2012 4th International Conference on Cyber Conflict
C. Czosseck, R. Ottis, K. Ziolkowski (Eds.)
2012 © NATO CCD COE Publications, Tallinn

Natural Privacy Preservation Protocol for Electronic Mail

Kim Hartmann
Institute of Electronics, Signal Processing
and Communication
Otto-von-Guericke University
Magdeburg, Germany
kim.hartmann@ovgu.de

Christoph Steup
Department of Distributed Systems
Otto-von-Guericke University
Magdeburg, Germany
steup@ivs.cs.ovgu.de

Abstract: Espionage plays a major role in military and paramilitary cyber warfare activities. While cyber espionage is mainly considered as the act of obtaining (confidential) information using illegal, technical methods, we have explored the possibilities of obtaining confidential material with technical methods using legal exploits. Due to routing conventions, messages containing confidential information may be sent through different states and herewith through conflicting communities. The servers that are used in this routing process are subject to the corresponding states legal system. In the case of electronic mail (e-mail), back-ups or copies being made are accessible to the corresponding authorities and/or private institutions. These copies of e-mails may be requested without knowledge of the sender or the sender's state and can be kept for an uncontrollable period of time. This may also heighten the risk of disclosure for encrypted messages.

We have developed a concept based on IPv6 to allow static and dynamic adjustment of the selected routes to maintain the specified or expected level of confidentiality. This concept may be developed further to be used as a privacy enhancing technology. The concept increases the level of control of transmitted data, technically enforces the expected or negotiated level of privacy and confidentiality, allows data tracking and heightens the user's awareness regarding the differences between postal and electronic mail.

Keywords: *privacy; confidentiality; IPv6; e-mail routing; IPv6 routing*

1. INTRODUCTION

Electronic mail (e-mail) is an important communication service based on TCP/IP and is sometimes said to be even more prominent than the World Wide Web. Especially in businesses, electronic mail is one of the major communication media used to transfer data and information [1].

As any communication medium that shall contact a preferably broad spectrum of individuals, e-mail needs to be easily accessible and hence needs to be able to transport data to almost any location. How this is done and the difficulties that arise due to this technique are described in the sections 2 and 3. At this point it is important to observe that the ubiquity accessibility of e-mail inherently implies a heightened exposure of the transferred data.

Since e-mail is mainly associated with a “point-to-point” communication between individuals or groups of individuals, users expect properties that are not given inherently. These properties are integrity, authenticity and a certain level of confidentiality. Different methods such as encryption and (digital) signing of e-mails aim at establishing one or more of these properties. However, these methods are barely being adopted by the broad public due to multiple reasons [2]. Some of the reasons may be the faulty assumption of a “point-to-point” communication or the association of electronic mail with postal mail and the expected legal implications, see section 2. Regardless what the reasons are, the result is that the majority of e-mails are transmitted without any guarantee of integrity, authenticity or confidentiality.

The small minority of e-mails that are protected by encryption and/or digital signatures are still at risk for manipulation and/or disclosure. Many encryption techniques rely on assumptions regarding the amount of time the protected data is exposed to attacks. It is commonly accepted, that it is rather difficult to hijack one specific e-mail. Expecting the common “man-in-the-middle”-scenario, where the attacker is a single individual without notable political or military power, this assumption may hold true.

However, if the standard “man-in-the-middle”-scenario may not be expected, as in the case of military or paramilitary cyber warfare activities, legal exploits may corrupt the idea of e-mails being hard to obtain. In fact, apart from espionage implications, e-mails may even be copied and preserved legally.

Current law, in most states of the European Union (EU), already demands the preservation of communication details for different periods of time, to allow the control of digital rights violations and for crime investigations. Obviously, this is not done for the purpose of espionage, but the technical practicability of the preservation of communication details and/or contents – without the knowledge of the involved communicating parties – must not be expected to be available to peaceful groups only.

We have developed a concept that provides the ability to influence the route selection and propose a model that additionally may take legal implications into consideration. This is either based on regional borders, “trusted parties” white-lists or information provided by the nodes involved in the e-mail transmission. Additionally to improving methods of control, our concept heightens the awareness regarding the differences between postal and electronic mail. The concept provides users with the ability to technically enforce a negotiated or expected level of confidentiality. We therefore believe that this concept may also be developed further to act as a new type of privacy enhancing technologies (PET).

The remaining part of this paper is structured as follows: The motivation for our work is given in the section 2 divided into legal and technical aspects of the problem described. Sections 3 and

4 give a short introduction to the prerequisites needed, while section 5 describes our concept. A concluding word and outlook is given in section 6.

