Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 7093642, 10 pages
http://dx.doi.org/10.1155/2016/7093642

Research Article

Business Information Exchange System with Security, Privacy, and Anonymity

Sead Muftic, Nazri bin Abdullah, and Ioannis Kounelis

SETECS, Inc., Rockville, MD 20852, USA

Correspondence should be addressed to Sead Muftic; sead.muftic@setecs.com

Received 30 September 2015; Revised 3 February 2016; Accepted 16 February 2016

Academic Editor: Bo Meng

Business Information Exchange is an Internet Secure Portal for secure management, distribution, sharing, and use of business e-mails, documents, and messages. It has three applications supporting three major types of information exchange systems: secure e-mail, secure instant messaging, and secure sharing of business documents. In addition to standard security services for e-mail letters, which are also applied to instant messages and documents, the system provides innovative features of privacy and full anonymity of users and their locations, actions, transactions, and exchanged resources. In this paper we describe design, implementation, and use of the system.

1. Introduction: Problems and Motivations

The research results described in this paper address the issues of *security*, *privacy*, and *anonymity* of users and their transactions when using Internet applications. One of the most popular uses of Internet is *exchange of information*—e-mail letters, documents, files, and/or instant messages. As such, the resources of these IT systems are under continuous attacks, from illegal users—hackers—as well as from regular application services providers, which perform tracking and profiling of users. At the moment, there are some individual "point solutions" for some of the indicated problems—protection of e-mail letters, files, and instant messages. But, to the best of our knowledge, there is no complete, comprehensive, and integrated solution for these problems.

These are the motives for our research and development results, described in this paper. Contrary to other existing solutions, our system has several important benefits: (1) security services for the three applications are integrated as they use the same security credentials; (2) the system is implemented as Web Portal, so in the background it is connected to existing Web-based mail systems (Gmail, Yahoo, Hotmail, and Outlook); and (3) the system uses strong cryptographic algorithms, standardized by NIST. Significant features are that the system is easy to install, easy to use, and easy to extend.

It effectively solves various problems of security, privacy, and also anonymity, both for *private users* and also for *corporate users*.

2. Related Work

In this section, the current situation with Internet security, privacy, and anonymity is reviewed and analyzed. General conclusion and a broad consensus is that today all three are lacking, causing serious problems when using the Internet for transactions that require some of these properties [1].

2.1. Internet Security Problems. The Internet is used today for many different purposes but it is increasingly used for exchange of all types of messages, documents, photos, e-mail letters, and so forth. Examples of such popular applications include e-mail, instant messaging mobile applications, banking websites, social media sites, various commercial websites, and web servers with information pages.

With all of these capabilities and features the Internet is used today for important personal and business transactions, handling sensitive and confidential data, and sharing documents and information of high sensitivity and value. Many Internet information exchange sites and applications are used by individuals to handle personal data, but more and more

are used by businesses to display, distribute, and share their information. This makes individuals, for privacy and security, and also businesses, for confidentiality and authorization, more and more dependent on the Internet to support their important transactions and handle sensitive personal and business data of high significance and value.

Unfortunately, in parallel with this trend of high and critical dependencies on the Internet environment, its websites, data, and transactions, is an exponential increase in illegal activities on the Internet. Typical threats that previously involved mostly viruses and malware targeting users' PCs have now evolved into far more serious problems of criminal acts, such as thefts of valuable information, business documents, financial and bankcard data, and personal data. There are numerous examples of large-scale penetrations into business systems, thefts of corporate and personal data, ransom actions, blackmailing companies, and destruction of entire websites.

Such incidents are the main reason why the World Economic Forum has declared Internet crime to be the second most serious international problem, immediately after international conflicts [2].

Internet security is very broad area, so it is not so simple to refer to research results contributing to the current outstanding problems. But, since all applications described in this paper store their data in databases, Internet security is analyzed with respect to research contributions in that IT area.

