Countering Phishing Threats with Trust-by-Wire in Packet-switched IP Networks – A Conceptual Framework

Stephan Kubisch, Harald Widiger,
Peter Danielis, Jens Schulz, Dirk Timmermann
University of Rostock
Institute of Applied Microelectronics and Computer Engineering
18051 Rostock, Germany
Tel./Fax: +49 (381) 498-7276 / -1187251
E-mail: {stephan.kubisch;harald.widiger}@uni-rostock.de
Web: http://www.imd.uni-rostock.de/networking

Thomas Bahls, Daniel Duchow
Nokia Siemens Networks
Broadband Access Division
17489 Greifswald, Germany
Tel./Fax: +49 (3834) 555-642 / -602
E-mail: {thomas.bahls;daniel.duchow}@nsn.com

***Abstract*—During the last years, the Internet has grown into a mass-medium for communication and information exchange. Millions of people are using the Internet for business and in social life. Users can be reached easily and cost-effectively. Unfortunately the Internet's open structure is the reason for its frequent misuse for illegal and criminal actions such as dissembling phishing attacks. Thus, anti-phishing techniques are needed to recognize potential phishing threats. But mostly these techniques are only of reactive nature, are soon circumvented by expert frauds, or are not efficient enough. This paper describes an anti-phishing framework. A concept for trust management and a mechanism called IPclip are presented. The main idea of IPclip is to guarantee trust-by-wire in packet-switched networks by providing trustworthy location information along with every IP packet. This information is used as supplementary and trustworthy trigger to identify potential phishing threats. Besides, the proposed framework allows for tracing the threat's origin by using a set of location information.**

***Index Terms*—(Anti-)Phishing, Internet Protocol, Internet Security, Trust-by-Wire, Trust Management.**

I. Introduction

"Hackers Tap Bank Web Sites In Unique Phishing Attack"
"Phishing attack plunders Monster.com"
"Fake heart attack headline leads to real phishing attack"
—

Headlines as the ones above can be read in newspapers and Internet news blogs around the world these days. They are all the result of illegal phishing attacks, which are a wide-spread form of cybercrime in the Internet. The term *phishing* derives from the words *password fishing* and *phreaking* (an early form of misusing classical telephone networks). It is one of the modern Internet's Achilles' Heels. The recent formation of the High Level Group on Cybercrime by the International Telecommunicaton Union (ITU) [1] shows that cybercriminality should not be underestimated. As the original Internet has grown from a pure scientific network into a full-blown world-wide information and communication medium [2], the requirements on network infrastructures and provided services have changed radically. Unfortunately, newly discovered loopholes are instantly exploited by malicious minds leading to the emergence of a "dark side" of the Internet. This has—among others—the following reasons:

- The Internet's complexity and therewith the anonymity of users are increasing. Nowadays, black sheeps can hide easily. Decades ago, the Internet was an environment where every party could be considered as a trustworthy entity. But it has developed into a mass-medium today.
- Aged protocols, which have originally *not* been designed for such a large community [3], show shortcomings. Nobody could foresee the backdoors and security risks.
- Another reason is the lack of inherent trust-by-wire in packet-switched networks. This is due to the fact that in circuit-switched networks, e.g., the plain old telephone system or the ISDN network, a fixed line directly references the calling person. Whereas this direct interrelationship is not given in todays packet-switched networks [4]. Current and future access networks and the Internet *are* flavors of packet-switched networks!

According to a recent report [5] analyzing data from July to December of 2006, most phishing attempts (more than 40 percent) originated in the US and more than 80 percent targeted the financial sector. During this period, Symantec's Probe Network "detected a total of 166248 unique phishing messages" and blocked over 1.5 billion messages in total. These numbers dramatically increased in 2007 and, according to the experts, phishers are getting more and more sophisticated. Furthermore, security threats and scams do not only result in (un)countable, financial damage. Reduced or even lost confidence of the mainstream of users in e-mail communication, modern e-services, and the Internet as a whole also follow from suchlike security issues [6]. Thus, to restore confidence, anti-phishing measures must be applied on a global scale.

This paper mainly addresses the third point of the reasons mentioned above. We present a conceptual framework for trust management to enhance the trust-by-wire in packet-switched networks. The so-called IPclip system provides the necessary functionality. We focus on IPclip's application as an anti-phishing mechanism with online-banking as exemplary use case. IPclip allows for detection and prevention of phishing attacks to protect the average Internet user from being "phished". Furthermore, the origin of a phishing attack can be traced by using a tuple of trustworthy location information. Thereby, IPclip does *not* replace existing anti-phishing techniques. It rather provides supplementary triggers.

Section II describes phishing basics. In Section III, we briefly revisit the state-of-the-art in anti-phishing efforts. Section IV introduces the general idea behind the IPclip mechanism. The use of IPclip in an anti-phishing scenario is discussed in Section V. The paper concludes in Section VI.