2. A FAULTY ASSOCIATION

E-mail is often associated with postal mail and often explained as being the digital version of post. This association is faulty in both legal and technical terms and leads to the illusion of using a secured communication medium, see subsections 2.A and 2.B.

A. Technological Issues

Communicating through e-mail is commonly misinterpreted in two ways:

- Due to the association of e-mail with postal mail, the user expects an e-mail to be sent to the receiver directly. Since postal mail is commonly protected through national law and closed mail allows for a reasonable expectation of privacy, the user expects the company transporting and delivering the mail to be subject to national law. Hence, the delivery of e-mail is also expected to be done without the carrier opening, reading or copying and long-term storing the contents, the envelope or other information regarding the communication or the communicating parties.
- The user expects e-mail to be the digital version of a letter. Hence, the user visualizes the e-mail as an enveloped, closed, formally and directly addressed letter, transferred through national or international companies underlying strict laws, guaranteeing the privacy and/or secrecy of correspondence. A reasonable expectation of privacy is given.

1. Point-to-Point-Communication?

Users commonly believe that e-mail enables them to directly communicate with another individual or a selected group of individuals. Technically speaking, a “point-to-point” communication is expected, but not provided.

To allow e-mail to reach a user almost independently of the user’s physical location and despite the offline/online-status a “live”, point-to-point-communication may not be expected. Most individuals today understand e-mail as the digital version of postal mail and hence the e-mail folder is viewed as a digital “postal mailbox”. This implies, that only the individual owning the folder and having access to it, may read the stored e-mail. Unfortunately, this assumption does not hold true.

While most e-mail providers will try to provide secure authentication methods to protect e-mail folders from being corrupted, legal implications may cause exceptions (cf. subsection 2.B).

The removal of an e-mail from the e-mail folder does not guarantee the removal of the e-mail from the server. Again, both technical issues (backup) as well as legal issues (data retention) may prohibit the deletion of contents for a certain amount of time.

Given that both the sender and receiver have e-mail folders and herewith e-mail servers that store the sent/received messages, there are already at least four parties involved in the communication.

However, the transfer of e-mail is mainly not done directly between the involved individuals mail-servers solely. This is mainly due to technical issues, as a) in most cases a direct route does not exist, b) routing conventions and c) traffic situations. The process of forwarding an e-mail through a network of nodes to one specific mail-server is called *e-mail routing* and will be explained further in section 3.

To guarantee the transmission of e-mail despite network difficulties precautions are made. Commonly, the nodes involved in the routing process will save a copy of the data prior to forwarding it. Normally, this data will only be stored for a short period of time. However, this "short period saving" is not guaranteed.

The selection of the route is done at the transport layer, i.e. based on IP routing conventions. These routing mechanisms take into account network and traffic parameters and chose the best (fastest and/or most reliable) route in technical terms. Whether state, company or legal borders are crossed is not part of the route selection process and mechanisms to provide this are currently not available. In fact, the route chosen is neither foreseeable nor evident to the users involved in the communication.

2. E-mail - An Enveloped Letter?

As e-mail is often associated with postal mail, the common visualization of an e-mail is an enveloped letter. This visualization has become so prominent, that the official symbol used by most mail-clients to display e-mails is an envelope.

However, sending a normal (unencrypted, unsigned) e-mail through the Internet should rather be associated with sending a postcard. An unencrypted, unsigned e-mail has neither protection nor guarantee of confidentiality. In this sense, e-mails are even less protected than postcards, as postcards commonly still remain protected by secrecy of correspondence laws.

As explained in subsection 2.A.1) an e-mail may not be expected to be transferred to the receiver directly, nor may it be expected that it is not copied or stored during its transmission. The regulations of the nodes depend on the node's location and the national law applying to them. This is not considered during route selection. No information about opening, copying or even routing of the e-mail is transferred to the user in a transparent or notable way. Moreover, users have currently no opportunity to influence the route selection.

B. Legal Issues

When using e-mail, the users involved assume the communication to be a point-to-point-communication between selected parties. This is neither the case for e-mail nor for postal mail. However, postal mail is commonly protected by secrecy of correspondence laws, guaranteeing that no-one except the sender, receiver and - in the certain, restricted cases – authorities may open or scan postal mail.

Due to the association between electronic and postal mail, the privacy regulations for postal mail are implicitly expected to naturally apply to e-mail as well. However, this assumption of the preservation of a "natural privacy" is currently not transferable to e-mail.

Current legal conventions within some states demand the preservation and surveillance of e-mail communication (with or without contents). In most cases, the communicating parties will not even be aware that their e-mail is being passed through another state due to routing conventions.

