 18.87% of the email providers analysed failed to deploy properly standards related to protecting the confidentiality. That figure raised to 32.32% for those standards related to the fight against email spoofing and identity theft.

[1] https://mecsa.jrc.ec.europa.eu

[2] Special Eurobarometer 462, 2017. Published July 2018.

[3] MECSA stats last checked 20/12/2018

There is a lack of incentives to adopt modern email security standards.

The adoption of email security standards is not mandatory. Email providers can achieve a degree of interoperability good enough to exchange emails with other providers, without supporting any security protocol. In this scenario, emails will be sent and received in plaintext (without encryption) and there will be no mechanisms to protect the integrity of emails or fight email identity theft. These email communications between email providers take place in a completely transparent way for end-users.

Unlike web users, who can rely on the padlock icon of the browser, email users lack indicators of the capability of email providers to protect their digital communications. Our experience with MECSA indicates that most users were unaware of the actual capability of their email provider to protect their email exchange.

As a result of this, there is currently a lack of incentives for email providers to adopt modern email security standards. This lack of incentives propagate along the supply chain. There is not always a big enough demand for email server software/appliance vendors to support these standards. As a result, many well-known email products (usually appliances and proprietary software) lack support for some of them.

The recommendations put forward in this report are the following ones:

Recommendation of a minimum set of email security standards to be adopted by service providers and development of technical guidelines.

A European recommendation on a set of modern email security standards to be supported by email providers would help to close existing gaps in their adoption. Public procurement of email server software/hardware products could refer to this recommendation when setting the mandatory functionalities and security requirements.

The development of technical guidelines and good practices for the deployment of email security standards would help to avoid common mistakes like missing certificate chains or syntax errors in the policies. This could be of particular importance in the case of SMEs that might lack the resources required to carry out the deployment of these standards.

Support on-going efforts to promote modern email security standards and incentivise their adoption.

The several on-going efforts to promote modern email security standards in Member States should be promoted. In this regards, we consider that MECSA is a valuable tool to contribute and complement these efforts.

Moreover, strategies to incentivise the adoption of email security standards should be considered. For example, the application of a security seal backed up by the objective assessment of the email security standards properly adopted by a given email provider, would help to boost end-user's trust and provide an incentive for manufacturers and service providers.

Contents

1 Introduction

With thousands of millions of emails exchanged on a daily basis, email is one of the most widespread forms of digital communications. In the current era of the digital society, email communications are massively used, not only to support inter-personal communications among citizens but also as a more traditional communication channel to complement the current ecosystem of online services, as shown in Figure 1 from the latest report on E-Communications and Digital Single Market [4] where 72% of the surveyed EU citizens answered they use email services.

Email is often used to transmit personal data, not only in citizen's personal communications, but also when used in e-government services or e-Health. Moreover, email addresses are massively used in the management of online digital identities, being email communications an integral part of online authentication systems (e.g. when used in a password recovery process). Effective mitigation of security and privacy risks in email communications is of paramount importance given the role that they play in the current digital society.

The importance of the protection of digital communications has been further highlighted in the latest policy initiatives [31, 30], where email communications are identified as one of the Over-The-Top services whose confidentiality shall be protected. In their recitals, the ePrivacy proposed regulation [31] highlight the importance of protecting the confidentiality of electronic communications following the fundamental right to privacy enshrined in Article 7 of the Charter of Fundamental Rights of the European Union [28].

Moreover, when personal data is exchanged over email, the General Data Protection Regulation EU 2016/679 [32] (GDPR) requires in its article 32 that appropriate technical and organizational measures shall be put in place to ensure the confidentiality and integrity of the relevant processing systems and services. Further, article 5 of the GDPR states than an appropriate level of the protection of the security (integrity and confidentiality) is a prerequisite for the processing of personal data.

This report presents the results of the MECSA project. MECSA is an online[1] tool developed by the Joint Research Centre to assess the security of email communications between email providers. MECSA

[1] https://mecsa.jrc.ec.europa.eu

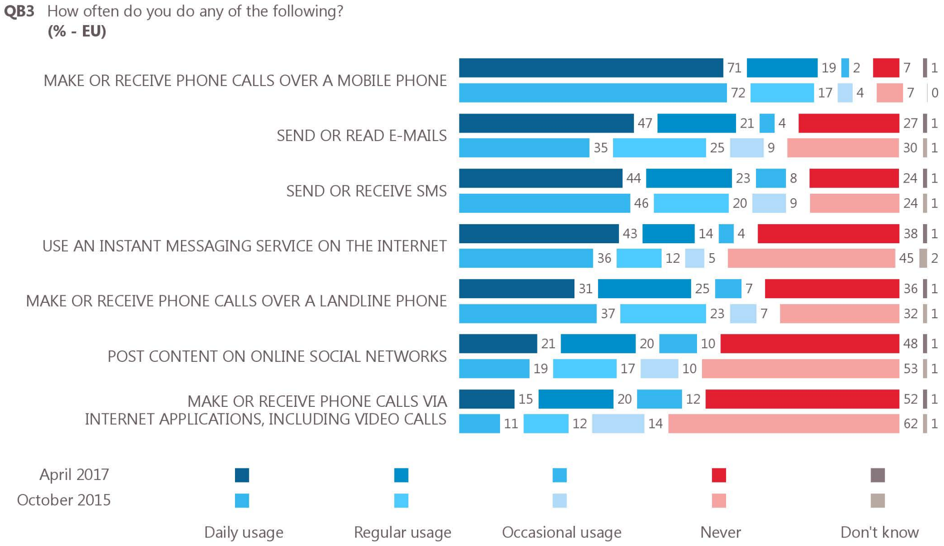

Figure 1: Experience using different communication services. Source: Special Eurobarometer 462

was launched to survey the security of email communications between providers.

The development of the MECSA platform has 3 main objectives. Its first objective is to provide us with a general overview on the state of security of email communications between providers. Its second objective focuses on the non-technical users of email, for whom MECSA aims to be a point of reference to raise awareness on the importance of email security, and offer them a one-stop shop where they can check the security offered by their email providers. Its third objective targets technical users, including administrators of email services, offering them a comprehensive report with details on which security measures their email provider supports and which ones it does not support.

The results presented in this report are the continuation of a previous work developed in the JRC by Sanchez *et al.* [16] and Malatras *et al.* [22] where we analyzed the vulnerabilities of the modern email services, and we reviewed the existing security standards in order identify which ones could be used to mitigate the vulnerabilities detected.