II. Phishing Basics

Main objectives of phishing attacks are identity theft and obtaining private user data like logins & passwords or credit card numbers by fraud. This information is then either directly misused or sold to third party scammers. The term phishing was coined in the 1990s when hackers stole America Online (AOL) accounts by scamming passwords from unsuspecting AOL users [7]. At that time, phishing attacks were exclusively done by sending faked e-mails in the name of a trustworthy institution asking the recipient to send back passwords or credit card details. Users replied to these e-mails and disclosed sensitive data. Today, phishing belongs to the most critical threats in the Internet and causes substantial financial damage for private users and enterprises. In a report of the Government Accountability Office (GAO) [8], the financial losses are estimated to "$49.3 billion in 2006 for identity theft and $1 billion annually due to phishing". Many more phishing strategies and attack vectors have developed since then. Some are given below:

- E-mail spam is the most wide-spread form to initiate a phishing incident [9]. Various sophisticated techniques have been developed to give spam a trustworthy appearance, to impede spam filters and reputation management systems, and to hide an e-mail's true origin.
- Obfuscated URLs and banner advertisements are presented on either malicious or even on trustworthy websites. Especially URL obfuscation is a prominent technique since many users just skim through the URLs. To embed corrupt content on trustworthy websites, cross site scripting techniques (CSS/XSS) exploit vulnerabilities of poorly encoded websites.
- As Instant Replay Chat (IRC) and Instant Messaging (IM) have become quite popular, phishers exploit the vulnerabilities and also the features of the manifold tools and chat clients.
- During Man-in-the-Middle attacks, the phisher puts himself between a user and a benign server and proxies the communication between them.
- Observation of user behaviour allows phishers to narrow their target group. For instance, users that do click on banners or users that have been cheated already.
- User hosts can be infected with key loggers and screen grabbers—small tools, which may have been attached to an e-mail for example. These tools minute pressed keys or capture parts of the screen and transmit the data directly to the phisher.

III. Common Anti-Phishing Mechanisms

As shown in Section II, phishers have a large number of methods at their disposal. Consequently, there is no single solution capable of combating all attack vectors. However, a mix of security mechanisms can give good protection if the required expert knowledge exists. Generally, the counter-measure can be classified in three levels: client-side, server-side, and enterprise-level. The client-side includes the users' hosts. The server-side includes the businesses' web servers and websites as well as custom applications. The enterprise-level comprises distributed or global technologies and third-party security services. Various filtering mechanisms can be applied on any level to filter e-mails, IPs, or HTTP content. When defining corporate or private security guidelines, it is important to keep strict standards-compliance to not offer any loopholes.

The client-side is most important for anti-phishing measures. Usually, desktop protection technologies like firewalls, anti-virus and anti-spam filters, and spyware detection tools are applied on a client's PC. Although many tools exist, the problem is the vigilance and the lack of expertise of the users. Typical mechanisms are:

- Browser tools, e.g., CallingID Toolbar and Link Advisor [10], which are easy to handle. But the success depends on the report of suspective websites to keep data bases and black lists up-to-date. Actually, existing toolbar mechanisms do not show the desired success [11].
- The format of e-mail should be reduced to a reasonable level. Particularly, HTML functionality should be turned off. HTML e-mails are the source of most phishing attacks.
- Digitally signed e-mails provide basic protection for the sender, the receiver, and the content of the e-mail.

At the server-side, the following measures are common:

- Threats and risks must be communicated to the end users to raise customer awareness with respect to recent and current security issues.
- Strong authentification mechanisms are mandatory to provide mutual trust. Token mechanism as offered by RSA Security, Inc. [12] are used widely.
- Naming conventions for hosts, websites, and URLs should be defined clearly and conveniently.
- The underlying source code of websites, their visual presentation, as well as the page interactivity must be coded properly.

On the enterprise level, companies and ISPs try to protect their customers and internal users. Enterprise solutions are often used in combination with client- and server-side approaches.

- E-mail server authentification mechanisms and signed e-mails are more complex and comprehensive approaches than their pendants on client- and server-side.
- Registrations of enterprise domain names and URLs must be kept up-to-date. Similarly looking alternatives should be checke regularly.
- Gateway services are mostly used to protect the own internal infrastructure by doing inband traffic control. However, it is promising to do outbound traffic control as discussed in [13].

None of the measures mentioned above is a 100% solution. Thus, they are labeled as *best practice*. Generally, it is necessary to handle phishing attacks on a global scale [1], [14], [15]. A first step in this direction was presented at the Internet Engineering Task Force (IETF)-Meeting in Paris in 2005. There, the concept for DomainKeys Identified Mail (DKIM) has been presented [16], [17]. Quite recently, this concept has been realized and launched by Yahoo and Ebay.

More details on the revisited basics in Section II and III are given in [7] for example.

IV. Trust-by-Wire & IPclip in General

The trust-by-wire framework including the IPclip mechanism was developed totally decoupled from potential use cases like the one addressed in this paper. Thus, this section provides a brief overview about the general IPclip mechanism before adapting it to the anti-phishing scenario in Section V. For detailed information on the general IPclip mechanism and its prototypic hardware realization, we refer to [18].

