Secure Email - A Usability Study

Projet Fin d'Études (PFE)
CryptogrAphie, Sécurité, et vie Privée dans les Applications et Réseaux (CASPAR)
Supervisor: Karima Boudaoud
Polytech Nice Sophia Antipolis

Adrian Reuter
Technische Universität München (TUM)
Email: adrian.reuter@tum.de

Ahmed Abdelmaksoud
Polytech Nice Sophia Antipolis
Email:

Wadie Lemrazzeq
Polytech Nice Sophia Antipolis
Email:

ABSTRACT

Keywords

Source Routing, Source Packet Routing, Segment Routing, MPLS, SPRING, RPL, DSR, RH0

1. INTRODUCTION

asdfasdfa

2. ANALYSIS OF END-TO-END ENCRYPTION TECHNOLOGIES FOR EMAILS

2.1 Pretty Good Privacy (PGP)

Developed by Phil Zimmermann in 1991, Pretty Good Privacy (PGP) is an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. In this study we will focus only on using PGP for e-mail security (e-mail encryption). It follows the OpenPGP standard for encrypting and decrypting data. Many e-mail clients provide OpenPGP-compliant e-mail security as described in RFC 3156 [1]. The current specification is RFC 4880 (November 2007) [2]. PGP encryption uses a serial combination of hashing algorithms (SHA-1, SHA-224 / 256 / 384 / 512), data compression algorithms (zip, zlib, and bzip2), symmetric encryption algorithms (3DES, AES-128 / 192 / 256, CAST5, IDEA) and finally asymmetric encryption algorithms (ElGamal, RSA (MUST NOT <1024 bits)). Symmetric-key cryptography involves using the same key to both encrypt and decrypt data.

In PGP, one-off key is generated randomly, which is known as the session key. The session key encrypts the message, which is the bulk of the data that needs to be sent. This type of encryption is relatively efficient, but it has a problem of sharing the session key with your recipient because without the key your recipient will only see the ciphertext. PGP solves this problem with public-key cryptography, also known as asymmetric cryptography. In this kind of encryption there are two keys: a public key and a private one. The public key of your potential correspondent can be found by searching through key servers or by asking the person directly. Moreover, each public key is bound to an e-mail address and has a unique fingerprint which can be used to get the right corresponding public key [?]. In PGP, public-key encryption isnâĂŹt used to encrypt the message, just the one-off session key that was generated to encrypt it. It would take too long and use a larger amount of computational resources. Since the body of the message usually contains the bulk of the data, PGP uses the more economical symmetric-key encryption for this. It reserves the lumbering public-key encryption for the session key, making the whole process more efficient. Our written signatures are frequently used to verify that we are who we say we are. They are far from foolproof, but they are still a useful way of preventing fraud.
Digital signatures are similar, using public-key cryptography to authenticate that the data comes from the source it claims to and that it has not been tampered with. Digital signatures work by using an algorithm to combine the senderâĂŹs private key with the data that they are authenticating. The plaintext of the message is fed through a hash function, which is an algorithm that transforms inputs into a fixed-size block of data, called a message digest. The message digest is then encrypted with the senderâĂŹs private key. This encrypted message digestis what is known as the digital signature [?]. In [?], the digital signature is sent alongside the message body (which can either be encrypted or in plaintext). When someone receives a digitally signed electronic mail (e-mail), they can check its authenticity and integrity by using the public key of the sender. First, a hash function is used on the message that was received and this gives the message digest of the email in its current form [?]. The next step is to calculate the original message digest from the digital signature that was sent. The senderâĂŹs public key is used to decrypt the digital signature, and this gives the message digest exactly as it was when it was signed by the sender. The final step is to compare the message digest from the email they received to the message digest that they derived from the digital signature. If the message has been altered, then the message digests will be completely different, and the recipient will know that there is a problem with the message. If the two message digests are not identical, there are three likely culprits [?]:

- Inhalt...

2.2 Secure Multipurpose Internet Mail Extension (S/MIME)

2.3 Pretty Easy Privacy (pEp)

3. CONCLUSION

4. EXAMPLARY CONTENT

In order to advance the research and standardization of a flexible and universal source routing mechanism, the Internet Engineering Task Force (IETF) has formed a working group (WG) in 2013. This WG, called *Source Packet Routing in Networking (SPRING)*, is chartered to identify source routing use cases as well as defining the requirements and mechanisms for implementing, deploying and administrating source routing enabled networks [3]. The working group yet developed a new source routing mechanism called *segment routing* [4], which is discussed in section 4.1. It further introduced two implementational approaches [5, 6], which will be discussed in section **??** and **??**. The working group is currently preparing their final document revisions for a technical review and adoption to IETF standards track [7].

4.1 Segment Routing

Segment routing is a new source routing mechanism developed by the IETF SPRING working group. It is based on so-called *segments* [4]. The SPRING architecture [4] defines that a segment represents *"an instruction a node executes on the incoming packet (e.g.: forward packet according to shortest path to destination, or, forward packet through a specific interface, or, deliver the packet to a given application/service instance)"*. A segment and its associated *Segment Identifier (SID)* is advertised within the segment routing domain with the help of the Interior Gateway Protocol (IGP) in use. Therefore the SPRING working group has defined extensions for the IGP protocols OSPF [8], OSPFv3 [9] and IS-IS [10]. With the help of these extensions, those protocols are able to carry the necessary segment routing signaling information. Segment routing introduces three major types of segments [11, 4]:

- IGP-Prefix Segments
- IGP-Node Segments
- IGP-Adjacency Segments

Each of these segment types are discussed in the following sections. The term *ingress node* identifies the node at which a packet enters the segment routing domain, whereas *egress node* identifies the node at which a packet exits the segment routing domain.