Previous work in this area is limited. Durumeric *et al.* [9] presented an empirical analysis of StartTLS, Sender Policy Framework [17, 19] (SPF), Domain-based Message Authentication, Reporting and Conformance [20] (DMARC) and DomainKeys Identified Mail [7] (DKIM) using a dataset from Google logs and the Alexa list of top 1M ranked websites. Even though in their paper they also present a study on Domain Name System (DNS) Hijacking, they do not mention neither DANE nor Domain Name System Security Extensions [2, 13, 34] (DNSSEC), a standard that would help to prevent such attacks.

Comparing with their results on the Google dataset, it seems that StartTLS support has improved. They reported that 58% of domains support StartTLS on all their communications with Google, which is 11% less than our results where all MTAs have StartTLS support with valid x509 certificates. This value is also similar in the tests on the Top 1M Alexa, where 82% of domains support StartTLS (87% in the MECSA results), but the percentage of domains with StartTLS properly configured increased from the 35% reported in Durumeric *et al.* [9] to a 69% in the MECSA assessments. The results for SPF, DKIM and DMARC based on the Google dataset are presented as % of emails sent/received, which we cannot compare with our results, presented as % of domains. But for the Top 1M Alexa websites, Durumeric *et al.* [9] report 47% of support for SPF and only 1.1% for DMARC. In these two standards our results present a notable increase, from 47% to 63% in SPF support, and from 1.1% to 44% in DMARC support.

Chung *et al.* [3] presented a comprehensive study on the deployment of DNSSEC. According to their best estimates, only 1% of domains supported DNSSEC in 2017. In our assessment we found that 10% of domains have DNSSEC enabled, and almost all of them, 9%, have their email service protected with DNS-based Authentication of Named Entities [14, 11, 8] (DANE).

The rest of the report is organized as follows. In Section 2 we briefly describe the email ecosystem, we highlight its main vulnerabilities and we present a list of modern email security standards that can be used to mitigate these vulnerabilities. In Section 3 we introduce the methodology used by the MECSA platform to assess the security of email communications. The results obtained during the 2018 campaign are presented in Section 4. Finally, in Section 5 we present our conclusions and recommendations.

2 Security in Email Communications: history, evolution and challenges

From an architectural point of view (see Figure 2), Modern email does not differ that much from traditional mail (post mail). In modern email, we have email users and email servers, whereas in the post mail we have mail users and post offices. Moreover, the process flow to deliver messages is basically the same. In the modern email, the messages sent go to the email server of the sender, from the sender's email server to the recipient's email server (provider-to-provider email communications), and finally to the recipient's inbox. On the other hand, in the post mail, the letters sent go to the sender's post office, from the sender's post office to the recipient's post office, and finally to the recipient's mailbox. Email services are built over a set of three well know standards: Simple Mail Transfer Protocol [18] (SMTP), Post Office Protocol - Version 3 [26] (POP3) and Internet Message Access Protocol [6] (IMAP). These standards were originally designed under the assumption that its users and the communications channels used were trusted. In reality, none of these assumptions holds true. Rogue Email Servers are usually behind spam and/or phishing campaigns, where they deliver millions of emails spoofing the identity of the sender. Furthermore, a malicious user can easily hijack the communication channel to redirect traffic, to block it, or to read everything sent and received, without leaving any trace. Since Mail Servers and communication channels were considered trusted, in the initial design of the core protocols that support email services (SMTP, POP3, IMAP), no previsions were made to protect the messages or to validate the identity of senders and recipients.

2.1 Email vulnerabilities

The original development of the core email protocols and the lack of adoption of new standards developed to secure email communications renders email communications vulnerable to various malicious attacks. Figure 3 represent different types of attacks that can target email communications. We have analysed the vulnerabilities of email communications and we have classified them in three groups, depending of the properties affected: confidentiality (Section 2.1.1), identity (Section 2.1.2) and integrity (Section 2.1.3).

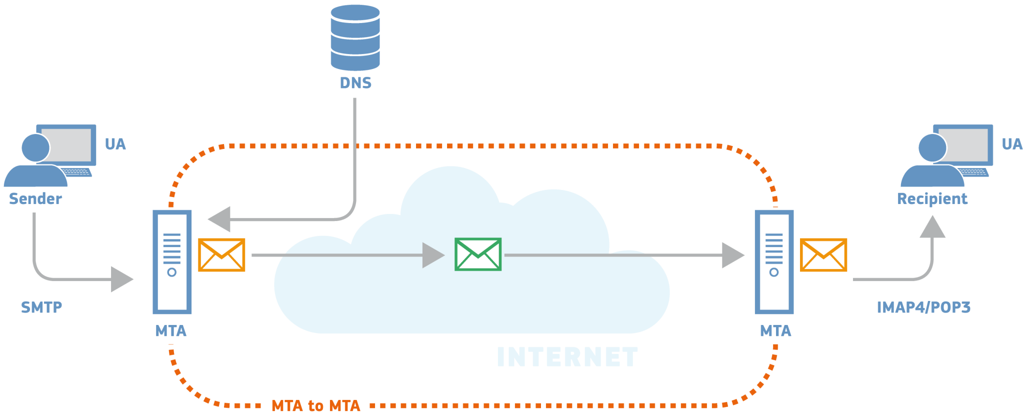

Figure 2: Email Architecture

2.1.1 Confidentiality

Without a secure communication channel, a malicious user could eavesdrop the communications between email servers. There are different ways in which an attacker could achieve this objective, such as passively monitoring data as it flows through intermediate routers or communication links, or performing a Man-In-The-Middle (MITM) attack at network level to change the flow of communications to his/her advantage and be able to monitor the communication. An example of this scenario would be the abuse of the Border Gateway Protocol [21] (BGP) to change the routing of IP packets effectively creating a network level MITM attack [27]. Such an attack vector is also known as BGP hijacking.

2.1.2 Identity

The protocol implicitly trusts the identity of the senders, assuming that all emails received are legitimate. This lack of authentication can be abused in order to spoof email identities, i.e. send emails pretending to be someone else. In order to carry out this attack, the malicious sender does not require tampering with the network communications of a legitimate server, which simplifies its execution.

Phishing is one of the malicious techniques that can take advantage of spoofed identities to carry out attacks, e.g. posing as the IT department of a bank, social network, online retailer, etc. and requesting the victim to log in to his account using a link provided in the email.