We claim, that a) there are differences in the understanding and the implications of secrecy of correspondence laws within different states and b) current laws already enforce the retention of communicated data (and communication related data) to different extents, providing different access options and storing the data for diverging periods of time.

Unfortunately, a complete analysis of the legal situation and understanding of the secrecy of correspondence can't be provided within this paper. To underline our claims, an impression of the understanding and implication of "secrecy of correspondence" is given for the United States and the European Union.

1. Secrecy of Correspondence in the U.S.

The Fourth Amendment to the United States Constitution is part of the Bill of Rights and protects citizens against "unreasonable searches and seizures". However, in the case of "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons and things to be seized" exceptions are possible [3].

If and when the Fourth Amendment also protects digital data, has been discussed heavily. This ambiguousness is due to exceptions possible based on the "probable cause"-clause in the Fourth Amendment and the question if a reasonable expectation of privacy for electronic communication is feasible.

Two recent cases on the topic show the difficulties:

- In *Rehberg v. Paulk* (11.03.2010), the United States Court of Appeals for The Eleventh Circuit ruled that a person "does not have a reasonable expectation of privacy in an e-mail once any copy of the communication is delivered to a third party" [4].
- In *United States v. Warshak* (14.12.2010), the United States Court of Appeals for the Sixth Circuit ruled that a person ".. has a reasonable expectation of privacy in his emails.." and that the Fourth Amendment rights were violated by the government by compelling the Internet Service Provider (ISP) to provide access to e-mails "..without first obtaining a warrant based upon probable cause" [5].

Although the situation regarding the secrecy of correspondence is complicated in the U.S., there is no law enforcing ISPs to store and provide communication data as in the EU (cf. subsection 2.B.2). The Electronic Communications Privacy Act (ECPA) has been criticised by privacy advocates for not protecting all electronic communication and consumer's records. Moreover it is claimed that the access to information stored at an ISP may be obtained too easily by governmental institutions.

In the United States Code, Title 18 – Crimes and Criminal Procedure, Part I – Crimes, Chapter 121 – Stored Wire and Electronic Communications and Transactional Records Access, § 2703, the requirements for the disclosure of costumer communications and records are given. Here it is stated, that the disclosure of data stored for less than 180 days is "only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction" [6]. Data stored for more than 180 days may be disclosed more easily. This also applies to (foreign) e-mails stored on servers in the U.S.

2. European Union and the Data Retention Directive

Most states of the EU have secrecy of correspondence laws, protected by the respective state's constitution. The secrecy of correspondence is explicitly protected by the European Convention on Human Rights, Article 8.

However, in March 2006 the Data Retention Directive was adopted by the EU. Members of the EU are required to store and provide the data specified within the directive for a period of at least 6 months, at most 24 months, for "the purpose of investigation, detection and prosecution of serious crime" [7,8].

The directive makes communication providers responsible for the gathering and storing of the required data. Affected by the directive are telephone, mobile telephone, internet access, e-mail and internet telephony communication data. The data stored must enable to identify the source and destination of the content transferred, the date, time, duration and type of communication as well as the device type used and - in the case of mobile communication - the location of the mobile equipment during the data transfer.

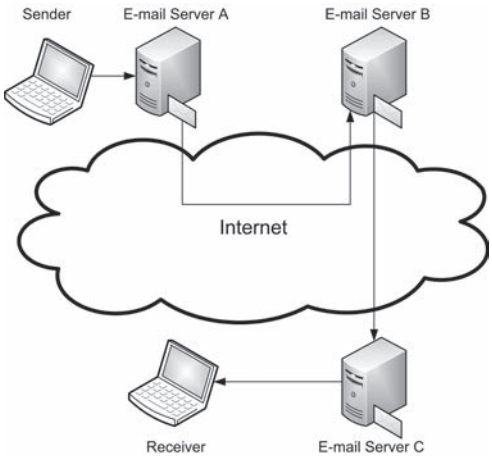
The member states were obligated to transfer the directive to national law until September 2007. Due to the existence of secrecy of correspondence laws within the member states, the implementation of the directive in national law was partially protested heavily. Currently 22 member states tried to transfer the directive to national law [9]. Sweden recently decided to postpone the decision. Romania, Germany and the Czech Republic had previously converted the directive to national law, but their respective courts ruled the directive to be unconstitutional. In 2010, the Irish High Court decided to challenge the Data Retention Law at the European Court of Justice. This was decided due to the previous juridical activities of the civil liberties campaign group "Digital Rights Ireland" (DRI) [10].

3. E-MAIL ROUTING

Sending an e-mail is done at the application layer of the OSI-Model. Common protocols involved in the process of sending and delivering e-mails are SMTP, POP3 and IMAP and their extensions. Relevant is, that all these protocols rely on the previous (i.e. lower) layers of the OSI-Stack to allow correct routing.