The name IPclip is derived from the CLIP functionality (Calling Line Identification Presentation) in ISDN (Integrated Services Digital Network) telephone networks. CLIP is an optional feature to submit the calling number to the telephonee to present it on, e.g., a display. This way, the callee can identify the caller. In case of packet-switched IP networks, the IP address of a user cannot be treated as equivalent to a fixed line telephone number. The reason is, as already mentioned in the introduction, that an IP address does not necessarily identify a distinct physical line. Furthermore, IP addresses *do not* allow any conclusions on the geographic location of a packet's origin. In contrast, fixed line telephone numbers *do* have a well-defined and known origin. The original idea and the name of the CLIP feature in classical ISDN telephone networks are thus adapted in our trust-by-wire framework for packet-switched IP networks. From a technical perspective, IPclip is a completely novel mechanism and cannot be compared with the classic ISDN CLIP.

A. Why the Internet Protocol and what Kind of Information?

An Internet user and his actual geographic position can be identified with IPclip using a tuple of information consisting of the customer's current IP address and some additional information. As IP addresses do not clearly reference to the users' locations, reliable location information must be included in the additional information. Preferably, standardized data formats should be used for it in order to ensure global interoperability, which is essential in the Internet. Due to its global availability, the GPS (Global Positioning System) data format is used to encode geographic location information [19] at the moment. The sum of all additional information—in the following just specified as location information (LI)—is used for analysis, classification, or stimulation of further actions.

To provide these LI on a global scale, an optional data field is inserted into every IP packet. The reason is that IP is the central protocol in the Internet and the World Wide Web. IP provides end-to-end connectivity between users, service providers, and network nodes in general. Besides, structure and size of optional fields inside IP, so-called IP options, are standardized [20]. This way, the IPclip mechanism is a standard-compliant solution for the delivery of supplementary LI. Every IP-capable device can either analyze and processes IP options or ignore them. But in any case, devices must at least be able to parse and skip IP options for reasons of interoperability. Next to the feature of adding additional LI into packets, the whole mechanism can be configured to remove suchlike IP options. This may be necessary if Internet users do not want to receive or are not allowed to receive sensitive information about the geographic origin of IP traffic. In these cases, the use of IPclip is totally transparent. However, this depends on the particular application.

The new IP option shows the typical TLV structure (Type-Length-Value) as sketched in Figure 1. The TLV structure must be understood by every IP-compliant network device. The type field is divided into a 3-bit field for various flags and a 5-bit IP option number. For prototyping, we have chosen 26 as option number for IPclip as it is not in use otherwise [21]. Length denotes the IP option length including type and length field. The value field of the new IP option contains the IPclip option. Figure 2 shows the structure of an IPclip option. The IPclip type field denotes the kind of information this IPclip option contains, e.g., GPS location information. The 4-bit status field contains flags for trust management. Since only two bits are currently in use (see Table I), the remaing bits are reserved for future extensions. The option information field contains the actual information, which depends on the IPclip type.

The addition of LI including its analysis and verification raises different important questions:

- Which is the place within the network infrastructure where the LI to be added is available?

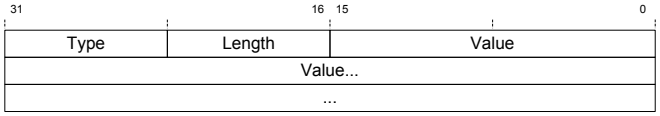

Fig. 1. TLV-structure of an IP option

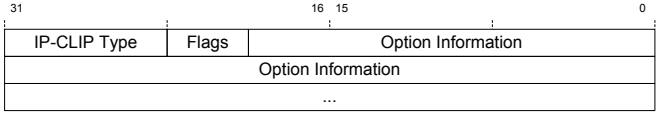

Fig. 2. Structure of an IPclip option inside the value field of an IP option

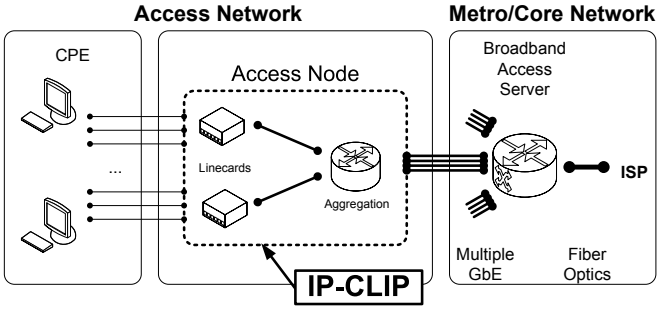

Fig. 3. Network structure with CPEs, access network, and core network.

- Which is the place within the network infrastructure where this LI can be added into IP packets?
- How can a trust relationship and a certain degree of credibility be described and how can it be ensured when analyzing and validating the additional information?

B. IPclip's Position within the Network Infrastructure

Network ingress—also known as access network—is the most reasonable place where LI can be added and verified. Access networks comprise Customer Premises Equipment (CPEs) as well as so-called access nodes like IP DSL Access Multiplexers (IP DSLAMs). Usually, access nodes consist of multiple linecards and an aggregation card. This structure is shown in Figure 3. While aggregation cards manage high-bandwidth interfaces towards the core network, linecards mainly concentrate high numbers of subscribers. Since the paper describes a conceptual framework, the generic term *access node* (AN) is used throughout the paper.