2.1.3 Integrity

Another consequence of not having a secure communication channel is the lack of integrity protection; we do not have the means to assure that the message received is the same one that was sent. An attacker has several options to execute this type of attack. One of them is to manipulate the email while it is in transit. In this case, the attack would leave almost no trace at SMTP level, therefore making it impossible to detect at the user side. Going a step further, an attacker could manipulate the traffic to receive the outbound connection of the sender Mail Transfer Agent (MTA), impersonating the identity of the legitimate recipient's MTA. The attacker can employ several means to achieve that, such as mounting a network-based attack. One effective way to perform such an attack would be the abuse of

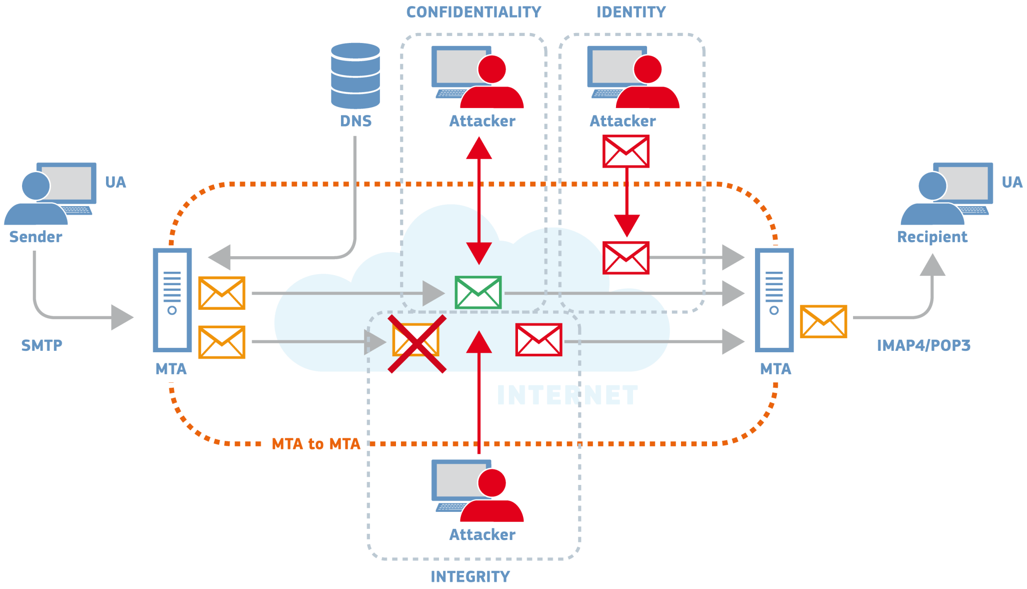

Figure 3: Email Communications Vulnerabilities

the DNS protocol [26].

A typical abuse of this vulnerability would be adding malicious content to emails (infected files), with the objective to spread a virus infection.

2.2 Modern security protocols

Since the initial development of the core email protocols (SMTP, POP3 and IMAP), different proposals for new protocols and/or extensions of previous ones have appeared to address email vulnerabilities (section 2.1). In a previous work developed at the JRC E.3 unit [16, 22], we have identified a set of modern security protocols that can help to mitigate the vulnerabilities of email services presented in the previous Section.

StartTLS [12, 25] is an extension of the SMTP protocol that allows the use of TLS in communications between SMTP clients and servers. Using StartTLS, client and server can create an encrypted channel to exchange SMTP messages, effectively protecting the communication from eavesdroppers. StartTLS is an efficient measure to mitigate the attacks on confidentiality of communications between MTAs.

An ***x509*** [1, 33, 5, 35] certificate is a standard description of public key certificates. The format of the certificate is established in the RFC 5280 [5], the ways to access it and to process it are defined in the RFC 4210 [1], and the RFC 3739 [33] defines what it calls a "Qualified Certificate" which is related to the European Directive on Electronic Signature (Directive 1999/93/EC [29]). An x509 certificate can be used for the following two main purposes.

- To verify the identity of the subject (e.g. a website) that owns the certificate, in such a way that you can be sure that the subject is really who it says to be. The URL of the website must match either the Common Name (CN) value in the Subject field, or the Subject Alternative Names (SAN).
- To send encrypted data that only the owner of the certificate will be able to decrypt (and read).

In the context of SMTP communications, x509 certificates are used to validate the identity of SMTP servers, during the TLS negotiation. Optionally, it can also be used to validate the identity of the client.

The use of certificates increases the trust in SMTP communications, the client can validate the identity of the server. The proper use of x509 certificates is an effective measure to protect the confidentiality of the communications, and to some extent the integrity (when communicating directly from sender to recipient).

Sender Policy Framework [17, 19] (SPF) is a protocol that allows email providers to announce a list of hosts authorized to deliver emails on its behalf. SPF records are published as TXT type records in the DNS of the email provider.

The SPF protocol is an effective measure to avoid the delivery of messages from illegitimate sources, fighting against phishing and identity theft. It helps recipients to identify messages sent from rogue hosts or networks. The application of the SPF protocol is an effective measure to mitigate the risk of identity spoofing (phishing and identity theft).

DomainKeys Identified Mail [7] (DKIM) is a standard that allows a recipient to validate the origin and contents of an email. It uses digital signatures to bind an email message with its origin. An email provider supporting DKIM has one or more private keys, and their associated public keys published as DNS records with the url *<selector>._domainkey.<domain>*.

The application of DKIM ensures recipients that the messages received have not been manipulated, therefore it is an effective measure to mitigate the attacks against the integrity of messages.

Domain-based Message Authentication, Reporting and Conformance [20] (DMARC) is a mechanism by which an email provider can publish policies regarding SPF and DKIM : how to perform validation, what to do if validation fails (reject, quarantine, none), and how to report. It can also be used to define a policy of accepting/rejecting certain percentage of failed messages, allowing a gradual deployment of SPF and/or DKIM .

DMARC , along with SPF and/or DKIM , is an effective measure to fight against identity spoofing and message tampering.

Domain Name System Security Extensions [2, 13, 34] (DNSSEC) is a protocol used to authenticate the response messages of DNS servers. This mechanism is useful to prevent applications from using altered or forged DNS records. The protocol is able to authenticate a set of DNS records through the verification of a cryptographic signature associated.

The use of DNSSEC assures that DNS records are valid and have not been modified or tampered with, increasing the level of trust. DNSSEC can have a positive impact in all three scenarios described in Section 2.1.

DNS-based Authentication of Named Entities [14, 11, 8] (DANE) is a mechanism that binds x509 certificates (or public keys) to domain names. In combination with DNSSEC , it allows a service to generate its own certificates, without requiring the services of a trusted CA.