The first ideas for protection of data in databases appeared in [3, 4]. Both papers suggested solutions only for data confidentiality and data integrity. Reference [5] considers primarily management of secret keys for database encryption. The solution closest to the ideas from this paper is described in [6]. The author describes use of cryptography at different database levels, use of combined secret key and public key cryptography, and user authentication based on several alternative protocols. However, the author himself indicates certain limitations of the proposed solution: *(a) it only protects against a narrow range of threats, namely, media theft and storage system attacks, and (b) the solution provides block-level encryption; it does not give the enterprise the ability to encrypt data within an application or database at the field level. Consequently, one can encrypt an entire database, but not specific information housed within the database*.

Based on all of these and many other examples, there is a general consensus about the important need to introduce some solution to the growing problem of illegal and destructive activities on the Internet, whether performed by hackers or regular Internet users and websites.

This paper introduces one possible solution with the potential to solve some of the current serious Internet security problems. Significant features, advantages, and differences with existing systems are that the system described in this paper is based on all relevant Internet security standards, it is applicable to existing e-mail systems, it uses strong cryptography, and it is interoperable with other similar systems.

2.2. Internet Privacy Problems. Another type of serious problem for Internet environments and transactions is the invasion of *users' privacy*. Many websites today require users to register their personal data before they perform some business transaction or use some commercial services. Payment sites, for example, require financial, bankcard, and other sensitive information.

Besides such explicit requests for users' personal data, nearly all websites, in order to provide any service to their visitors, require users' browsers to accept *cookies*. Most of the popular browsers have an option to reject cookies, but when that feature is used many websites will not function correctly. Involuntary acceptance of cookies and their use for tracking user locations and actions is today standard practice and even mandatory at many websites.

Even worse, these cookies are used by all other Web servers connected in an advertising network. Today, advertising networks of various companies place multiple cookies in users' browser during a single session. Later, they share users' data for their commercial benefit, almost always without user consent, sometimes even without user knowledge.

These intrusive technologies are becoming more and more sophisticated, and worse and worse for users. Companies are working on and placing "sophisticated" cookies into their pages that cannot even be detected. Using such technologies, users are tracked, profiled, and exposed to unwanted messages and advertising campaigns without any option to avoid such practices. There are many recent innovative ideas to enhance privacy of users by introducing new and innovative concepts [7] or "community applications" based on innovative principles and protocols [8].

Research on privacy of users and applications is just at its initial phase. Some papers confuse privacy with anonymity. Since our paper suggests providing privacy for users based on the concept of proxy servers, we analyze some of the research papers dealing with proxy servers.

The paper by Tsai et al. from Chinese Culture University of Taipei, Taiwan, describes real-time website security protection mechanism based on the concept of proxy [9]. Users transmit information to the social networking through proxy. The proxy detects and determines security threats of the social networking website, including web-based malware, phishing websites, and malicious connections. The proposed idea is integration with the commercial protection software and online vulnerabilities scanning services into a single security module. It simultaneously executes webpage security threat scans and sends the result to the client. However, their proxy is designed and implemented only for scanning the threats from websites visited by the user. The user has a choice to continue accessing the website when threat's information has been exposed. The implementation shows that (a) the proxy is dealing more with threat scanning rather than protection of user identities or profiles; (b) the analysis of threats has been tested only within the functionality of Facebook application; (c) there are no specific security elements within the proxy to protect user identities when accessing visiting sites.

