Secure e-mail authentication policy 1.1

Generally, cybercrime involves unlawful activities committed in cyberspace, and the computer is used as a medium or tool to commit those crimes. These acts are sometimes known as “old crimes, new tools”, since the crimes committed are originally old or traditional types of crime (from the offline world), but the techniques of committing the crimes have changed within the digital environment. One example is computer fraud, which is committed by manipulating computer data belonging to others in order to dishonestly obtain or embezzle money or property, to cause loss.

“New crimes, new tools” refers to another type of cybercrime; the crimes involve a situation where the suspect uses the computer system to alter certain data in that system. These crimes are committed against the computer system.

They include sabotage, vandalism, electronic wiretapping, and gaining illegal access by impersonating an authorized user or exceeding a person’s authority.

Moreover, spreading computer viruses, cyber war, cyber terrorism, denial of service (DoS), invasion of privacy (such as access to personal information), hacking, phishing or identity theft, cybersquatting, cyberstalking, mass web defacement and faring are all categorized as cybercrimes.

In summary, cybercrimes are evolving and will continue to evolve with new technology and versatile criminal minds.

According to a recent study (see footnote 1 at the bottom of page 2), the most significant threats involving e-mail users appear to be spam, phishing and denial of service:

i Spam: Spam refers to unwanted notices. They are mostly marketing notices. There are different definitions of spam; we use the term to refer to e-mail sent to many recipients (bulk), without appropriate labels allowing quick filtering by receivers (or receiving domains) not desiring to receive e-mail of this class. Spam annoys users, wastes the recipient’s time and network resources, and reduces the reliability and the functionality of e-mail, but serves the interests of the spammer.

ii Phishing: Phishing refers to luring Internet users to websites that masquerade as legitimate websites (e.g. banks, credit card companies, auction sites, popular social websites and Internet service sites) and directing the users to enter sensitive information, such as user names, passwords, credit card details and bank account details. The information thus acquired may be re-sold or used to commit cybercrimes including theft, identity theft and fraud. The Identity Theft Resource Center (ITRC) defines “identity theft” as “a crime in which an impostor obtains key pieces of personal identifying information (PII), such as Social Security numbers and driver’s licence numbers, and uses them for their own personal gain” (www.idtheftcenter.org/).

   According to the ITRC, individual identity theft falls into three categories:

   a Financial identity theft: the thief may impersonate the victim to get a loan from a financial institution, take over the victim’s bank account(s), pass bad checks, etc.

   b Criminal identity theft: for example, a criminal identifies him or herself to authorities as another individual in order to commit a crime, get special permits, commit acts of terrorism, and so on.

   c Identity cloning: the thief uses another’s information to assume his or her identity in daily life, for such purposes as opening a new phone or wireless account and getting utility services.

iii Denial of service: DoS e-mails are intended to cause harm to the operation of the e-mail system of the recipient and/or a third party. The most common DoS e-mail attack is by “clogging”, i.e. sending many e-mails to the recipient and/or a third party with the goal of causing excessive overhead. A “Joe Job” attack is a special form of clogging; it sends many e-mails with an incorrect, spoofed sender address,

with the goal of causing the recipients to send error ("bounce") messages to the spoofed sender address, thereby overloading it with the processing of these bounces.[1]

Focusing on the predominant e-mail sender authentication proposals, the main motivation of which is to identify and block spam, phishing and other abusive e-mails, we can consider the Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM), which are based on the Domain Name System (DNS).

The following policy seeks, among other benefits, to reduce the threats previously mentioned.

All .POST domain name owners (registrants) using e-mail originating from a .POST domain, shall comply with this policy to secure their e-mail servers.

The e-mail and DNS server should be secured in accordance with the four principles below:

– Do not use open relay; enable SMTP authentication.

– Activate reverse DNS lookup and greylisting on the e-mail server.

– Enable Domain Keys Identified Mail (2048-bit key signature).

– Implement a Sender Policy Framework.

Domain Keys Identified Mail (DKIM) recommendations

All .POST domains with MX records should introduce mandatory DKIM entry with 2048-bit key signature (subject to support by the DNS vendor).

.POST domains without MX records should still introduce an empty DKIM entry, for example:

**._domainkey.domain.POST. IN TXT "v=DKIM1; p="*

Sender Policy Framework (SPF) recommendations

All .POST domains with MX records should introduce mandatory SPF entry specifying authorized SMTP servers.

.POST domains without MX records should introduce an SPF entry explicitly indicating that no sending servers are available:

@ IN TXT "v=spf1 -all"

Domain-based Message Authentication, Reporting and Conformance (DMARC) recommendations

All .POST domains with MX records should implement mandatory DMARC protocol at least as p=none, eventually as p=quarantine, and ideally as p=reject.

.POST domains without MX records should always have DMARC implemented to protect the domain name with the policy p=reject:

Note. – Close attention should be paid by those implementing DMARC in a production environment and the policy should first be implemented as mentioned on the www.dmarc.org site.

The implementation of DMARC enhances the security, integrity and trustworthiness of the e-mail channel by preventing the delivery of invalid or spoofed e-mail purporting to originate from an in-zone domain.

A compliance report should be presented to the secretariat once these principles have been set up.

[1] Amir Herzberg, DNS-based e-mail sender authentication mechanisms: A critical review, Computers & Security, Volume 28, Issue 8, November 2009, pp. 731–742, ISSN 0167–4048, dx.doi.org/10.1016/j.cose.2009.05.002.