The use of DANE increases the level of trust as well as the security and privacy of the communications. Along with DNSSEC , it can be used to mitigate the attacks on confidentiality.

Emerging standards. Apart from the well-known existing standards, at the time this report has been written, the Using TLS in Applications (UTA) [15] Working Group of the Internet Engineering Task Force (IETF) is working on other drafts that will have a positive impact on the increase of security of email communications.

SMTP Strict Transport Security [24] (MTA-STS) is a mechanism to publish policy directives regarding the use of TLS connections and x509 certificate validation. It is developed as an alternative to the use of DANE + DNSSEC . MTA-STS will be an efficient measure to mitigate the attacks against the confidentiality of communications between MTAs.

SMTP TLS Reporting [23] describes a mechanism to report statistics and information related to the establishment of TLS communications between SMTP servers. This information can be helpful to deploy technologies like MTA-STS, as well as to detect problems caused by configuration errors, attacks, etc. It can be an efficient measure to mitigate the attacks against the confidentiality of communications between MTAs.

RequireTLS [10] is an SMTP service extension that allows SMTP clients to specify either if they want their emails to be delivered using TLS, all the way from the sender MTA to the final recipient MTA , or if they want to prioritize delivery, overriding protocols like DANE or MTA-STS if necessary.

3 Methodology

To evaluate the security of email communications between providers we have developed a set of non-intrusive tests, and we have integrated them into an online platform: My Email Communications Security Assessment[1] (MECSA) platform.

MECSA is a public service where users can request an assessment of their email provider. After submitting their email address, they will receive an email sent by the MECSA platform. To initiate the assessment, they have to reply to this email. Following a privacy by design approach, the email address received will be deleted from our database as soon as the assessment has finished, or after 24h without receiving a reply to the email sent.

The process to test an email provider is very simple. It only requires three steps:

1. The user submits his email address to the MECSA platform.
2. MECSA sends an email to the address submitted, requesting a reply to initiate the process. The user has to reply to start the assessment. If the user does not reply, the email address will be deleted from the MECSA database after 24h.
3. When MECSA receives the reply, it will initiate the assessment. Once it is finished, MECSA will send an email to the user with the report identifier, and it will delete the message received and the email address of the user.

This interaction with the user allows the MECSA platform to tests the security of email communications in both directions, i.e. given an email address, it analyses the security measures applied by the email provider when it receives emails (inbound), and when it delivers them (outbound). Moreover, it prevents abuse of the platform, requiring users to have a valid email account in the domain for which they request an assessment.

MECSA will check if the email security standards described in Section 2.2 are applied (StartTLS, x509, SPF, DKIM, DMARC, DANE and DNSSEC).

StartTLS is tested for each Mail Exchanger (MX) in the inbound (email reception) and for each email server in outbound (email delivery) directions. To evaluate the application of the x509 standards we follow a strict approach. We execute four different tests:

- Does a trusted Certificate Authority (CA) sign the certificate?
- Does the certificate validate the hostname we are connecting to (Full Qualified Domain Name, FQDN)?
- Is the certificate expired?
- Is the certificate revoked (we check the Revocation List, RCL)?

The assessment for the SPF standard has three steps. First, we check if there is a DNS SPF registry. Second, we use a python library (pyspf) to check the syntax of the SPF registry. Finally, we use the IP address of the sender, its hostname and the domain name of the email address to evaluate the compliance with the SPF record (pyspf). DKIM is evaluated by a python library (dkimpy), using the reply email received. The test on the application of DMARC checks for the existence of a DMARC record, and it does a syntax check on the record found (if any). DANE is validated per email server. It applies to the incoming servers of email providers, and we test it independently of the results on the DNSSEC test. The DNSSEC executed by the MECSA platform requires answering the following questions.

- Is the email domain protected by DNSSEC?

[1] https://mecsa.jrc.ec.europa.eu

Score	StartTLS	x509	SPF	DKIM	DMARC	DANE	DNSSEC
★★★★★	✓	-	-	-	-	✓	✓
★★★★⯪	✓	✓	-	-	-	✗	✓
★★★★⯪	✓	✓	-	-	-	✓	✗
★★★★☆	✓	✓	-	-	-	✗	✗
★★★⯪☆	✓	✗	-	-	-	✓	✗
★★★⯪☆	✓	✗	-	-	-	✗	✓
★★★☆☆	✓	✗	-	-	-	✗	✗
☆☆☆☆☆	✗	-	-	-	-	-	-

Table 3.1: Definition of Confidentiality Scores

- Are the TXT records of the email domain protected by DNSSEC?
- Are the Mail Exchange (MX) records of the email domain protected by DNSSEC?
- For each MX, is the MX domain protected by DNSSEC?
- Are the TXT records of the MX domain protected by DNSSEC?
- Are the TLSA records of the MX domain protected by DNSSEC?

The results of all tests are combined in a summary report, where we provide score in three different domains: confidential delivery (confidentiality), phishing and identity theft (identity) and integrity of messages (integrity):

- *Confidential Delivery*: This parameter focuses on the privacy of communications between MTAs. It measures the ability of establishing secure communication channels when receiving or delivering messages. It is related to the confidentiality attacks described in Section 2.1.1. In Table 3.1 we can see the correspondence between protocols supported and score obtained.
- *Phishing and Identity Theft*: This parameter focus on two aspects related to the authorship of email messages. On one hand, it measures the ability of identifying messages sent from unauthorized sources. On the other hand, it measures the ability of protecting its users from identity theft. It is related to the identity attacks described in Section 2.1.2. The correspondence between protocols supported and score obtained can be seen in Table 3.2.
- *Integrity of Messages*: This parameter focuses on the detection of modifications suffered by email messages when traveling from MTA to MTA. It is related to the integrity attacks described in Section 2.1.3. In Table 3.3 we can see the correspondence between the protocols supported and the score assigned.

In addition to the summary report, MECSA provides and advanced report that can be used by professional users (including email administrators) to learn more details on the results obtained.

