A confident email system based on a new Correspondence Model

Laurent Cailleux
French Ministry of Defence
DGA Maitrise de l'Information
35998 Rennes Cedex, France
laurent.cailleux@intradef.gouv.fr

Ahmed Bouabdallah Jean-Marie Bonnin
Institut Mines-Telecom / Telecom Bretagne
Université européenne de Bretagne
Cesson-Sévigné, France
{ahmed.bouabdallah, jm.bonnin}@telecom-bretagne.eu

Abstract— **Despite all the current controversies, the success of the email service is still valid. The ease of use of its various features contributed to its widespread adoption. In general, the email system provides for all its users the same set of features controlled by a single monolithic policy. Such solutions are efficient but limited because they grant no place for the concept of usage which denotes a user's intention of communication: private, professional, administrative, official, military.... The ability to efficiently send emails from mobile devices creates new interesting opportunities. We argue that the context (location, time, device, operating system, access network…) of the email sender appears as a new dimension we have to take into account to complete the picture. Context is clearly orthogonal to usage because a same usage may require different features depending of the context.**

It is clear that there is no global policy meeting requirements of all possible usages and contexts. To address this problem, we propose to define a correspondence model which for a given usage and context allows to derive a correspondence type encapsulating the exact set of required features. With this model, it becomes possible to define an advanced email system which may cope with multiple policies instead of a single monolithic one. By allowing a user to select the exact policy coping with her needs, we argue that our approach reduces the risk-taking allowing the email system to slide from a trusted one to a confident one.

Index Terms—**Email, security, confidence, trust, correspondence, policy, email security**

I. Introduction

Despite all the current controversies, the success of the email service is still valid. The ease of use of its various features contributed to its widespread adoption. This situation is even more pronounced in the professional environment where its use requires the implementation of many services that contribute to secure systems. The legal framework also governs the use of email. It imposes rules with which the email services provider (ESP) must comply by integrating them into their solutions.

In general, the email system provides a set of features for all its users. In some cases, it is possible to set policies for specific users or groups of users, but the description of a dedicated policy is not standard and could be difficult to implement. For this reason, most email systems provide a single monolithic policy applicable to all its users and governing in a uniform way the contract between them and their ESP.

Such solutions are efficient but limited because they grant no place for the concept of usage. It is clear that the use of email systems fits into a particular usage denoting a user's intention of communication (UIC): private, professional, administrative, official, military... In some cases, a user may for example send private messages and in others cases, she has to send professional ones. But UIC can however be more refined through an official message or a registered one.

A sophisticated usage can only be supported by an email system integrating a dedicated set of features. On the other hand the sets of features involved by two distinct usages may be completely different. The cases of private and professional usages are in this sense exemplary because they together require contradictory features (privacy versus archiving). There is therefore no global policy meeting requirements of both usages.

The ability to efficiently send emails from mobile devices (laptop, smartphone...) creates new interesting opportunities for ESP. We argue that the context (location, time, device, operating system, access network…) of the email sender appears as a new dimension we have to take into account to complete the picture. Context is clearly orthogonal to usage because a same usage may require different features depending of the context.

To address this problem, we propose to define a correspondence model which for a given usage and context allows to derive a correspondence type encapsulating the exact set of required features. With this model, it becomes possible to define an advanced email system which may cope with multiple policies instead of a single monolithic one.

An ESP may therefore offer a wide range of email services to meet the need of users. For instance, a user could have a basic email service while another might have a more evolved and adapted service to professional exchanges. In the first case, the system could only verify if the email does not contain viruses or if the message size is not greater than what is allowed. In the case of professional service, the system could require a particular authentication mechanism according to the user location and check whether emails are properly secured with the recommended signature cryptographic algorithm or if the message contains all mandatory information. The system could also apply an appropriate need to know according to the sensitivity of emails and security clearance of users.

Thanks to this new model, it becomes therefore possible to define email policies exactly matching with specific usages and contexts. By allowing a user to select the exact policy coping with her needs, we argue that our approach reduces the risk-taking allowing the email system to slide from a trusted one to a confident one.

In this paper, we introduce a general concept of correspondence, which encapsulates a set of policies. These policies represent the set of constraints associated to a particular and dedicated end-to-end usage and context of the email system. These constraints could be distributed on the different components of the email system. The concept of correspondence therefore preserves their global coherence by articulating them to a given usage in a given context.

This paper is organized as follows. Section 2 introduces a state of art of email concepts, email security concepts, administrative domain concepts and limitations of current models. In section 3, we present our main contributions in the form of a generic correspondence model. Section 4 describes implementation of the correspondence model and we conclude in section 5.