A group of researchers from University of California and Brigham Young University [10] introduced a "Delegate,"

a proxy-based architecture for secure websites access from untrusted machines. Delegate is designed in the context of untrusted machine security vulnerabilities, such as key logging, password sniffing, shoulder surfing, and session hijacking. The objectives of the architecture are as follows: (a) authenticate users who access web service providers from untrusted machines with temporary credentials in order to avoid being manipulated in the future; (b) detect and prevent session hijacking in order to stop malware to perform unauthorized transactions while users perform their regular operations; (c) limit the scope of potential damage by reducing the attack surface while user is accessing web from an untrusted machine; (d) minimize modifications required by a web server or a user in order to deploy the system. Overall, the architecture of the Delegate is concerned only with confidentiality of user information, but not providing user privacy when they are online on the Internet. It has still several shortcomings in terms of trustworthiness of proxy, as it does not apply any trust framework, such as PKI and Trusted Computing. Without use of public key cryptography it is very difficult to enforce user control and consent, including privacy of users and their data. As clearly described above, the solution in this paper addresses certain aspects of security and not privacy of users.

Wu and Huang from Zhejiang University of China presented a "*Proxy-Based Web Services Security*" that implements authentication based on PKI and authorization based on Privilege Management Infrastructure (PMI) [11]. However, the concept of the proxy they introduced is not an independent third party, but it is a service located in both client and the server. The service captures both HTTP requests and response messages and then extracts SOAP messages from the HTTP message body. SOAP messages are encrypted, signed, authenticated, and authorized by the service provider in each client and server machine. User can customize their security-related parameters (e.g., encryption and signature methods and public and private keys) using the GUI tool. The architecture does not describe user certificates, where/how they are generated, key storage, or identity management.

A journal paper titled A Proxy-Based Security Architecture for Internet Applications in an Extranet Environment authored by Dowling and Keating proposed relatively similar approach of proxy-based security as what we present in this paper [12]. The major components of their architecture are (a) proxy-based security services and (b) advanced authorization and access controls. Security proxies are deployed at client and server sites to filter networked application's communications for vulnerability scanning. They use standard digital certificates, such as X.509 Public Key Certificate (PKC), to securely bind a set of access privileges to an identity when single identity is accessing different resources. However, the Certification Authority (CA) Server in the proxy is used in offline mode so real-time validation of certificates, especially using Certificate Revocation Lists (CRLs), is not possible. The operation performed by CA Server, such as issuing, revoking, and updating CRLs, is performed manually. This implies that there are time gaps in the process of managing certificates which introduces time periods when the system is vulnerable to impersonations. Certificate trust parameters (certificate policies) are stored in local security databases maintained at the client and server proxy sites which contradicts well established practice and recommendations that these policies are maintained and enforced by special type of CA Servers, usually called Policy CA Servers.

The concept of the proxy, which at first appears equivalent to the architecture described in this paper, is described in [13, 14]. But the concept of the proxy in [13] is completely different from the secure proxy described in this paper. Their proxy plays active role in reencrypting user ciphertexts from one to another key. With this approach users must put the complete trust in the proxy, so user privacy cannot be provided and user documents are visible to the proxy. The functionality of the proxy described in [14] is different from [13], but in essence it is also trusted server. Secure proxy from this paper does not need user's trust as it has no access to user's identity data (encrypted in DB tables) and to user's security credentials (encrypted with user's password or asymmetric public key).

Although some reports and research papers try to objectively analyze pro and con aspects of the sharing of private data, they generally acknowledge that consumers do not want to share personal data without being informed and giving consent [15]. In 2005, a CBS News survey found that most Americans believed that their privacy was under "serious threat." Similarly, in 2009, a survey by Turow found that a large majority of Americans resist tailored advertising [16]. In combination with many resolutions by the European Union, all this indicates that there is a serious need to address the *privacy* of individuals and companies on the Internet when performing casual browsing as well as important business transactions.

Therefore, another innovative idea described in this paper, besides Internet security, is a solution to ensure privacy of users while performing Internet web transactions. The advantages of our solution are that it provides comprehensive protection of privacy, that is, protection of user identities, security credentials, application data, actions, and locations.

2.3. Internet Anonymity Problems. Bitcoin is an interesting and important concept, as well as an increasingly used system for performing payments and other financial transactions [17]. It has many benefits, the most important of which is *anonymity of users* when performing payment transactions. Judging by the popularity of Bitcoin, this feature appears to be very attractive for many Internet users. Combined with the TOR protocol [18], for which the Bitcoin software components are already enabled, the system provides a significant degree of user anonymity.