The inherent physical line information, e.g., the port number on the AN, can already be treated as some flavor of LI. Thus, our approach is based on the assumption that LI can be added either by the CPEs (only GPS location information) or by the IPclip mechanism in the ANs (GPS location information *and* access port number *and* access node ID). However, verification and validation of the LI and thereupon taken measures are solely done in the ANs. The reason for doing so is that CPEs are typically not considered as trustworthy network elements by network carriers and service providers. CPEs are usually not within the carriers' management domains. By contrast, ANs are part of the access network and thus within a carrier's management domain. A tuple of information available in ANs is used as precise LI to identify and locate an Internet user:

- the geographic location of the access node
- the access port number the user is connected to
- the access node ID

That is why the IPclip functionality is implemented in the ANs as highlighted in Figure 3.

C. Trust Management with IPclip

As already mentioned in the beginning, phishing threats shall be detected using a trustworthy LI. But how can the required level of trustability and credibility be guaranteed? The problem is within the CPEs, which are mostly configured by ordinary

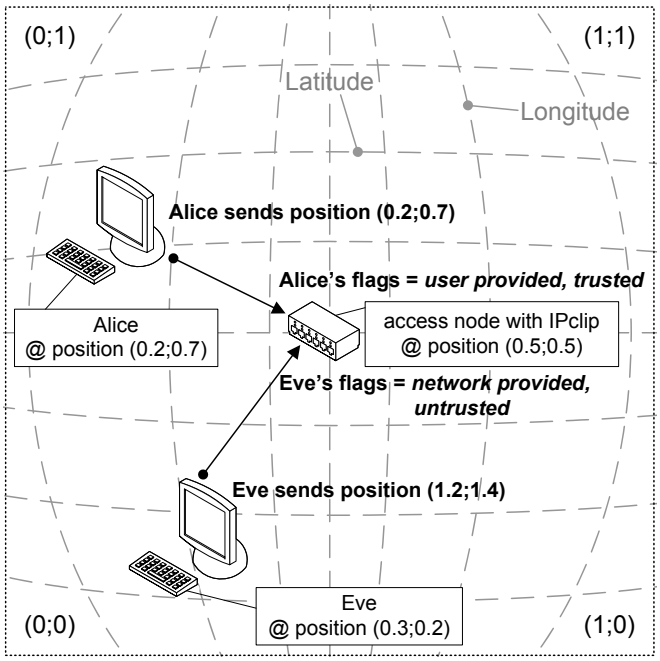

Fig. 4. Verification of the location information. The square's edge length (= SCA) and the hosts' positions have been normalized ($0 \leftrightarrow 1$). In a realistic scenario, they are given in GPS coordinates (longitude & latitude).

Internet users with lack of expertise [22]. Internet users may *unintentionally* mis-configure their CPEs and provide wrong LI. But frauds and scammers may also *intentionally* provide incorrect LI to pretend a different origin, e.g., in case of a faked phishing website. Because of that, CPEs cannot be considered as trustworthy entities. A user provided IPclip option and the LI must thus be verified and checked for plausibility. Optionally, the respective access port number is added to the user provided LI.

The IPclip functionality can detect incorrect LI. Therefore, it uses the given fact that only customers can be connected to an AN, which are within a *reasonable geographic distance* relative to that AN. We call this geographic distance the *subscriber catchment area* (SCA) of the respective AN. The SCA is a configurable parameter and defined as the egde length of a square with the AN being located in its center point. Figure 4 illustrates this setting with normalized coordinates. Two user hosts (Alice and Eve) are located at (0.2;0.7) and (0.3;0.2) respectively. The plausibility of the CPE provided LI is determined by a comparison with the inherent geographic location of the AN (0.5;0.5) with respect to the SCA. If the comparison indicates that IP packets carry incorrect CPE provided LI—maybe due to mobility, misconfiguration, or intentional manipulation—the existing but incorrect LI will be replaced with the inherent LI of the AN. In case that the CPE provides no LI at all, the IPclip mechanism will insert the AN's inherent geographic location as new IP option with IPclip location information into these IP packets. In any case, IP packets will carry LI about their origin when leaving the IPclip-capable AN—at least with the precision of the AN's

TABLE I
INTERPRETATION OF IPCLIP'S FLAGS WITH RESPECT TO TRUSTABILITY

Value	Source / Credibility	Option Description
00	user provided / untrusted	A user provided IPclip option did not pass verification.
01	user provided / trusted	A user provided IPclip option did pass verification.
10	network provided / untrusted	A user provided IPclip option did not pass verification. It is replaced in the AN.
11	network provided / trusted	The AN has added a new IPclip option.

TABLE II
INTERPRETATION OF IPCLIP'S FLAGS IN AN ANTI-PHISHING SCENARIO

Value	Source / Credibility	Option Description
00	user provided / untrusted	The LI was provided by the originator of the website. But it is not trustworthy. Block this website!
01	user provided / trusted	The bank has inserted the location information. It is trustworthy. Proceed with this website.
10	network provided / untrusted	Incorrect LI was detected and replaced with IPclip's own LI. Block this website!
11	network provided / trusted	No LI has been provided. IPclip inserted its own LI. Block this website!

geographic location, the port number, and the access node ID or at best with the exact and correct CPE provided LI.