Fig. 1 shows how an e-mail is assumed to be forwarded. The sender of the e-mail composes the e-mail using a mail client or - more generally speaking - a Mail User Agent (MUA) and transfers it, by sending the e-mail to the senders mail-server. Here the local Mail Submission Agent (MSA) receives the message, looks-up the destination of the e-mail and forwards the message to the receiver.

FIGURE 1. BASIC VIEW ON E-MAIL COMMUNICATION FLOW



As mentioned previously, the routing through the Internet involves further parties and also the “look-up” of the receiver’s MSA must be specified more correctly. Figure 2 shows a more detailed description of the routing process. As can be seen, the sender’s MSA relies on the feedback given by a Domain Name System (DNS) server to resolve the receiver’s domain name and determine the correct mail exchange (MX) server at the receiver’s domain.

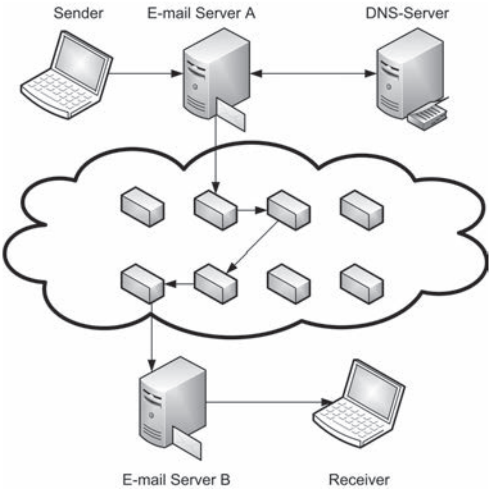
The DNS server responds with a list of MX records. The sender’s MSA then transmits the message by passing it either directly to the correct Mail Transfer Agent (MTA), or by forwarding it through (several) MX servers closer to the destination.

It is clear that several servers are involved in the process of sending an e-mail, especially between different domains. Apart from the servers involved, one must also consider other network components (e.g. routers, gateways) needed to forward the message to the appropriate server.

The route selection is based on network properties, such as distance metrics. These metrics are internal properties and are acquired and used by routers without the user’s knowledge.

To ensure e-mail delivery in case of network failures, nodes, such as routers, gateways and e-mail servers, store a copy of the e-mail locally to retransmit it if necessary. The lifetime of these copies is unspecified and depends on local factors such as memory usage or legal issues.

FIGURE 2. EXTENDED VIEW ON E-MAIL COMMUNICATION FLOW INCLUDING ROUTING AND DNS RESOLUTION



Given the numerous instances involved in the transmission of an e-mail, the fact that the nodes involved commonly store back-up copies of the IP-Packets and that the route selection is based on network properties, the vulnerability of e-mail communication becomes clear. If this vulnerability of e-mail transmission, the unguarded handling of e-mail by private and industrial users and the difficult and diverging legal situations are combined, the threats become apparent. Threats may be cyber espionage in general, industrial or military and paramilitary espionage. This may either be done by:

- Accessing the respective nodes involved in e-mail transmission. This may even be legal given some circumstances (cf. section 2.B),
- Attacking nodes known to be part of the routing of e-mails that are expected to carry useful information. Such nodes may be identified easily by finding the corresponding MTA(s) of a specific domain, e.g. a domain known to belong to military, governmental or similar institutions.

While MSA and MTA servers may only be guarded through intensive precautions done by the network administration, the route selection may be hardened through other concepts. The proposed method will allow controlling the transmission of data and preventing the transmission through untrusted nodes. This prevents both the usage of legal exploits as well as it may allow the selection of secure routes.

4. INTERNET PROTOCOL VERSION 6

IPv4 (Internet Protocol Version 4) [11] was standardized in 1981 when only 200 computers where interconnected. At this time, the defined address length of 32 bits was declared to be sufficient.

Due to the vast increase of computers connected to the Internet, the free IPv4-Addresses are about to be exhausted. This address exhaustion has been anticipated and threatened to have a limiting effect on the growth of the Internet. To prevent this limitation, a solution called IPv6 (Internet Protocol Version 6) was developed and published in 1998 [12]. This protocol extends the addresses to 128 bits, which is currently believed to be sufficient for some time.

The transition from IPv4 to IPv6 is ongoing, but the pace at which the transition is done is varying heavily, depending on the region [13]. However, it may be expected that eventually all nodes connected to the Internet will use IPv6.