Score	StartTLS	x509	SPF	DKIM	DMARC	DANE	DNSSEC
★★★★★	-	-	✓	✓	✓	-	✓
★★★★⯨	-	-	✓	✓	✓	-	✗
★★★★⯨	-	-	✓	✓	✗	-	✓
★★★★☆	-	-	✓	✗	✓	-	✓
★★★★☆	-	-	✗	✓	✓	-	✓
★★★★☆	-	-	✓	✗	✓	-	✗
★★★⯨☆	-	-	✗	✓	✓	-	✗
★★★⯨☆	-	-	✓	✓	✗	-	✗
★★★⯨☆	-	-	✗	✓	✗	-	✓
★★★⯨☆	-	-	✓	✗	✗	-	✓
★★★☆☆	-	-	✓	✗	✗	-	✗
★★★☆☆	-	-	✗	✓	✗	-	✓
★★⯨☆☆	-	-	✗	✓	✗	-	✗
★★⯨☆☆	-	-	✗	✗	✓	-	-
☆☆☆☆☆	-	-	✗	✗	✗	-	-

Table 3.2: Definition of Phishing and Identity Theft Scores

Score	StartTLS	x509	SPF	DKIM	DMARC	DANE	DNSSEC
★★★★★	-	-	-	✓	✓	-	✓
★★★★★	✓	✓	-	✓	✓	-	✗
★★★★☆	✓	✓	-	✓	✗	-	✓
★★★⯨☆	✗	-	-	✓	✓	-	✗
★★★⯨☆	✗	-	-	✓	✗	-	✓
★★★⯨☆	✓	-	-	✓	✗	-	✗
★★★⯨☆	✓	✗	-	✓	✗	-	✓
★★★⯨☆	✓	✗	-	✓	✓	-	✗
★★★⯨☆	✓	✓	-	✗	✓	-	✓
★★★☆☆	✗	-	-	✓	✗	-	✗
★★★☆☆	✓	✓	-	✗	✓	-	✗
★★⯨☆☆	✗	-	-	✗	✓	-	-
★★☆☆☆	✓	✓	-	✗	✗	-	-
★☆☆☆☆	✓	✗	-	✗	✗	-	-
☆☆☆☆☆	✗	-	-	✗	✗	-	-

Table 3.3: Definition of Integrity Scores

4 Results Obtained

As of today (December 2018), the MECSA platform has generated more than 14600 reports, from more than 4600 different email providers. Figure 4 summarizes these results on the three categories evaluated: confidentiality, identity and integrity. Only 25.66% of the domains analysed by MECSA support a minimum set of the recommended email security standards, i.e. they scored at least 3.5 stars in each of the three categories evaluated. Out of this 25.66%, only 19.02% adopted all of them.

Definitions and assumptions:

- Email Provider: An email provider is an entity responsible of providing email services to an end user, independently of the infrastructure it uses. In practice, it is the domain name of the email address.
- MECSA will assess a protocol as supported when it succeeds in, at least, 80% of the tests. As example, a provider with 2 MX servers that support StartTLS and 1 outbound server that sends emails in plain-text would succeed in of 66.6% of the StartTLS tests (not supported), therefore it would receive a score of 0 stars, according to table 3.1
- The categories are obtained querying the Fortiguard[1] web filter service, sending the domain name of the email provider.

Confidential Delivery
The results obtained with the MECSA platform show that 69% of the email providers tested do protect the confidentiality of the emails they send and receive (their user's email communications). Another 18.87% of email providers offer a minimum level of protection of the confidentiality of email communications, most of them failing to have either a valid certificate or a consistent support for the StartTLS standard (e.g. having support for sending emails but not for receiving them, or vice versa). The results presented in Figure 4 show that more than 12% of email providers do not protect the confidentiality of their user's email communications.