For trust management, special status flags are set during the IPclip verification and validation process. This simple approach differs from typical reputation management systems as reviewed in [23]. These flags give information about the credibility of the LI on the IP level. They are used for control and management but can also be used as triggers for further actions on the application level. Currently, two flags are used, which give conclusions on the origin and on the correctness of the LI. The trust relationship is preserved by these flags at any time since they are assigned in the network carrier's management domain. As a central part of the IPclip system, the naming convention for these flags has been adapted to the commonly used lingo in the area of communication technology. Table I briefly summarizes the interpretation of the status flags:

User provided, trusted: The LI has been provided by the user/CPE and has been found correct and plausible during verification (Alice in Figure 4).

User provided, untrusted: The LI has been provided by the user/CPE. But it did not pass the verification procedures.

Network provided, untrusted: The LI has firstly been provided by the user/CPE but did not pass verification. Furthermore, the incorrect LI has been overwritten with the AN's inherent LI (Eve in Figure 4).

Network provided, trusted: The IP packets did not carry any user/CPE provided LI at all. The LI has been provided by the IPclip mechanism in an AN.

To conclude the overview on the IPclip system, its main tasks are summarized below:

- LI needs to be inserted into *every* IP packet using the IP option format—either by the CPEs or by IPclip.
- User provided LI must be detected and validated. Existing information will be overwritten if necessary.
- Status flags need to be assigned for trust management.
- Optionally, IPclip location information can be removed from IP packets.

V. AN ANTI-PHISHING FRAMEWORK USING IPCLIP

Anti-phishing techniques try to analyze and filter contents, addresses, and the behaviour of, e.g., suspicious websites or dubious e-mails. But all information that is useful for analysis and recognition of potential threats is within manipulation reach of phishers. Hence, typical anti-phishing efforts as summarized in Section III are just reactive. Furthermore, current countermeasures mostly represent some flavor of *inband traffic control* and phishers can take counter-countermeasures to annihilate anti-phishing efforts. Instead, IPclip provides trustable information and triggers on the IP level, which are out of the scammers' reach. The LI provided by IPclip is a piece of information that cannot be circumvented or manipulated. From an ISP's or network carrier's point of view, this is some kind of *outband traffic control* as discussed in [13].

A. Use Case 1 – Public Location Information

Using the trust-by-wire approach as an anti-phishing measure shall be explained in more detail for an online banking service: During a phishing attack, e.g., initiated by a spam e-mail, a phisher pretends to be a trustworthy financial institution—a bank. The goal of the attack is to thieve sensitive information like login data and transaction numbers (TANs) of the victim's bank account. To get that information, the potential victim is given a modified or obfuscated hyperlink to a deceptive website, which resembles the original website of the bank. The user believes to be in a secure area and discloses sensitive data, which is logged and misused by the attacker.

IPclip can be used to prevent such an attack by processing the extra LI and flags in the IP packets. What does that mean for a phishing attack? If a bank publishes information about the geographic location of its own web server or IT infrastructure, any initiator of a phishing attack pretending to be the bank would have to have exactly this LI included in his IP traffic. If now a phisher pretends to have that bank's LI, the validation procedures of IPclip would recognize incorrect information (see Section IV-C). In this case, the information is replaced with the AN's inherent LI and the status flags are set to network provided and untrusted. With these information, the victim's browser recognizes that the website that is currently accessed is not the bank's original website. In this scenario, the status flags are interpreted as given in Table II. Only if the LI is validated as user provided and trusted, the user should proceed with that website. Otherwise, the website should be blocked by the

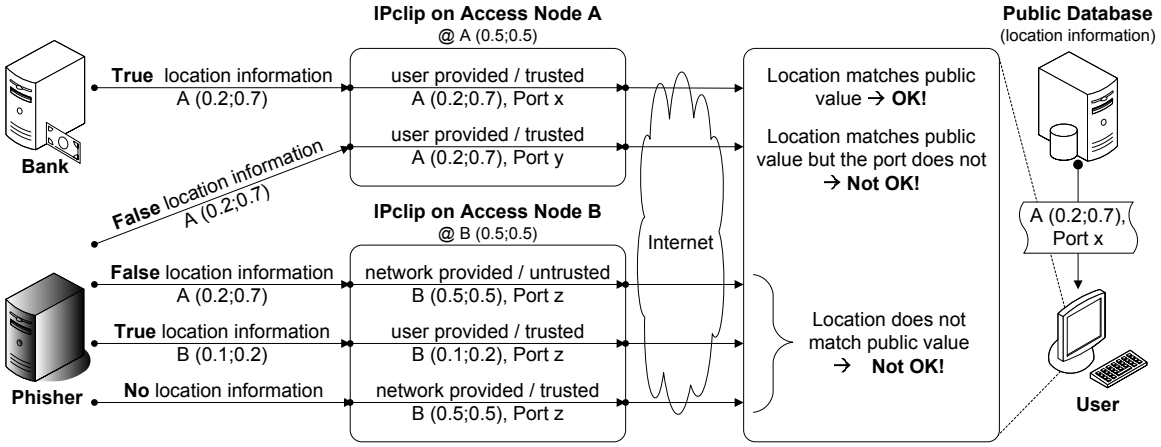

Fig. 5. Anti-phishing use case with plain text location information. Normalized coordinates are used with respect to access node A's & B's SCA (see Figure 4).

browser or a clear warning should open up. To be sure about the website's origin, the LI has to be checked. That is possible by making the LI of the bank's website publicly available in a dedicated database. The user's browser can then compare the LI of the respective IP packets with the bank's public LI in the database. In case the information is correct, users can be sure to be connected to the benign and authentic website. If a bank does not provide any LI for any reason, IPclip inserts its inherent trusted LI. However, trustworthy websites should *always* provide valid LI.