II. State of the art

A. Email concepts

Despite the age of email, concepts have changed little. Certainly, developments have taken place, but the main protocols remain the same. In email concepts, it exists two main classes of protocols; Message format and its routing.

In email system, message format is based on Internet Message Format (IMF) standard [1]. The goal of IMF is to provide syntax for text messages that are sent between computer users, within the framework of electronic mail messages.

The main standard of the second classes of protocol is Simple Mail Transfer Protocol (SMTP) [3]. The objective of SMTP is to transfer email reliably and efficiently between two components of an email system. With SMTP, often related to the Domain Name System [4, 5], it became possible to transfer email from end-user to end-user. SMTP is an application layer protocol for email transfer and is often associated with extensions that provide a number of services [6, 7].

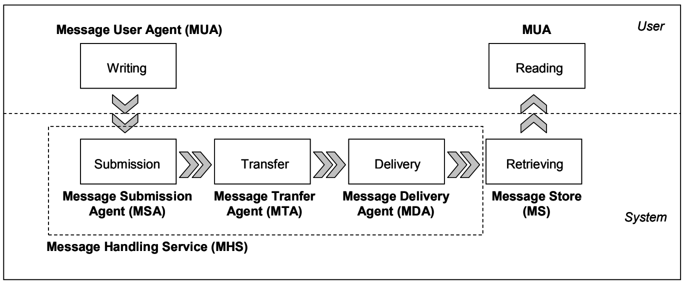
Message User Agent (MUA)
MUA
User
Writing
Reading
Submission
Transfer
Delivery
Retrieving
Message Submission Agent (MSA)
Message Tranfer Agent (MTA)
Message Delivery Agent (MDA)
Message Store (MS)
System
Message Handling Service (MHS)

Figure 1: Components and events in email system

Two other standards of the email routing classes exist. IMAP4 [8] or POP3 [9] allows a user to download a message from its mailbox. A global and comprehensive description of Internet Mail Architecture is given in [10]. Different components and events are described in Fig. 1.

B. Email security concepts

The first email systems were very basic. They didn't include security services and policies were limited. With the threats emerging, ESPs, enterprises and organizations email systems had to evolve. New security objectives and security properties have been defined. It was then necessary to describe the security services to implement these properties [11]:

1. non repudiation of origin,
2. data integrity,
3. data origin authentication,
4. data confidentiality,
5. authorization and access control

In order to apply these properties, different mechanisms have been defined. The main two are cryptographic signature and encryption mechanisms. A valid cryptographic signature allows the recipient to ensure properties 1, 2 and 3. Encryption service guarantees property 4. Property 5 is often performed by proprietary mechanisms.

There are several protocols that provide email signature and email encryption services. PGP (Pretty Good Privacy) [12] and S/MIME (Secure/Multipurpose Internet Mail Extensions) [13] are two main protocols that provide these services. S/MIME is based on a centralized trust model and needs a Public Key Infrastructure (PKI), a trusted third party to provide authenticity of public keys. PGP is based on a decentralized trust model also called Web of Trust. They are oriented towards end-to-end communication and most email clients are compliant with these standards.

Securing hop by hop is usually performed through TLS (Transport Layer Security) [14] which is also implemented in email architecture. It allows client/server applications to communicate in a way that is designed to prevent eavesdropping and tampering.

To implement these protocols, it is necessary to define security policies. These can be more or less complex and tailored in different ways (Signature Policy, Encryption policy…). The scope of application of the security policy depends on the domain of membership of the various components of the email architecture. Email flows must satisfied security policies defined in an administrative domain called ADMD and described below.

C. Concept of Administrative Management Domain

The concept of ADministrative Management Domain (ADMD) is described in the Internet Mail Architecture document [10]. An ADMD is defined as a main actor in Internet mail architecture and is associated with a domain name. An ADMD is an entity, which is under the responsibility of an administrative authority. It applies its independent set of policies and can have trust-based decision-making.

In email communication, one can meet several scenarios. The two main are the following: intra-ADMD and inter-ADMD. These descriptions are briefly presented in IETF

Internet Draft [15] that addresses an alternative mechanism to secure SMTP. In intra-ADMD, emails are transmitted between MHS (Message Handling Service – cf. Fig. 1) components in the same administrative environment, using the same domain name. In this type of model, application of policies and specially security policies are convenient. There is only one administrative authority and all MHS components are under the responsibility of this authority. In the case of inter-ADMD communication, emails are exchanged between ADMD. The originator and recipient of an email are not in the same ADMD but they have to develop trust relationships between theirs respective ADMD. For example, they have to, respectively, create signature and verification of their messages.