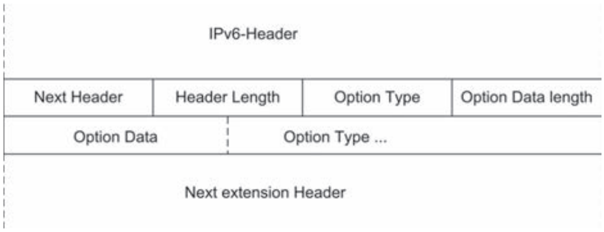
Besides providing a solution for the limited address space under IPv4, further improvements were made by IPv6 [14]. One of these improvements is the extensible header structure of IPv6. It consists of a base IPv6-Header and optional header extensions. This allows including additional transportation information.

A. Hop-by-Hop-Options

The information provided through the Hop-by-Hop-Options must be checked by each node along the route. Through these options, it is possible to pass further parameters and/or restrictions to the nodes processing the packet.

The Extension-Header contains a Next-Header-Field necessary for each IPv6-Extension-Header and a Header-Length-Field, to describe the basic layout. Hereafter an arbitrary number of options may be specified, by inputting a triplet of Options-Type, Options-Data-Length and Option-Data into the header.
The structure of an example Hop-By-Hop-Options-Header is depicted in Figure 3.

FIGURE 3. AN EXAMPLE HOP-BY-HOP-OPTIONS-HEADER



The uppermost three bits of the option type have a special meaning. The third bit defines the options data as unchangeable during transmission if set to 0. The other two bits describe what a node needs to do if the option type is unknown. There are four possible values:

00 – Skip the option
01 – Discard the whole packet
10 – Discard the packet and send ICMP error back
11 – Discard the packet and send ICMP error back if not multicast

Fortunately, the Hop-by-Hop-Options may be declared as mandatory. If a node cannot fulfill a specified option, the packed is dropped an error message is sent back to the previous node.

To ensure that the options are processed prior to the packet contents, the options should be placed directly behind the standard IPv6-Header-Fields. This is also recommended in the IPv6 RFC to restrict processing time in nodes.

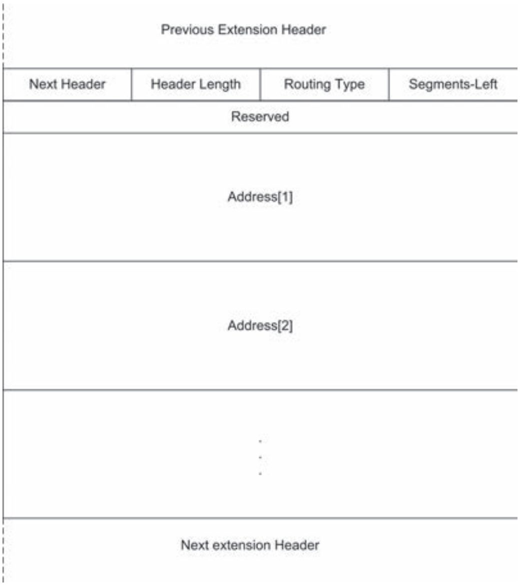
B. Routing-Options

The Routing-Options-Header enables users to specify the route a packet should take. The specified route may be "strict" or "loose".

In the case of a "strict" route, the packet must be forwarded exactly along the nodes specified. If the route is declared "loose", the given route may be considered as a recommendation.

The Routing-Options-Header keeps track of the next target in the route, by providing a counter, which is incremented by each node.An example of a Routing-Options-Header is depicted in Figure 4.

FIGURE 4. AN EXAMPLE OF A ROUTING-OPTIONS-HEADER



The described IPv6-Standard and the improvements made with the standard allowed us to develop a concept that may be integrated directly in the "backbone" of the Internet.

5. NATURAL PRIVACY PRESERVATION PROTOCOL (N3P)

The proposed Natural Privacy Preservation Protocol (N3P) is an extension of IPv6.

The IPv6 specification provides two approaches (cf. section 4) to influence the route selection at the network layer.

One method uses the Routing-Options-Header and is referred to as "Offline Route Selection" (cf. subsection 5.A), while the other method uses the Hop-by-Hop-Options and is called "Online Route Selection" (cf. subsection 5.B).

The offline route selection depends on a "white-list" of trustworthy nodes and needs to obtain this knowledge prior to the sending of data. The online method depends on the correct processing of the Hop-by-Hop-Options in each node, hence changes in the software of the nodes may be necessary. Hardware changes are only needed, if hardware modules to heighten the trustworthiness of a node are considered necessary. In both cases further work regarding the protection and trustworthiness of nodes should be done.

A. Offline Route Selection

The target of the offline route selection is to obtain a route prior to the message transmission, which is verified to satisfy the expected or needed level of privacy and to enforce exactly this route. The Hop-by-Hop-Options of the N3P-Packet are set, but may be omitted. This allows the offline route selection to use nodes that cannot process the Hop-by-Hop-Options, but that are considered as trustworthy by an authority.