[1] https://fortiguard.com/webfilter

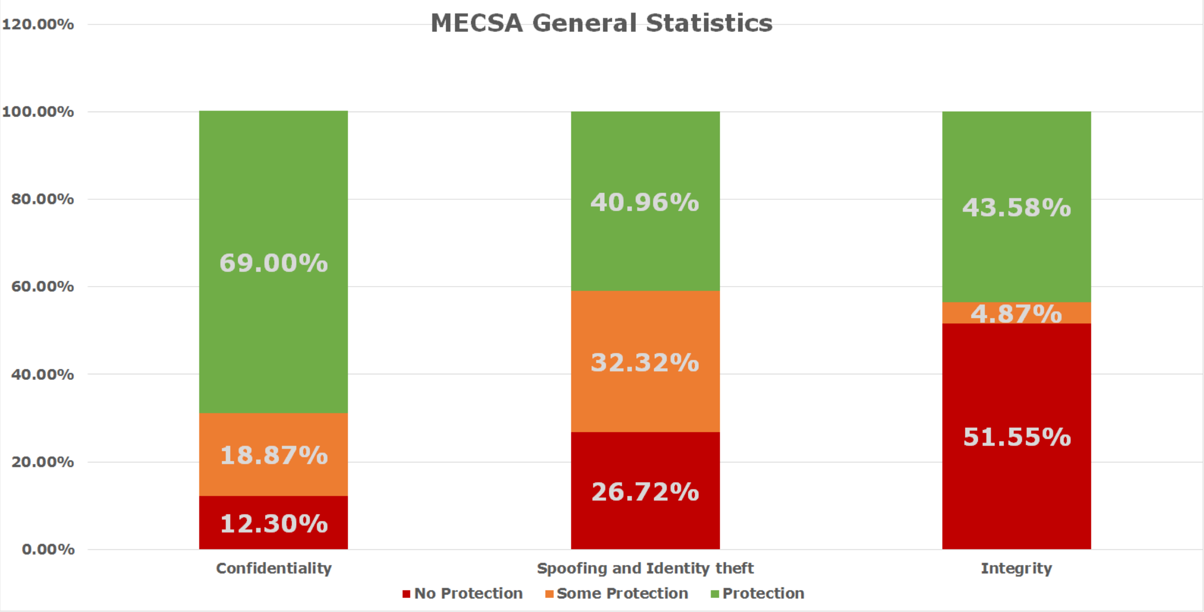

Figure 4: Overall Results from the MECSA platform

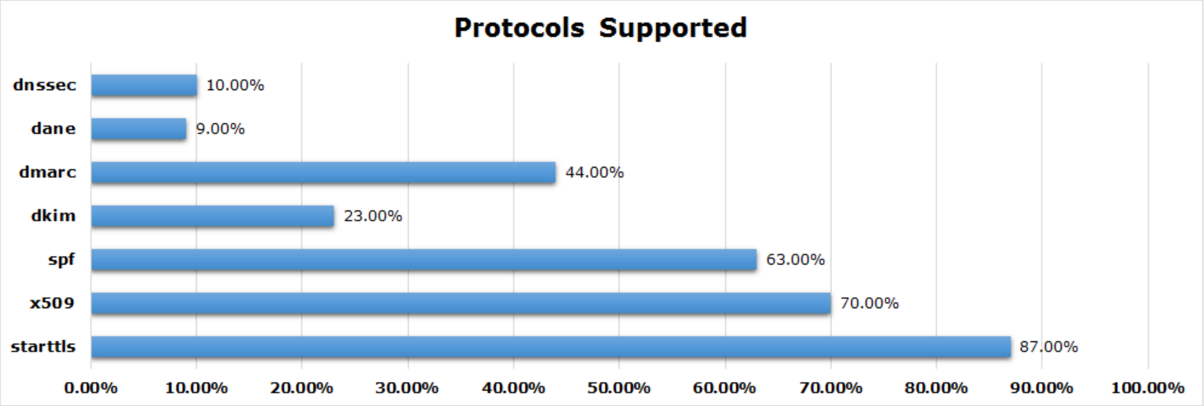

Figure 5: Overall Results from the MECSA platform by Protocol

Phishing and Identity Theft
Phishing and identity theft is the category with a lower percentage of protection, only 40.96% of the email providers would offer protection against it. In this case, the amount of providers with minimum level of protection, i.e. partially supporting the protocols needed (SPF, DKIM, DMARC, DNSSEC) or supporting them with errors is 33.32%. More than one fourth of email providers, 26.72%, do not support any of the standards related to the protection against phishing and identity theft.

Integrity of Messages
Regarding the protecting the integrity of email communications, the results in Figure 4 show that 43.58% of email providers protect it. Although the percentage is slightly larger that the percentage for protection against phishing and identity theft, the number of providers with minimum support (i.e. support with errors) is much more lower, only 4%. More than 50% of domains do not protect the integrity of their user's email communications, mainly because the standards used to evaluate (positively) this domain, DANE and DNSSEC, are the ones with less support, as we can see in Figure 5.

Figure 5 presents the percentages of support, by protocol. StartTLS is the standard most supported, 87% of the email providers have StartTLS enabled in at least 80% of their communications. But only 70% use a valid certificate. The most common errors we found are the usage of self-signed certificates, failing to provide the full chain of certificates to the root Certification Authority (CA), and having certificates that do not match the Full Qualified Domain Name (FQDN) of the corresponding MX.

SPF is supported by 63% of the email providers tested, and there is another 4% that publish an SPF DNS record, but with syntax errors. Among the syntax errors detected there are two that account for most of them: *'Void lookup limit of 2 exceeded'* and *'Too many DNS lookups'*. The first one occurs when an SPF record includes references to more than 2 URLs without DNS resolution, whereas the latest occurs when an SPF record includes too many external references. DKIM is supported by less than half of the email providers tested, 44%. DMARC is supported by 23% of the providers tested. DMARC is meant to be deployed along SPF and/or DKIM. In our results, the optimal situation (i.e. SPF and DKIM) occurs in about 78% of the providers with DMARC support, the worse case, DMARC alone, appears in only 2% of the tests.

Only 9% of the email providers tested have DANE enabled, making it the standard with lowest support. But in this case we did not detect any configuration/deployment errors, all domains with TLSA records were validated correctly. Support for DNSSEC is similar than DANE, only 10% of the email providers tested were protected by DNSSEC.

Figure 6 presents the results as percentages of each domain protected, by category. As previously mentioned, to obtain the category of the URL, we used the Fortiguard[2] web filter application. In the

[2] https://fortiguard.com/webfilter

Table 4.1: default

Category	Domains	Category	Domains
Newly Observed Domain	1315	News and Media	42
Business	1058	General Organizations	31
Information Technology	646	Shopping	30
Education	347	Sports	26
Government and Legal Organizations	248	Web Hosting	23
Search Engines and Portals	133	Political Organizations	21
Web-based Email	95	Meaningless Content	19
Not Rated	80	Society and Lifestyles	17
Health and Wellness	69	Games	16
Personal Websites and Blogs	65	Arts and Culture	14
Reference	65	Global Religion	13
Finance and Banking	63	Personal Vehicles	11
Travel	62	Newsgroups and Message Boards	10
Entertainment	47		

Table 4.2: Number of domains in each category, for categories with more than 10 domains

results presented, we have eliminated from the list those domains with less than 10 samples. In Table 4.2 we have all the categories ordered by the number of domains per category. The top category is *Newly Observed Domain*, which means a domain recently configured or activated, followed by the *business* category.

In only 2 categories all the email providers protect their user's email communications in the three domains assessed (confidentiality, phishing and identity theft and integrity), '*Society and Lifestyles*' and '*Games*'. Surprisingly, one of the most common categories, *'Business'*, does not support measures to protect the identity of its users nor the integrity of the messages sent and/or received by their users. Moreover, its average score in confidentiality is one of the worst.