Despite its benefits, the use of Bitcoin has also introduced many serious problems. These are all caused by the anonymity of its users and their transactions. Although some researchers question the true anonymity of Bitcoin transactions [19], the security mechanisms and features of the system are very sophisticated and breaking its anonymity does not appear to be a simple task [7]. Anonymity for payment transactions is very desirable property, but complete anonymity is not practical for many reasons. For example, illegal money laundering cannot be prevented. There are many examples of

illegal ransoms by hackers using Bitcoin. Further, regulatory controls by government and financial authorities are not possible. These several real-life examples clearly indicate that although anonymity with Bitcoin payments is theoretically "almost" perfect, it is quite inadequate for serious, real-life transactions and applications.

In order to provide privacy to users, reference [20] suggests the use of the so-called private credentials. With such credentials issuers do not have to be involved during authentication and users disclose only those attributes required by the relying parties and can do so without being easily tracked across their transactions. Authors define user identities relative to the relying parties where users reveal alternative identities to different parties. The solution suggested in this paper, based on pseudonyms, is much simpler, as users have single identity (pseudonym) and are definitely more flexible for maintenance, distribution, and updates.

Therefore, in addition to the proposed solutions to some Internet security and user privacy problems, the third significant contribution described in this paper is a protocol for *anonymity* of users not only for payments, but also for other types of Internet transactions.

2.4. Conclusions: Internet Security, Privacy, and Anonymity. Based on the information covered in the previous three subsections, it is clear that an effective security system, as well as one that protects the privacy and anonymity of users, is urgently needed and highly desirable for the Internet. Furthermore, this system should not be based on and dependent on the services of trusted third parties, as practice has shown that application and security protocols that they use are usually based on the requirement to share user identities, resources, transactions data, or even sensitive personal secrets, such as bankcard numbers. The essence of the system described in this paper is that data owners are in control of the distribution and use of their data. This means that the sharing of and use of data are controlled and under the consent of the data owners. With the described security system service providers are not able to collect users' data in the course of providing their services.

The concept of digital identity introduces some interesting complexities and challenges [21, 22]. The first challenge is that a single user may have more than one valid digital identity for different contexts of online applications or services. Secondly, digital identity in the Internet world is not fixed, but dynamic, since it changes over time and therefore needs to be updated. Therefore, digital identities are not necessarily unique, static, or permanent. There may be some online services for which a user may prefer to use a *pseudonym* or needs to be *anonymous* to varying degrees. The availability of pseudonyms and anonymity options opens up a multitude of variations on what constitutes a digital identity.

In conclusion, the system described in this paper supports *secure, private,* and *anonymous* business information exchange transactions. It includes three subsystems: exchange of e-mail letters, instant messages, and documents. The solution is in the form of an integrated system so all three types of information exchange applications can be used on a single, integrated portal. The system is easy to set up, to sign in to, and to activate. It also performs all of its security management functions in the background and transparently to users, and all security features are activated by default, so that user intervention is minimal.

Based on an extensive search and analysis of various research results, published papers, patents, and standards, it may be claimed that the described concept and its specific details represent a significant and an effective solution for the targeted problems which is beyond the current state-of-the-art Internet security technologies.

3. Structured Approach and Definitions of Security, Privacy, and Anonymity

In this section, the concepts of security, privacy, and anonymity used in this paper are precisely described and defined. For the purpose of this paper, the same term is used for all individuals, business entities, and various servers on the Internet: *parties*. When a user initiates a transaction, such as sending an e-mail letter, visiting a web server, uploading a file, or sending a payment, three types of parties are involved with respect to that transaction:

(i) Transaction partners—these are parties explicitly selected by the user to participate in the transaction.

(ii) Legal entities—these are parties that participate in the transaction but are not explicitly selected by the user.