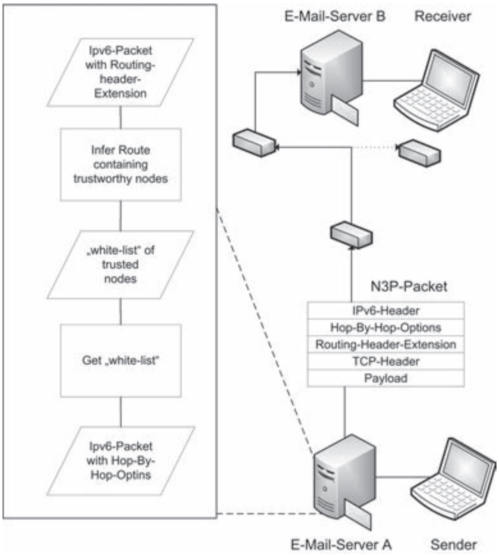
The mechanism can be divided into three major steps.

- First the "white-list" must be acquired.
- Secondly the route must be selected on which the message is to be transmitted.
- Finally the route must be attached to the packet in the IPv6-Routing-Header and the route must be marked as "strict".

The basic steps can be seen in Figure 5.

Acquiring a trustworthy and correct "white-list" is quite complex but crucial. The "white-list" should be adjusted to the required level of confidentiality and is hence communication specific. Moreover, it must be protected against forgery and manipulation. This can be achieved through different solutions, for example digital signatures.

FIGURE 5. OVERVIEW OF THE OFFLINE-ROUTE-SELECTION


E-Mail-Server B
Receiver
Ipv6-Packet with Routing-header-Extension
Infer Route containing trustworthy nodes
„white-list" of trusted nodes
Get „white-list"
Ipv6-Packet with Hop-By-Hop-Optins
N3P-Packet
IPv6-Header
Hop-By-Hop-Options
Routing-Header-Extension
TCP-Header
Payload
E-Mail-Server A
Sender

The route selection can be done in various ways. One simple solution is to “trace route” the target of the packet and check the resulting route against the white-list. However, this solution has the major drawback, that a failed check cannot be handled easily and needs additional mechanisms. Another approach is to obtain a topological view of the network through information provided by present routing protocols e.g. OSPF or EIGRP. This view may be utilised to run a routing algorithm locally and use the information as additional parameters. One example of a routing algorithm would be the Bellman-Ford-Algorithm with an additional confidentially-check for each node. If a node does not fulfil the confidentially requirements it is removed from the topology. After each node is checked, a route can be searched with the original algorithm. Other routing algorithms may also be modified to include the “white-list-checking”.

Since the whole route selection and verification process is done at the sender, there is no need to modify intermediate nodes.

Two difficulties are:

- To obtain a trustworthy and up-to-date white-list
- The handling of node/network failures. As routing is done at the sender only, every node is a single point of failure on the static route.

An efficient solution is to partition the route into segments, where each segment must start and end at a trusted node. This makes the routing faster, as the amount of nodes that must be checked in each step is reduced. Additionally the effect of node failure on the overall routing is reduced.

B. Online Route Selection

If the route is not given prior to the transmission the routing process is called “Online Route Selection”. In this case, the selection of appropriate nodes is not decided prior to the sending of the data and “hard-coded” in the Routing-Header, but is instead done by the nodes along the route, chosen by the protocol specifications. This allows to abandon the usage of “white-lists” that may be difficult to obtain, synchronise and to keep updated.

To decide whether a node is sufficient or not in online route selection, two details must be known: The location of the node - to be able to derive legal implications - and the level of confidentiality a node can guarantee for a packet passed through that node.

While the first information (location) may be observed without the node cooperating, the latter is more complicated to obtain: The nodes involved must implement a method to decide and deliver their level of confidentiality. This implies that either the nodes must be trusted (without node adjustment) or further precautions to ensure the integrity of the method and its results must be taken (With node adjustment).

1. With Node Adjustment

To assess the “trustworthiness” of a node, reliable information about the nodes location must be obtained. Moreover, it must be guaranteed that a node is able to preserve the requested level of confidentiality (in terms of storage, processing, storage time, localisation etc.).
Since this information may not be obtained reliably without the node cooperating, we developed a 5-level confidentiality rating for nodes. Each node implementing the proposed method is assigned a confidentiality level, based on analysing the physical placement (legal issue) and the processing behaviour (information stored, period of time records are kept, data protection, etc.). The node’s level of confidentiality may be considered as a property of the node. A specific level may be demanded in the Hop-by-Hop-Options, declaring the minimum level needed to process the packet.