Figure 5 demonstrates the verification mechanism and how the flags are set for different eventualities. IPclip is located in the ANs *A* and *B* at the geographic positions *A*(0.5;0.5) and *B*(0.5;0.5) in the center of their particular SCA square (the GPS coordinates have been normalized, see Figure 4). The bank server is located at position *A*(0.2;0.7). Figure 5 also shows the different options a phisher has to provide LI. The phishing host (shown in black) can be connected to either the same AN (*A*) or a different AN (*B*) with the latter being the usual case. The bank inserts its LI *A*(0.2;0.7) into every IP packet. The IPclip functionality verifies this LI using the SCA of AN *A*. The bank's LI is plausible and the flags are set to user provided and trusted. Additionally, the access port number is added to the existing LI. Basically, a phisher has now the following options in such an IPclip-managed environment:

Provide no LI: Whether or not a phisher is connected to the same AN, IPclip inserts the ANs inherent LI plus port number and sets the flags to network provided. But as mentioned above, trustworthy websites should always provide valid LI.

Provide the true LI: Whether or not a phisher is connected to the same AN, IPclip tags the LI as user provided and trusted. But the LI does not match the bank's public LI.

Provide false LI or the bank's LI: In case a phisher knows the bank's LI (it is public), he pretends to be the bank and sets his LI to *A*(0.2;0.7). If the phisher connects to the same AN like the bank, IPclip would set the flags to user provided and trusted because the provided LI appears plausible with respect to the SCA. Additionally, IPclip adds the access port number to the existing LI. But the user host compares the public LI with the IPclip LI and detects a mismatch regarding the access port numbers. This is to be interpreted as a security risk. If the phishing host connects to a different AN than the bank's server, IPclip detects wrong location information and sets the flags to network provided and untrusted.

B. Use Case 2 – Encrypted Public Location Information

In contrast to the use case discussed above, there are reasons *not* to publish a bank's LI in "plain text" format. The geographic location of a bank's network access points and IT infrastructure should not be disclosed! Financial institutes are not willing to publicize the geographic location of their IT infrastructure as the use case in Figure 5 illustrates. By encrypting the plain text LI, e.g., using some flavor of hashing like MD5 or other algorithms, that would not be an issue any more. The bank still inserts plain text LI into IP packets. But now, IPclip computes the hash value for the provided LI and replaces the existing information with its hashed pendant and the access port number. Thereby, the access port number might also be included in the encryption process. User provided encrypted LI must not be allowed! The encryption is only done by IPclip in the AN. The publicly available LI of the bank's server is only given in an encrypted style—irreversibility is mandatory. This way, the true location of the bank's infrastructure remains secret but the same level of security and trust is given.

Figure 6 illustrates this specific use case. When the bank provides its LI (X), IPclip hashes it (HASH_X) and adds the access port number. Each user compares that LI-tuple with the values given by the public database. The user thus verifies the origin and trustworthiness of the communication partner. Again, a potential phisher has only the following choices, which are similar to the first use case:

Provide no LI: As a trustworthy institution should always provide LI, this is no option for a phisher independent of the AN he is connected to. IPclip inserts its own LI in form of a hash value (HASH_IPclip) and sets the flags to network provided and trusted. HASH_IPclip does not match HASH_X.

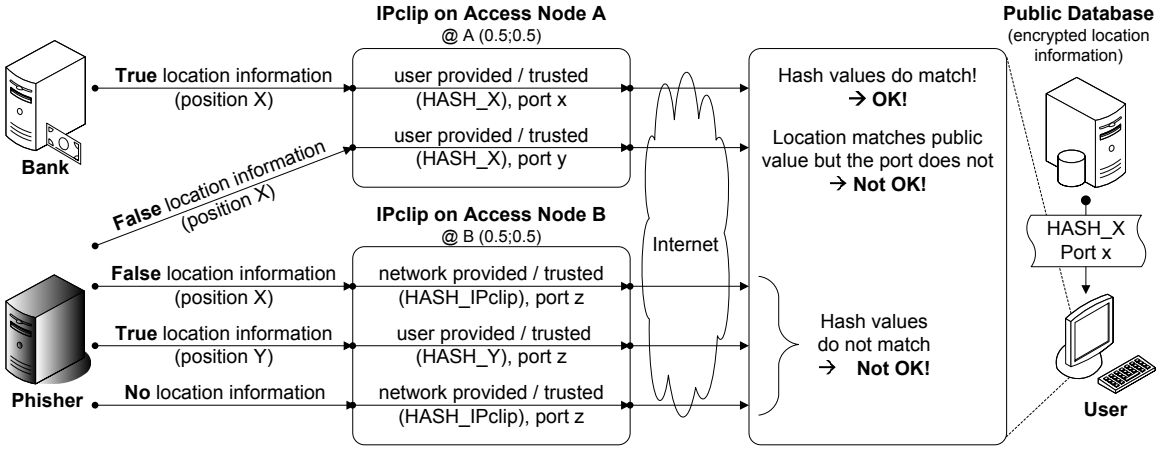

Fig. 6. Anti-phishing use case with hashed or encrypted location information.