A global architecture could integrate several ADMDs. It is typically the case of internet that is composed of a lot of ADMD. Each ADMD has its independent set of policies but relationships between ADMD involve potentially complex arrangement that is why the concept of trust boundary has been introduced. Interactions between ADMDs involve many combinations of administrative and operational relationships. Fig. 2 described architecture with ADMDs and relationships between different types of ADMDs. Inner circle represent an ADMD and outer circle represent trust boundary of ADMD.

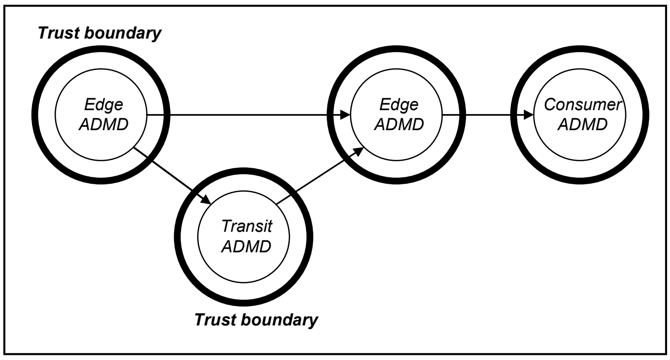

Figure 2: Relationships between different types of ADMD

D. Limitations of current models

In order to take into account particular threats and security objectives, trusted email systems have been defined. These systems meet specific requirements of an organization but they have several important limitations.

These systems require the implementation of many features including security services encapsulated in a single monolithic policy which is the same for all its users. These solutions could be efficient but limited because there is no relation between the nature of the exchange and the applied policy. A common user may indeed have various and different usages of email systems: private, professional, administrative, official, military ... But for a given usage, a user should ideally be able to select the policy which encapsulates the exact set of associated features. The main solution to solve this issue would be to define a system which encapsulates security services required by the most restrictive usage. But although this approach seems to be a good solution, some usages may have requirements that can be opposed. For example, a system that implements a archiving mechanism of all the outgoing messages could not be in compliance with the requirements of privacy. Thus, the encapsulation of security services is not a solution.

Furthermore, email systems can evolve. For example, the appearance of a new threat can lead to the definition of new security services and specification of a new policy. Thus, email systems must be able to evolve in a fast way and according to the new requirements.

To summarize, current email systems implement monolithic policies and they do not address aspects related to the multi-usages concept. Furthermore, to face the new threats, these systems must be able to evolve and take into account new usages.

III. CORRESPONDENCE MODEL

A. Trust versus Confidence

To address the different limitations presented in the previous paragraph, we slightly recall the concepts of trust and confidence.

Trust is a domain which was the object of numerous works and publications [16,17,18]. N. Luhmann suggest an interesting distinction between trust and confidence [19]. “The distinction between confidence and trust depends on our ability to distinguish between dangers and risks, whether remote or a matter of immediate concern”. The concept of trust implies a risk-taking differently from the one of confidence which can be associated to the idea of assurance.

The application of these concepts in email systems finds all its interest. We could imagine a system providing various sets of services allowing to minimize for the user the risk-takings by selecting for each usage and associated context [20,21] the right policy. It is the exact and systematic matching between the changing users needs and the dynamically provided policy which will ensure by reducing the risk-taking, the confident character of the email service. On the other hand, the qualification of trust comes from the risk-takens related to the application of a static monolithic policy poorly fitting to every usage and context.

B. Concepts of correspondence model

A correspondence model allows to define and to enforce policies appropriated to each usage of sending email and according to the current context of the sender.

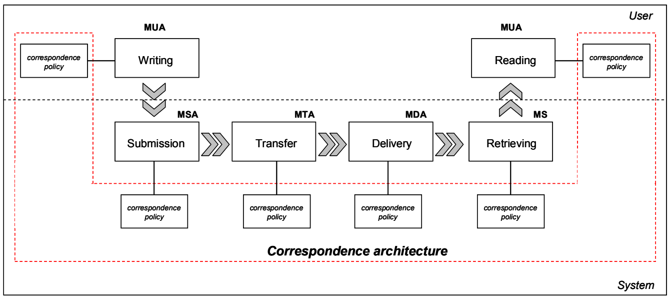

Figure 3: Correspondence architecture in email system

Fig. 3 depicts one way to graft the correspondence model on the email architecture. For each step of an email routing, each component should be solicited to enforce the local part of the correspondence policy according to the usage and context of the email.