(iii) Illegal entities—these are parties that should not participate in the transaction or get any information about it, usually called hackers.

As an example of transaction partners, when a user sends an e-mail letter to several users, then all the recipients are transaction partners, as they are explicitly selected by the user to participate in the transaction. Examples of legal entities participating in that transaction are all the intermediate Mail Servers to which e-mail letter is copied, as e-mail is a store-and-forward system. Another example is a website, which a user visits by specifying its URL. Legal entities are all the web servers that have links from the server that the user visits. These Mail and web servers are legal participants in a transaction, as they have been selected and preconfigured by the parties that are transaction partners for the specific transaction. Illegal entities are hackers, spam sites, and similar parties that should not be involved in a transaction or get any information about it.

Besides classification of all potential participants in a transaction into three categories, user data are also structured with respect to their type, sensitivity, and consequences for security, privacy, and anonymity in three categories:

(i) User identification data—those are data and parameters that identify the user, such as Distinguished Name (DN), login name, password, e-mail address, and IP number.

(ii) Metadata—data that specify some property of the user, such as her location, DoB, gender, search keywords, and location.

Table 1: Security specifications.

Parties	Partners	Legal	Illegal
IDs	✓	✓	✘
Metadata	✓	✓	✘
Content	✓	✓	✘

(iii) Transaction data (content)—data contained in a transaction, such as body of an e-mail letter, payment information, and web page.

Protecting the content of transaction data and user identities against illegal entities is the subject of Internet *security*; protecting user identities and metadata against legal entities not directly involved in the transaction is the subject of *privacy*, while protecting user identities against legal parties participating directly in the transaction is *anonymity*.

Based on the three types of parties and three categories of data, the following definitions may be established.

Definition 1 (internet security). An Internet application or a broader Internet environment provides *security* if the content of any type of data is not accessible (revealed) to any party other than transaction partners and/or legal parties. This is achieved by application of three security services: confidentiality, integrity, and availability (CIA).

This property is specified in the form of Table 1 (✓ denotes accessibility and ✘ denotes nonaccessibility).

With systems that provide *security*, based on Definition 1, users' identities and metadata of their transactions are still available to all legal parties. This is consistent, for example, with the definition of secure e-mail [23], where the content of an e-mail letter is readable only by the intended recipient. E-mail addresses (identities) of both parties in the header and the subject of the e-mail letter, location from which the e-mail letter was submitted, date/time, and so forth (metadata) are accessible to all legal parties, which in this example are intermediate mail servers and may be their administrators.

If, in the course of execution of a transaction, identities of transaction parties are not available and not accessible to any party except transaction parties directly involved in the transaction, such a system provides *privacy* of users. This concept may be precisely specified with the following definition.

Definition 2 (internet privacy). An Internet application or a broader Internet environment provides *privacy of users* if the identities of transaction parties are not accessible (revealed) to any party other than transaction partners directly involved in the transaction.

The concept is equivalent to security, except that targeted adversaries are different. In case of security, adversaries are hackers and illegal users, while in the case of privacy adversaries they are regular application services providers.

This property can be specified in the form of Table 2.

Finally, if, in the course of execution of a transaction, metadata of users are not available to any party on the Internet and, furthermore, identities of participants are not available even to transaction partners, such a system provides *anonymity of users*. This property is formally defined as follows.

Table 2: Security and privacy specifications.

Parties	Partners	Legal	Illegal
IDs	✓	✘	✘
Metadata	✓	✘	✘
Content	✓	✘	✘

Table 3: Security, privacy, and anonymity specifications.

Parties	Partners	Legal	Illegal
IDs	✘	✘	✘
Metadata	✘	✘	✘
Content	✓	✘	✘

Definition 3 (internet anonymity). An Internet application or a broader Internet environment provides *anonymity of users* if the identities of transaction parties and also transaction metadata are not accessible (revealed) to any party, including even direct transaction partners.