Provide an encrypted LI: For a user host, it is not allowed to insert encrypted LI.

Provide the true LI: IPclip computes the hash value for the provided LI (HASH_Y) and replaces the provided plain text LI. The flags are set to user provided and trusted. But the hash value differs from the bank's public hash value (HASH_X).

Provide false or the bank's LI: The phisher cannot present false LI to pretend to be the bank's host because this LI is not known to him. It is publicly available but only in an encrypted format, from which the original LI cannot be recomputed. However, assuming that the phisher is aware of the bank's plain text LI and is connected to the same AN, IPclip would tag the user provide LI as trustworthy. But like in use case 1, the difference in the access port numbers is the crucial trigger.

In any of the circumstances mentioned in the use cases 1 and 2, user hosts are aware of the trustability and the geographic origin of the hosts they are communicating with (bank website or phisher). Only if the provided LI is both user provided and trusted and the access port numbers match, a website is not blocked. Thus, phishing attempts can be inhibited. Thereby, IPclip is an additional and first of all an independent trigger, which can support existing anti-phishing measurements. Additionally, it is compatible to other security mechanisms like DKIM or the Encapsulating Security Payload (ESP) protocol of the IPsec framework.

Various alternatives to plain text LI exist as discussed in Section V-A. We exemplarily proposed the use of MD5 hashes, which is feasible without more ado with the IPclip mechanism. But since IPclip options can serve as a generic container, other triggers, e.g., token-based mechanisms as mentioned in Section III, might also be a good solution. These tokens provide inherent automatic validation and are already widely used for user authentification—but in the discussed use cases, they would authenticate the bank's website.

C. Tracing Phishers

IPclip-enabled packet-switched networks provide another important feature: tracing the phisher's origin! The provided LI in the IP packets can also be exploited to find the originating host and probably the phisher himself. IPclip location information cannot be fiddled. Thus, the trustable information leads to the starting point of the phishing attempt. In the worst case, this is just a trojaned host. In the best case it is the scammer himself. If no or false LI has been provided by a phisher, the trace leads at least to the site of the AN and the access port the malicious host is connected to. Starting at that point, pinpointing the exact location of the phishing host might be possible as well. Locating the AN and the access port is also possible when using encrypted LI as IPclip can insert the access port number and node ID into the option next to the encrypted LI. A promising approach to catch and trace phishers are so-called honeypots or honeynets as discussed in [24]. In this case, prepared and purpose-built networks and hosts attract phishing e-mails—besides a multitude of other threats and malware. These honeypots can be used to collect information on phishing threats, to extract and analyze IPclip location information, and to trace the threats origin. But to guarantee this favorable avenue of the trust-by-wire framework as well as to consolidate the operation of the sceneries illustrated above, some requirements and constraints need to be taken into account:

Firstly, the existence of an IPclip-capable IP stack is necessary in those network elements and end-hosts, which make use of the IPclip LI and the flags. Other network elements do not need to have an IPclip-capable IP stack, since standard-compliant IP options must at least be recognized and skipped.

Secondly, a fully IPclip-terminated domain is mandatory. Already a single access node without any IPclip functionality uncloses a risky loophole in the network infrastructure. IP packets with manipulated LI and even fiddled flags can be injected into the network without being validated by a trustworthy IPclip instance. Thus, the presence of IPclip at all access nodes is obligatory. A practicable IPclip domain would be a single self-contained provider network, for example.

Thirdly, legal questions on the availability, the analysis, as well as the storage of sensitive information like the geographic position of Internet users do also arise. But they are out of the

scope of this paper. Moreover, these questions are the same as are already discussed in other areas dealing with similarly sensitive, private information.

VI. Conclusions

The paper discussed a conceptual framework to tighten measures against phishing frauds. A trust-by-wire concept and the IPclip mechanism were briefly recapitulated. Trustworthy triggers for trust management are provided using a flavor of location-based information. This mechanism was then discussed with respect to an anti-phishing scenario. The first use case in Section V-A utilized plain text, public LI to emblematize the approach whereas the second use case in Section V-B described a more secure alternative using encrypted, public LI.

As the outlined anti-phishing use cases illustrated, phishers are forced into a position with only little "elbowroom" in an IPclip-managed network due to the following reasons:

- The additional information cannot be circumvented by phishers since IPclip is located within the management domain of the network carriers and ISPs.
- On the one hand, IPclip allows for detection and prevention of phishing attempts. On the other hand, the LI inside the IPclip option allows for tracing the geographic origin of the phishing attack with serviceable accuracy.
- Phishing and other cybercrimes are strongly motivated by the relatively little effort and the very short time needed to generate money. Legal measures cannot change that fact and—as has been proven over the last month and years—did not change that fact. But the motivation for phishing can be decreased with the framework presented in this paper. Because, from a technical point of view, phishers are now in need to react.