4.1.1 IGP-Node Segment

An IGP-node segment has global scope and thus is identified by a globally unique SID. Each node is assigned a SID and advertises its nodal segment via the IGP protocol [12]. Global scope in this context means that all nodes within a segment routing domain add an entry in their Forwarding Information Base for the instruction associated with that segment [13]. The node identified by the node-SID is always reached by the shortest path, which is determined by the IGP algorithm [4]. That means an ingress node can impose a source route to a packet by specifying another node to be traversed by prepending the correspondent node-SID to that packet.

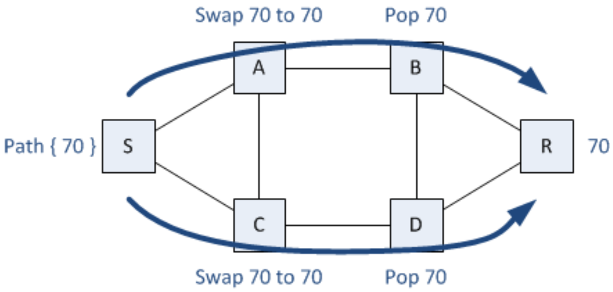

Figure 1: Node Segments [12]

Figure 1 shows an exemplary scenario: Node R advertised its node-SID 70 to all other nodes within the domain. Node S can instruct incoming packets to traverse node R by prepending the node-SID 70 to it. Hence the packet will be either forwarded via the path {S,A,B,R} or {S,C,D,R}, depending on which of both paths have been investigated as the shortest path. Intermediate nodes do not change the prepended SID, thus symbolically swapping it from 70 to 70, except for the last node. The last node on the path towards R is directly connected to R and thereby can remove the SID as this information is not needed anymore [12].

5. REFERENCES

[1] M. Elkins, D. D. Torto, R. Levien, and T. Roessler, "MIME Security with OpenPGP." RFC 3156 (Proposed Standard), Aug. 2001.

[2] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format." RFC 4880 (Proposed Standard), Nov. 2007. Updated by RFC 5581.

[3] A. Retana and S. Bryant, "Charter: Source Packet Routing in Networking," 2013. `https://datatracker.ietf.org/doc/charter-ietf-spring/`; last accessed on 2016/12/20.

[4] C. Filsfils, S. Previdi, B. Decraene, S. Litkowski, and R. Shakir, "Segment Routing Architecture," 2016. `https://tools.ietf.org/html/draft-ietf-spring-segment-routing-10`; last accessed on 2016/12/19.

[5] C. Filsfils, S. Previdi, B. Field, and I. e. a. Leung, "IPv6 Segment Routing Header (SRH)," 2015. `https://tools.ietf.org/html/draft-previdi-6man-segment-routing-header-08`; last accessed on 2016/12/20.

[6] C. Filsfils, S. Previdi, B. Decraene, S. Litkowski, and R. e. a. Shakir, "Segment Routing with MPLS data plane," 2016. `https://tools.ietf.org/html/draft-ietf-spring-segment-routing-mpls-05`; last accessed on 2016/12/18.

[7] SPRING working group, "Status report for SPRING WG meeting on 2016-11-17," 2016. `https://www.ietf.org/proceedings/97/slides/slides-97-spring-0_ietf97_spring-wg-status-00.ppt`; last accessed on 2016/12/18.

[8] P. Psenak, C. Filsfils, R. Shakir, H. Gredler, W. Henderickx, and J. Tantsura, "OSPF Extensions

for Segment Routing," 2015. https://tools.ietf.org/html/draft-ietf-ospf-segment-routing-extensions-10; last accessed on 2016/12/20.

[9] P. Psenak, C. Filsfils, R. Shakir, H. Gredler, W. Henderickx, and J. Tantsura, "OSPFv3 Extensions for Segment Routing," 2016. https://tools.ietf.org/html/draft-ietf-ospf-ospfv3-segment-routing-extensions-07; last accessed on 2016/12/19.

[10] S. Previdi, C. Filsfils, H. Gredler, S. Litkowski, B. Decraene, and J. Tantsura, "IS-IS Extensions for Segment Routing," 2016. https://tools.ietf.org/html/draft-ietf-isis-segment-routing-extensions-09; last accessed on 2016/12/20.

[11] S. Salsano, L. Veltri, L. Davoli, P. L. Ventre, and G. Siracusano, "PMSR-Poor Man's Segment Routing, a minimalistic approach to Segment Routing and a Traffic Engineering use case," *arXiv preprint arXiv:1512.05281*, 2015.

[12] Y. El Fathi, "Introduction To Segment Routing," 2013. http://packetpushers.net/introduction-to-segment-routing/; last accessed on 2016/12/20.

[13] Cisco Systems Inc., "Segment Routing: Prepare Your Network for New Business Models," 2015. http://www.cisco.com/c/en/us/solutions/collateral/service-provider/application-engineered-routing/white-paper-c11-734250.html; last accessed on 2016/12/14.