2. Without Node Adjustment

If the node adjustment is not possible, the option of gathering information about the location from neighboring nodes persists (for example DNS-Look-Up). The legal implications drawn from the physical placement of the node may then be used to derive an approximation of the level of confidentiality.

The DNS-Look-Up and the decision of forwarding the message to another node must be done by the current node. If this is applied recursively and consequently, a route of trusted nodes is selected. However, this implies that each node selected must be able to request the physical or network-based placement of the next node and evaluate its assumed confidentiality.

Independently of whether the confidentiality rating is done with or without node adjustment, the rating expected by the sender/receiver of a packet is placed in the Hop-by-Hop-Options-Field and marked with a type value of 0x84 to declare the options mandatory and unchangeable. The lower bits in the field represent an id of our specific option.

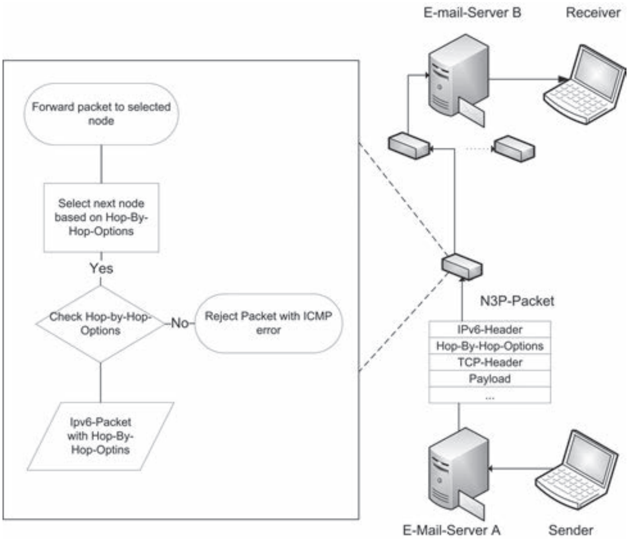
If a node does not fulfil the Hop-by-Hop-Options specified, either the node itself drops the packet (method "with node adjustment") or the current node may not forward the packet to the selected node (method "without node adjustment"). A basic view of the mechanism used by the online route selection can be seen in Figure 6.

The online route selection is more flexible and less restrictive than the offline route selection, however online selection implies larger implementation efforts.

In online selection, the decision of the confidentiality level of a node is crucial. As legal implications may influence confidentiality and depend on a node's location, some of our efforts are to automatically derive a value according to a node's placement. This value shall then be taken into consideration to determine the node's rating.

Other difficulties inherent to the online route selection are that concepts to ensure the trustworthiness of a node need to be implemented and an intelligent route selection procedure must be included to avoid looping.

FIGURE 6. OVERVIEW OF THE ONLINE-ROUTE-SELECTION


E-mail-Server B
Receiver
Forward packet to selected node
Select next node based on Hop-By-Hop-Options
Yes
Check Hop-by-Hop-Options
No
Reject Packet with ICMP error
Ipv6-Packet with Hop-By-Hop-Optins
N3P-Packet
IPv6-Header
Hop-By-Hop-Options
TCP-Header
Payload
...
E-Mail-Server A
Sender

6. CONCLUSION AND OUTLOOK

Due to the faulty association of electronic and postal mail, governmental, entrepreneurial and private risk factors are induced by the misinterpretation of e-mail as a fast, reliable and secure communication medium.

It was shown that this is a misinterpretation in both legal and technical terms. The described exploit arose due to the combination of legal and technical issues. Interestingly, the complicated legal situation is both responsible for the unguarded use of e-mail and at the same time the reason for the implementation of techniques to silently copy and store transferred data. Although the intention is crime prevention and investigation, these techniques may also be adapted and used by other groups for lower purposes. This is especially the case if these groups do not consist of single criminal elements, but may rather be seen as military or paramilitary groups that have considerable influence on their local legislation.

Due to the described legal situation, especially within the EU, it is plausible to expect an increase of attacks on network structures known and demanded to save vulnerable data. Studies evaluating this assumption should be done. It should especially be evaluated if the amount of targeted attacks on infrastructures known to store vulnerable data increased since the integration of the EU Data Retention Directive.

The combination of technical issues and the legal situation in some countries leads to an uncontrollable amount of network nodes that silently may store transmitted data without restrictions. Access to the data is subject to the node's local government and may be legal, even if illegal in the sender's or the receiver's country. Both sender and receiver will not be aware of the fact that a copy of their communication may be processed outside their legal borders.