Concerning the message, it is a transmitted object from a sender to a recipient. IMF does not contain explicit information related to the used correspondence. In order to explicitly provide this kind of information, we have extended IMF with the definition of eXtended Internet Message Format (XIMF) technology [22]. A prototype implementing the SMTP transmission of the correspondence information has been developed and is currently under tests.

IV. Implementation

An implementation based on correspondence model has been carried out on an email client and on an email server. The email client is Trustedbird[1]. This email client (a project managed by French ministry of defence) based on Thunderbird, provides extended security services. It is able to apply several types of policies according to the correspondence type. For example, it is possible to describe a military message format using metadata present in message and to apply specific security policies to this format [23]. The description of policies is achieved with the XML language.

The email server used for the demonstration is based on Postfix[2] mail server. This development implements mechanisms for the verification and enforcement of policies according to the correspondence type.

With this prototype, we have demonstrated the concepts of our correspondence model.

V. conclusion

In this paper, we presented an innovative correspondence model applied to email systems. Basic email systems allow multiple usages but with a single and monolithic policy. This is a major limitation of current email systems. Our model allows, for each end-user's usage and context, the precise definition of the associated correspondence. We can define an advanced email system that allows implementation of multiple policies adapted to multiple usages. Such systems allow ESP to considerably extend in a confident way their offers by precisely fitting with customers needs.

The main interest of this model is to provide new outlooks for intra-organization email systems, but also for inter-organization email systems. The next challenge of our project is to demonstrate that our correspondence model could be deployed on a larger scope.

References

[1] P. Resnick, "Internet Message Format," RFC 5322, IETF, October 2008.

[2] N. Freed and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, IETF, November 1996

[3] J. Klensin, "Simple Mail Transfer Protocol," RFC 5321, IETF, October 2008.

[4] P.V. Mockapetris, "Domain names - implementation and specification", RFC 1035, IETF, November 1987

[5] R. Elz and R. Bush, "Clarifications to the DNS Specification", RFC 2181, IETF, July 1997

[6] J. Klensin, N. Freed, M. Rose, E. Stefferud, and D. Crocker, "SMTP Service Extensions", STD 10, RFC 1869, IETF, November 1995.

[7] T. Banday, "A Practical Study of E-mail Communication through SMTP", Sprouts: Working Papers on Information Systems, 2010

[8] M. Crispin, "Internet Message Access Protocol – Version 4rev1," RFC 3501, IETF, March 2003

[9] J. Myers and M. Rose, "Post Office Protocol - Version 3", RFC 1939, IETF, May 1996

[10] D. Crocker, "Internet Mail Architecture," RFC 5598, IETF, July 2009.

[11] S. Turner and R. Housley, "Implementing email security and tokens: current standards, tools, and practices".Wiley publishing, Inc., 2008.

[12] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format", RFC 4880, IETF, November 2007.

[13] B. Ramsdell and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification" 5751, IETF, January 2010.

[14] T. Dierks and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, IETF, August 2008.

[15] T. Finch, "Secure SMTP with TLS, DNSSEC and TLSA records, draft-ietf-dane-smtp-00", IETF, Internet draft, work in progress, January 2013.

[16] G. Zhao and D. Chadwick, "Trust Infrastructure for Policy based Messaging In Open Environments," Wetice, pp.144-149, 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05), 2005

[17] J. McGibney and D. Botvich, "Establishing Trust Between Mail Servers to Improve Spam Filtering", pp. 146-155, 4th International Conference on Autonomic and Trusted Computing, ATC'07, Hong Kong, China, 2007

[18] D. Pölz and W. N. Gansterer, "Trustnet Architecture for E-mail Communication," dexa, pp.48-52, 2009 20th International Workshop on Database and Expert Systems Application, 2009

[19] N. Luhmann, "Familiarity, Confidence, Trust: Problems and Alternatives", 2000

[20] A. Bouabdallah, F. Toutain, M. Szczerbak, J.M Bonnin, "On the benefits of a network-centric implementation for context-aware telecom services", 15th International Conference on Intelligence in Next Generation Networks (ICIN 2011), IEEE, 4-7 oct. 2011, Berlin, Germany

[21] M. Szczerbak, A. Bouabdallah, F. Toutain, J.M Bonnin, "Generalizing contextual situations", 6th IEEE International Conference on Semantic Computing (ICSC 2012), IEEE, 19-21 sept. 2012, Palerme, Italy.

[22] L. Cailleux, "Trustedbird", fOSSa2010, January 2010.

[23] L. Cailleux, "A new security service for future MMHS", IEEE military communications and information systems conference, October 2013

[1] http://www.trustedbird.org
[2] http://www.postfix.org