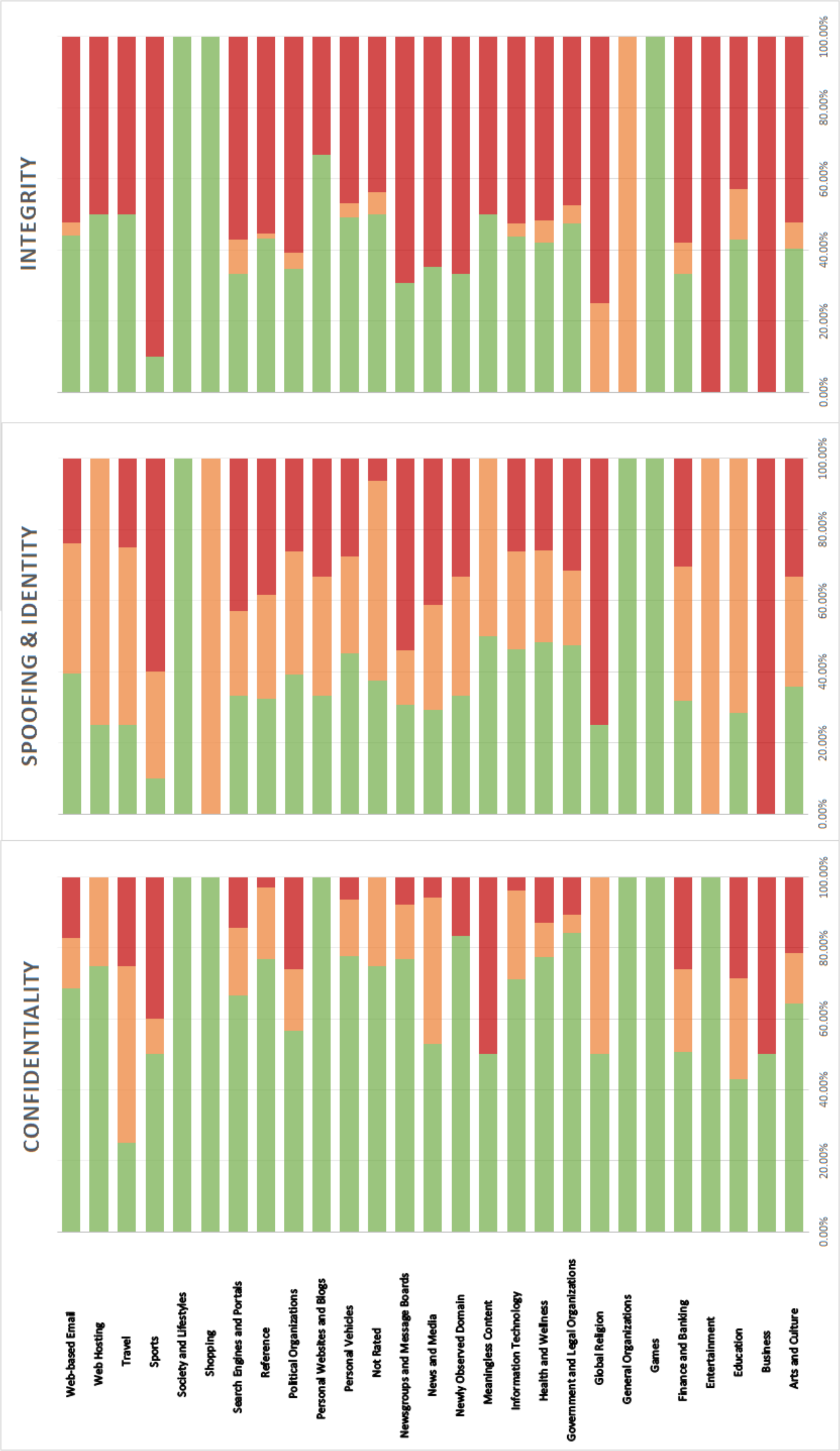

Figure 6: MECSA Results by Category

5 Conclusions

This report presented the results of the MECSA project, a tool created to evaluate the level of adoption of relevant security standards in email communications between providers. It evaluates a given email provider on the basis of the security standards that it supports. In particular, MECSA checks the support of StartTLS and validation of x509 certificates, SPF, DKIM, DMARC, DANE and DNSSEC.

The results obtained reveal serious gaps in the adoption of these standards. In terms of confidentiality, more than 12% of email providers fail to encrypt communications with other providers, and ca. 19% follow an opportunistic encryption approach by not using valid x509 certificates. Furthermore, the adoption of DNSSEC and DANE standards falls below 10%. Standards designed to protect against phishing and identity theft received a fair degree of adoption with over 63% of domains supporting SPF, although its combination with DMARC falls to slightly more than 22%. Regarding the integrity of messages, DKIM is supported only by 44% of the providers tested, and its combination with DMARC falls to less than 20%.

In the light of the data presented in this report, we recommend to study the following actions.

Recommendation of a minimum set of email security standards to be adopted by service providers and development of technical guidelines.
The adoption of email security standards is not mandatory. Email providers can achieve a degree of interoperability good enough to exchange emails with other providers, without supporting any security protocol. In this scenario, emails will be sent and received in plaintext (without encryption) and there will be no mechanisms to protect the integrity of emails or fight email identity theft. These email communications between email providers take place in a completely transparent way for end-users.

Unlike web users, who can rely on the padlock icon of the browser, email users lack indicators of the capability of email providers to protect their digital communications. Our experience with MECSA indicates that most users were unaware of the actual capability of their email provider to protect their email exchange.

As a result of this, there is a current lack of incentives for email providers to adopt modern email security standards. This lack of incentives propagate along the supply chain. There is not always a big enough demand for email server software/appliance vendors to support these standards. As a result, many well-known email products (usually appliances and proprietary software) lack support for some of them.

A European recommendation on a set of modern email security standards to be supported by email providers would help to close existing gaps in their adoption. Public procurement of email server software/hardware products could refer to this recommendation when setting the mandatory functionalities and security requirements.

We found that in many cases email providers attempted to adopt security standards but failed to deploy them correctly. In particular, more than 18.87% of the email providers analysed failed to deploy properly standards related to protecting the confidentiality. That figure raised to 32.32% for in deployment of those standards related to the fight against email spoofing and identity theft.

The development of technical guidelines and good practices for the deployment of email security standards would help to avoid common mistakes like missing certificate chains or syntax errors in the policies. This could be of particular importance in the case of SMEs that might lack the resources required to carry out the deployment of these standards.

Support on-going efforts to promote modern email security standards and incentivise their adoption.

Only 25.66% of the email providers analysed by MECSA were found to have properly adopted the minimum set of modern email security standards recommended to ensure the confidentiality, integrity and authenticity of the communications. Out of this 25.66%, only 19.02% adopted all recommended email security standards.

26.72% of email providers did not adopt any email security standard to fight email spoofing and identity theft. Moreover, 12.30% of email providers did not employ any security standard to protect the confidentiality of the email exchange between email providers.

The several on-going efforts to promote modern email security standards in Member States should be promoted. In this regards, we consider that MECSA is a valuable tool to contribute and complement these efforts.

Moreover, strategies to incentivise the adoption of email security standards should be considered. For example, the application of a security seal backed up by the objective assessment of the email security standards properly adopted by a given email provider, would help to boost end-user's trust and provide an incentive for manufacturers and service providers.

Acronyms

BGP Border Gateway Protocol [21] 10

CA Certification Authority 18

DANE DNS-based Authentication of Named Entities [14, 11, 8] 8

DKIM DomainKeys Identified Mail [7] 8

DMARC Domain-based Message Authentication, Reporting and Conformance [20] 8

DNS Domain Name System 8

DNSSEC Domain Name System Security Extensions [2, 13, 34] 8

FQDN Full Qualified Domain Name 18

GDPR General Data Protection Regulation EU 2016/679 [32] 7

IMAP Internet Message Access Protocol [6] 9

MECSA My Email Communications Security Assessment 3

MITM Man-In-The-Middle 10

MTA Mail Transfer Agent 10

MTA-STS SMTP Strict Transport Security [24] 12

MX Mail Exchanger 13

POP3 Post Office Protocol - Version 3 [26] 9

SMTP Simple Mail Transfer Protocol [18] 3

SPF Sender Policy Framework [17, 19] 8

Bibliography

[1] C. Adams, S. Farrell, T. Kause, and T. Mononen. Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP). RFC 4210 (Proposed Standard), September 2005. Updated by RFC 6712.