As copies of communication packets may be kept for an undefined and uncontrollable amount of time and the selected route is unknown, this may also comprise threats for encrypted messages. Encrypted messages may be exposed to surveillance and investigation without time limitations and may be compared with other encrypted/unencrypted messages from the sender.

Our method extends a solid, implemented, standardized and accepted protocol and herewith provides the ability to monitor, influence and control the IP routing. Since the new IPv6 standard is still being introduced, the proposed method may currently be adapted easily.

Two ways of extending/using the IPv6 standard were shown: The Routing-Header and the Hop-by-Hop-Options-Header. This provides the ability to either determine a static route prior to the message transmission or dynamically, e.g. "online" demand that only sufficient nodes may process a message and reporting must be done if the node is insufficient.

Difficulties in the offline/static route selection are to obtain a consistent and trustworthy "white-list" of nodes and to keep this up-to-date during transmission. However, since Internet connections have become more reliable and appropriate authorities exist, this problem may be expected to be solved rapidly. Further problems to investigate are the handling of manipulated nodes (list manipulation, route manipulation, spoofing, DDoS, etc.).

The difficulties arising in the online/dynamic route selection are a bit more complicated and wider:

- It must be ensured that the selected routes eventually allow the delivery of the transmitted messages.
- It must be guaranteed that the nodes either are trustworthy themselves or that trustworthy nodes possess the ability to gather information about other nodes before forwarding packets to them.
- An automated decision of a node's rating based on its location is under development.
- Implementation (hardware or software) of a node's confidentiality level rating method must be done and its reliability must be guaranteed.
- The proposed method should be tested with manipulated nodes to assess the potential effects.

Both the online and offline techniques have challenges, but also provide a unique gain of control to the e-mail routing process. In fact, the proposed concept may easily be transmitted to any type of communication based on IPv6.

Due to the control and feedback given to the user, our concept may be extended to a PET. Our concept entitles the user to influence the routing process and technically enforces the negotiated/expected level of privacy. The concept increases the user's awareness regarding the differences between electronic and postal mail and the resulting implications.

REFERENCES:

[1] Plantronics Inc. (2010). *How we work* [Online] Available: http://www.plantronics.com/us/howwework/

[2] S. Gaw et al.,"Secrecy, Flagging, and Paranoia: Adoption Criteria in Encrypted E-Mail," in Proc. of CHI 2006 Conference on Human Factors in Computing Systems, Montreal, Canada, 2006 © ACM Press, doi: 1-59593-372-7.

[3] T. Jefferson et al., *The Declaration of Independence and the Us Constitution with Bill of Rights & Amendments Plus the Articles of Confederation*. Washington, DC, Bottom of the Hill Publishing, 2010.

[4] J. L. Clerk, *"Charles A. Rehberg v. James V. Paulk," U.S. Court of Appeals for the eleventh circuit*, no. 09-11897, pp. *001-040* Mar, 2010.

[5] S. A. Spiegel, *"United States of America v. Warshak S.," U.S. Cout of Appeals for the sixth circuit*, no. 06-00111, pp. 001-098, Dec, 2010.

[6] Cornell University Law School. (2008, Jan, 8). *18 USC § 2703 – Required disclosure of customer communications or records*. [Online] Available: http://www.law.cornell.edu/uscode/text/18/2703.

[7] European Union, "DIRECTIVE 2006/24/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," *Official Journal of the European Union*, No. L 105, pp. 054-60, Mar, 2006

[8] The Register. (2005, Dec 14). *MEPs vote for mandatory data retention*. [Online] Available: http://www.theregister.co.uk/2005/12/14/eu_data_retention_vote/.

[9] European Commision. (2012, Jan 10). *European Commision Home Affairs*. [Online] Available: http://ec.europa.eu/home-affairs/policies/police/police_data_en.htm.

[10] Irish Times. (2010, May 5). *European cour to rule on storage law*. [Online] Available: http://www.irishtimes.com/newspaper/ireland/2010/0506/1224269793253.html.

[11] Information Sciences Institute University of Southern California. "INTERNET PROTOCOL DARPA INTERNET PROGRAM PROTOCOLSPECIFICATION," Defense Advanced Research Projects Agency, Arlington, RFC 791, 1981.

[12] S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification," The Internet Society, Reston, USA, RFC 2460, 1998.

[13] J. Prévost. (2003. Nov 10). *Deploying and using IPv6*. [Presentation]. Available: http://www.cu.ipv6tf.org/pdf/JP-DeployingIPv6.pdf.

[14] Dittler, H. P. *IPv6 das neue Internet-protokoll Technik – Anwendung –Migration*. 2. ed. Heidelberg, Germany: dpunkt.verlag, 2002