Additional recommendations for enhancing the security of e-mail accounts are as follows:

– *Hashed password storage:* passwords may be stored as salted hashes, following the current NIST recommendation on secure hash functions. These specifications recommend usage of the SHA–256 or bcrypt algorithm with at least 64,000 rounds;

– *Two-factor authentication:* When users need to reset their passwords to the mail platform, a two-factor authentication must be performed first.

The secretariat will check whether the domain name is compliant with the policy before authorizing the domain name owner to allow its e-mail services to be operated.

The details for implementation of the four principles of this policy are out of the scope of this policy document. Domain name owners should verify the details with their local e-mail or DNS technical provider.

Explanation of referenced standards

The following standards are important parts of the e-mail policy to secure the e-mail server under .POST:

– Domain-based Message Authentication, Reporting and Conformance (DMARC) is a technical specification created by a group of organizations to help reduce the potential for e-mail–based abuse, such as e-mail spoofing and phishing e-mails, by solving some long-standing operational, deployment, and reporting issues related to e-mail authentication protocols.[2]

– Sender Policy Framework (SPF) is an e-mail validation system designed to prevent e-mail spam by detecting e-mail spoofing, a common vulnerability, by verifying sender IP addresses. The primary objective of SPF is to control forged e-mail. SPF is a relatively simple system that utilizes text entries in the domain's DNS allowing domain owners to specify what servers are permitted to send mail on behalf of a particular domain. With SPF, administrators can specify which hosts are allowed to send mail from a given domain by creating a specific SPF record (or TXT record) in the DNS.[3] SPF depends on the use of SPF lookups by the recipient server to validate that messages are authentic. On the other hand, SPF does not address aspects of securing e-mail content.[4]

– Domain Keys Identified Mail is a method for associating a domain name with an e-mail message. It defines a domain-level digital signature authentication framework for e-mail in order to permit verification of the source and contents integrity of messages. Indeed, DKIM allows a person, role or organization that owns the signing domain to claim some responsibility for a message by associating the domain with the message. It is important to highlight that DKIM separates the identity of the signer of the message from the purported author of the message. Signer and author could be different. Assertion of responsibility is validated through a cryptographic signature and by querying the signer's domain directly to retrieve the appropriate public key. Message transit from author to recipient is through relays that typically make no substantive change to the message content and thus preserve the DKIM signature.[5] Compared to SPF, DKIM is a more advanced system utilizing cryptographic authentication to verify a signature assigned to a message on the sender's server.

  DKIM requires configuration support on the SMTP server in addition to DNS entries that must be made on the sender's domain. DKIM provides a technology to secure message header fields and message body, but it does not guarantee non-repudiation, originator authentication and protection after signature verification.[6] In addition, it does not provide confidentiality.

2 www.dmarc.org.

3 en.wikipedia.org/wiki/Sender_Policy_Framework.

4 M. Wong and W. Schlitt, Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1, RFC4408, Experimental, April 2006, IETF, available at: tools.ietf.org/html/rfc4408.

5 T. Hansen, D. Crocker, and M. Kucherawy, DomainKeys Identified Mail (DKIM) Signature, RFC6376, Informational, September 2011, IETF, available at: https://tools.ietf.org/search/rfc6376.

6 T. Hansen, D. Crocker, and P. Hallam-Baker, DomainKeys Identified Mail (DKIM) Service Overview, RFC5585, Informational, July 2009, IETF, available at: tools.ietf.org/rfc/rfc5585.txt.

Additional notes:

a Sender authentication technologies like Domain Keys Identified Mail and Sender Policy Framework not only help control spam but also improve deliverability of legitimate messages.

b Both SPF and DKIM attempt to validate the authenticity of a message by looking at the sending domain name and qualifying that the server sending the message is legitimate. However, SPF and DKIM each approach this task differently and have their own unique methodologies and implementations.

c When you add authentication information to your domain, an added benefit is that many ISPs use authentication to track sending reputation. With authentication handled by your domain, reputation with the receiving ISPs is influenced by your domain and the e-mails sent on behalf of your domain. This means you maintain control over the e-mails that affect deliverability for your domain. A positive reputation for your domain builds trust and improves deliverability, affecting whether your e-mails are caught by spam filters and how quickly the receiving servers will accept mail from your domain.

d The combined use of SPF and DKIM reduces the number of false positives and can increase the receiving network's confidence in authentication, to the point of it being willing to start blocking messages that fail both authentication processes.

e The SPF information policy details are outside the scope of this policy and have to be defined by the domain name owner. Please contact the secretariat for further details regarding the implementation.

f Mailing list: this topic should be further studied and considered for future improvements of the policy.

Recommendations for e-mail servers exchanging with .POST domains

For other e-mail servers intending to receive e-mails from a .POST domain, it is highly recommended that the above policy be adopted in order to strengthen the effectiveness of the policy and obtain all the advantages at both ends of the DKIM and SPF implementation.

Compliance check

For an industry-standard mail solution, it is important that all security features be properly implemented and that the parameters be set correctly.

Secure mail solutions provided under .POST will need to have a compliance verification to ensure the e-mail server/DNS is validated and to verify that this policy has been implemented correctly.

Compliance can be verified directly by the domain name owner using the tools below. A report with the results must be submitted to the UPU for evaluation. The UPU will provide the requester with final recommendations about its compliance for use of e-mail under .POST.

Tools to check for compliance with DKIM and SPF

– www.dmarcanalyzer.com/dkim/dkim-checker

– https://vamsoft.com/support/tools/spf-policy-tester

– www.isnotspam.com