This property can be specified in the form of Table 3. This is, for example, consistent with the definition of anonymity for Bitcoin transactions [24] or with blind signatures [25].

These three definitions are used for guidance and as targets for design and validation of the security system described in the next section.

4. The Concept of the BIX System

The BIX System offers three applications in the form of an integrated security portal. Each of these applications provides security, privacy, and anonymity to users and their transactions in accordance with the three definitions. Their security features are specified in Table 1, privacy features are specified in Table 2, and anonymity features are specified in Table 3.

4.1. E-Mail with Security, Privacy, and Anonymity. The first application is a secure e-mail system. *Security* of e-mail letters is based on the standard approach, defined by the RFC 3851 (S/MIME) [23]. Therefore, the system provides data confidentiality (using encryption), data integrity (using hashing), sender's authenticity (using digital signatures), and receiver's authenticity (using digital enveloping). The system is based on use of X.509 certificates and scales globally based on the concept of the distributed and federated security architecture using BIX Proxy Servers and PKI [26].

In addition to standard S/MIME security services, a distinguished and unique feature of the secure e-mail application is *privacy* of users. Based on Table 2, this feature means that identities of the sender and also the recipient are not available to any party, including even mail servers. This feature is achieved by using *pseudonyms* as e-mail addresses instead of

regular e-mail addresses. These pseudonymous addresses are registered in the BIX Mail System where e-mail addresses, as an example, have the form 1234567890@bixsystem.com. The e-mail ID "1234567890" is just an example of a 10-digit random number, assigned to each user in the process of registration in the BIX System.

The BIX Mail Server is accessible through the BIX Proxy Server. If users want to use their native e-mail systems, they can still use their current e-mail addresses, such as (using the example of the two authors of this paper) nazri@kth.se and kounelis@kth.se. In this case, the BIX Proxy Server redirects e-mail letters to the native e-mail server, but such an arrangement does not provide privacy of users. However, even in this case, BIX Proxy Server encrypts the subject of the letter, which provides an additional degree of e-mail confidentiality.

The BIX Proxy Server is a web-based application accessed by standard browsers. Each instance of that server is connected to the TOR network [18]. Therefore, the system also provides *anonymity* of user locations, as (a) their locations and (b) the location of the BIX Proxy Servers that they use are not revealed to any of the native e-mail servers. For enhanced anonymity, the user browser can also be enabled to access the TOR network directly or a special TOR browser may be used [27]. This approach provides anonymity of users even against the BIX Proxy Servers.

In conclusion, in addition to standard S/MIME encryption/signing of e-mail messages, the described system provides *privacy of users* based on our three new innovative concepts: (a) using *pseudonyms* instead of full e-mail addresses, (b) *encryption of subjects* of e-mail letters, and (c) *anonymity of users* using the anonymizing TOR network.

4.2. Instant Messaging with Security, Privacy, and Anonymity. Instant messaging (IM) is a standard application that may be deployed on PCs as well as on smart phones. Users send short messages that are instantaneously delivered to their recipients. This type of application is very popular with individuals, but it is also becoming popular for professional communications. IM protocol and broadcast servers may also be used as an instantaneous communication mechanism for other Internet applications (medical, financial, security alerts, political notifications, etc.). Because IM applications are popular with a general public concern about privacy, and also with businesses for use with their important and sensitive business transactions, it is important that they provide security, privacy, and anonymity of users and messages.

Security of the IM system described in this paper is based on the same concept and security as for e-mail messages [23]. Certificates for public key cryptography are generated and distributed using PKI. The details are described in [28]. Messages are not encapsulated in the standard PKCS#7 format, as that would represent an overload for the mobile application and, at this stage of standardization, interoperability between independently developed secure IM systems is not needed.