[2] R. Arends, R. Austein, M. Larson, D. Massey, and S. Rose. DNS Security Introduction and Requirements. RFC 4033 (Proposed Standard), March 2005. Updated by RFCs 6014, 6840.

[3] Taejoong Chung, Roland van Rijswijk-Deij, Balakrishnan Chandrasekaran, David Choffnes, Dave Levin, Bruce M. Maggs, Alan Mislove, and Christo Wilson. A longitudinal, end-to-end view of the DNSSEC ecosystem. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 1307–1322, Vancouver, BC, 2017. USENIX Association.

[4] European Commission. Special eurobarometer 462. e-communications and digital single market. `http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/SPECIAL/surveyKy/2155`.

[5] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280 (Proposed Standard), May 2008. Updated by RFC 6818.

[6] M. Crispin. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. RFC 3501 (Proposed Standard), March 2003. Updated by RFCs 4466, 4469, 4551, 5032, 5182, 5738, 6186, 6858, 7817.

[7] D. Crocker, T. Hansen, and M. Kucherawy. DomainKeys Identified Mail (DKIM) Signatures. RFC 6376 (INTERNET STANDARD), September 2011.

[8] V. Dukhovni and W. Hardaker. The DNS-Based Authentication of Named Entities (DANE) Protocol: Updates and Operational Guidance. RFC 7671 (Proposed Standard), October 2015.

[9] Zakir Durumeric, David Adrian, Ariana Mirian, James Kasten, Elie Bursztein, Nicolas Lidzborski, Kurt Thomas, Vijay Eranti, Michael Bailey, and J. Alex Halderman. Neither snow nor rain nor mitm...: An empirical analysis of email delivery security. In *Proceedings of the 2015 Internet Measurement Conference*, IMC '15, pages 27–39, New York, NY, USA, 2015. ACM.

[10] Jim Fenton. SMTP Require TLS Option. Internet-Draft draft-ietf-uta-smtp-require-tls-06, Internet Engineering Task Force, December 2018. Work in Progress.

[11] O. Gudmundsson. Adding Acronyms to Simplify Conversations about DNS-Based Authentication of Named Entities (DANE). RFC 7218 (Proposed Standard), April 2014.

[12] P. Hoffman. SMTP Service Extension for Secure SMTP over Transport Layer Security. RFC 3207 (Proposed Standard), February 2002. Updated by RFC 7817.

[13] P. Hoffman. Cryptographic Algorithm Identifier Allocation for DNSSEC. RFC 6014 (Proposed Standard), November 2010.

[14] P. Hoffman and J. Schlyter. The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA. RFC 6698 (Proposed Standard), August 2012. Updated by RFCs 7218, 7671.

[15] Internet Engineering Task Force (IETF). Using tls in applications: Charter. `https://datatracker.ietf.org/doc/charter-ietf-uta/`.

[16] Iwen Coisel Ignacio Sanchez, Apostolos Malatras. A security analysis of email communications. JRC Technical Report JRC99372, European Comission.

[17] S. Kitterman. Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, Version 1. RFC 7208 (Proposed Standard), April 2014. Updated by RFC 7372.

[18] J. Klensin. Simple Mail Transfer Protocol. RFC 5321 (Draft Standard), October 2008. Updated by RFC 7504.

[19] M. Kucherawy. Email Authentication Status Codes. RFC 7372 (Proposed Standard), September 2014.

[20] M. Kucherawy and E. Zwicky. Domain-based Message Authentication, Reporting, and Conformance (DMARC). RFC 7489 (Informational), March 2015.

[21] K. Lougheed and Y. Rekhter. Border gateway protocol 3 (bgp-3). RFC 1267, RFC Editor, October 1991.

[22] A. Malatras, I. Coisel, and I. Sanchez. Technical recommendations for improving security of email communications. In *39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pages 1381–1386. Croatian Society MIPRO, 2016.

[23] Daniel Margolis, Alexander Brotman, Binu Ramakrishnan, Janet Jones, and Mark Risher. SMTP TLS Reporting. RFC 8460, September 2018.

[24] Daniel Margolis, Mark Risher, Binu Ramakrishnan, Alexander Brotman, and Janet Jones. SMTP MTA Strict Transport Security (MTA-STS). RFC 8461, September 2018.

[25] A. Melnikov. Updated Transport Layer Security (TLS) Server Identity Check Procedure for Email-Related Protocols. RFC 7817 (Proposed Standard), March 2016.

[26] J. Myers and M. Rose. Post Office Protocol - Version 3. RFC 1939 (INTERNET STANDARD), May 1996. Updated by RFCs 1957, 2449, 6186.

[27] Ola Nordström and Constantinos Dovrolis. Beware of bgp attacks. *SIGCOMM Computer Communication Review*, 34(2):1–8, 2004.

[28] Council of European Union. Charter of fundamental rights of the european union 2012/c 326/02.
`http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:C2012/326/02`.

[29] Council of European Union. Directive 1999/93/ec of the european parliament and of the council of 13 december 1999 on a community framework for electronic signatures.
`http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:31999L0093`.

[30] Council of European Union. Proposal for a directive of the european parliament and of the council establishing the european electronic communications code (recast) com/2016/0590 final - 2016/0288 (cod).
`https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0590`.

[31] Council of European Union. Proposal for a regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing directive 2002/58/ec (regulation on privacy and electronic communications) com/2017/010 final - 2017/03 (cod).
`https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52017PC0010`.

[32] Council of European Union. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation) (text with eea relevance).
`https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016R0679`.

[33] S. Santesson, M. Nystrom, and T. Polk. Internet X.509 Public Key Infrastructure: Qualified Certificates Profile. RFC 3739 (Proposed Standard), March 2004.

[34] S. Weiler and D. Blacka. Clarifications and Implementation Notes for DNS Security (DNSSEC). RFC 6840 (Proposed Standard), February 2013.

[35] P. Yee. Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 6818 (Proposed Standard), January 2013.

KJ-NA-29674-EN-N

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
ec.europa.eu/jrc

@EU_ScienceHub

EU Science Hub - Joint Research Centre

Joint Research Centre

EU Science Hub

Publications Office

doi:10.2760/166203
ISBN 978-92-76-00256-7