The proposed framework can be used on a stand-alone basis or can support existing filtering and analysis tools with independent triggers. It is furthermore compatible to orthogonal measures like DKIM. In [1], the ITU's roadmap especially seeks for *global* frameworks to suppress fraudulent phishing and other cybercrimes. Regional efforts in that area do not match up with the borderless and open nature of the Internet. Besides, the real potential of the trust-by-wire framework and IPclip can only be exploited when both are applied on a global scale. Loopholes may otherwise exist, which can in turn be exploited by malicious individuals. Thus, this conceptual framework is a small step in the ITU's direction.

Currently, the framework is discussed for an IPv4 environs. But IPv6 will be the dominating protocol in the prospective Internet. Future work will thus focus on the adaptation of the trust-by-wire idea and the IPclip functionality to IPv6 environments. Furthermore, a hardware prototype is currently set up for an FPGA development board. The target platform is an FPGA inside the ANs. Line rates of several gigabit per second must be processed.

Acknowledgement

We would like to thank the Broadband Access Division of Nokia Siemens Networks in Greifswald, Germany for their inspiration and continued support in this project. This work is partly granted by Nokia Siemens Networks as well as the 4th Priority Research Program on Information- and Communication Technologies, Mecklenburg-Vorpommern, Germany.

References

[1] International Telecommunicaton Union, High Level Group on Cybercrime, "ITU Global Cybersecurity Agenda," September 2007. [Online]. Available: http://www.itu.int

[2] L. Kleinrock, "An Internet Vision: The Invisible Global Infrastructure," *Ad Hoc Networks*, vol. 1, no. 1, pp. 3–11, 2003.

[3] ——, "The Internet Rules of Engagement: Then and Now," *Technology in Society – Technology and Science Entering the 21st Century*, vol. 26, no. 2-3, pp. 193–207, 2004.

[4] kc claffy, S. D. Meinrath, and S. O. Bradner, "The (un)Economic Internet," *IEEE Internet Computing*, vol. 11, no. 3, pp. 53–58, May-June 2007.

[5] Symantec Security Response & Business Intelligence, *Symantec Internet Security Threat Report – Volume XII*, September 2007. [Online]. Available: http://www.symantec.com

[6] D. Fallows, "Spam – How It Is Hurting Email and Degrading Life on the Internet," PEW Internet & American Life Project, Tech. Rep., October 2003. [Online]. Available: http://www.pewinternet.org

[7] G. Ollmann, "The Phishing Guide – Understanding and Preventing Phishing Attacks," White Paper, September 2004, NGS Next Generation Security Software Ltd. [Online]. Available: http://www.ngsconsulting.com

[8] United States Government Accountability Office (GAO), "CYBERCRIME – Public and Private Entities Face Challenges in Addressing Cyber Threats," Report to Congressional Requesters, June 2007, GAO-07-705. [Online]. Available: http://www.gao.gov

[9] N. Leavitt, "Vendors Fight Spam's Sudden Rise," *IEEE Computer*, vol. 40, no. 3, pp. 16–19, March 2007.

[10] CallingID, "Why you need Calling ID," White Paper, March 2005. [Online]. Available: http://callingid.com

[11] L. Cranor, S. Egelman, J. Hong, and Y. Zhang, "Phinding Phish: An Evaluation of Anti-Phishing Toolbars," Carnegie Mellon University, Tech. Rep. CMU-CyLab-06-018, November 2006.

[12] RSA Security Inc., "SecurID." [Online]. Available: http://www.rsa.com

[13] M. Parameswaran, X. Zhao, A. B. Whinston, and F. Fang, "Reengineering the Internet for Better Security," *IEEE Computer*, vol. 40, no. 1, pp. 40–44, January 2007.

[14] Symantec Corporation, *Phish Report Network*. [Online]. Available: http://www.phishreport.net

[15] Anti-Phishing Working Group, *Phishing Activity Trends*, June 2007. [Online]. Available: http://www.antiphishing.org

[16] E. Allman, J. C. M. Delany, M. Libbey, J. Fenton, and M. Thomas, "Domainkeys Identified Mail (DKIM) Signatures," RFC 4871, May 2007.

[17] D. Crocker, "DomainKeys Identified Mail (DKIM)." [Online]. Available: http://www.dkim.org

[18] H. Widiger, S. Kubisch, P. Danielis, J. Schulz, D. Timmermann, D. Duchow, and T. Bahls, "Trust-by-Wire in Packet-switched Networks: Calling Line Identification Presentation for IP," in *1st ITU-T Kaleidoscope Conference – Innovations in NGN*, Geneva, Switzerland, May 2008, submitted.

[19] National Marine Electronics Association (NMEA), "NMEA 0183 Standard," January 2002. [Online]. Available: http://www.nmea.de

[20] Information Sciences Institute, University of Southern California, "Internet Protocol Specification," RFC 791, September 1981.

[21] Internet Assigned Numbers Authority, "IP Option Numbers," February 2007. [Online]. Available: http://www.iana.org

[22] S. Gajek, A.-R. Sadeghi, C. Stueble, and M. Winandy, "Compartmented security for browsers – or how to thwart a phisher with trusted computing," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security*, Vienna, Austria, April 2007.

[23] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, "Reputation Management Survey," in *Proceedings of the 2nd International Conference on Availability, Reliability and Security*, Vienna, Austria, April 2007.

[24] The Honeynet Project, "Know Your Enemy: Honeynets," White Paper, May 2006. [Online]. Available: http://www.honeynet.org