Privacy of this enhanced secure IM system is achieved using the same approach as with the secure e-mail system. User identities are 10-digit random numbers, so they cannot be linked to real identities. Standard IM servers have no problem distributing such security-encapsulated IMs to their recipients, as they have anonymous user identities linked to anonymous identities of their mobile phones or PC workstations, used for transfer of messages. Based on Table 2, the identities of users that exchange IMs are known to each other, so that the designed secure IM application "translates" anonymous identities to real identities locally at the users' mobile phones or PC stations. Thus, real identities are known only to transaction partners exchanging secure IMs and not to any other component in the system. This approach provides security and privacy but not anonymity, as IM servers know that a user with anonymous identity ID-1 is transferring an IM to a user with anonymous identity ID-2.

To achieve full *anonymity* of users, even against IM servers, BIX Proxy Servers are used and incorporated in the protocol. Therefore, encrypted messages are routed by users to IM servers through those servers. In this way, the BIX Proxy Servers are used as "agents" for users connected to them. If an IM sender is connected to one server and the recipient is connected to the other, then these two servers appear to the IM server as sender and recipient of the IM. Thus, the IM servers do not know which two users are exchanging secure IMs. "Translation" of the BIX Proxy Server's address in a receiving IM to the address of the real recipient for delivery of the message to the correct recipient is performed by the Proxy Server. As explained earlier, in that process, the BIX Proxy Servers cannot read the content of messages, as they are encrypted. The servers do not even learn anonymous identities of participating parties (designated by 10-digit identifiers), as messages are delivered to the station and identified by a station session identifier, from which the user has logged into the BIX Proxy Server.

In conclusion, the described secure IM application has three distinctive and innovative features: it provides *security* of messages (by their encryption), *privacy* of users (using their pseudonyms), and *anonymity* of users (using BIX Proxy Servers).

4.3. Documents with Security, Privacy, and Anonymity. The application for protection of documents provides the possibility of sharing documents not only between two persons, but also within a group. The core *security services* are based on the PKCS#7 standard, so security services applied to documents are the same as those applied to e-mail letters (S/MIME). However, straightforward PKCS#7 packaging does not allow sharing of documents, meaning that both creator and authorized user should be able to access the protected document. The reason for this is that the PKCS#7 standard provides "forward" security only; that is, the document creator protects it for the designated recipient. After security encapsulation, the document may not be accessed by its creator, unless a clear copy is kept in some archive.

To enable *sharing of documents* so that both the creator and the recipient may access it after security packaging, the system introduces the concept of "*cross encapsulation*." To explain this approach, four standard PKCS#7 security services are first extended with an additional service—*proof of receipt*. Proof of receipt is the service that the recipient of

a document provides to the creator, confirming receipt of the document.

For extended security services applied to a document, new cryptographic concepts of "*forward encapsulation,*" "*backward encapsulation,*" and "*cross encapsulation*" are specified. "Forward encapsulation" involves two standard PKCS#7 services combined together—digital signature and digital enveloping. Both are applied by the sender of a document and provide to the document's recipient the proof of correct content, authenticity of the sender, and authenticity of the recipient. Equivalent cryptographic services, provided by the recipient to the sender, are called "backward encapsulation." This service is automatically created for the sender in the process of verification of the document by the recipient. In that process, the recipient recovers the hash of the document and its encryption key from the "forward encapsulated" PKCS#7 document. Then, she digitally signs the hash and envelopes encryption key for the sender. The created object represents "backward encapsulation," as it enables the document sender to access and open the document, just as the recipient can.

After creating "backward encapsulation," the recipient packages a "forward encapsulation" object and a "backward encapsulation" object into what in this paper is called "*cross encapsulation.*" This is a new and extended PKCS#7 format. It comprises standard PKCS#7 components: body (document), all certificates, certificate chain, and CRLs, but signature and enveloping sections are extended with "forward" and "backward" encapsulations. Such a new and extended type of the PKCS#7 object is called "*cross encapsulation.*"

It is not difficult to understand how this procedure can be extended to support multiple users sharing the same document.

The described scheme provides strong security for both document creator and its authorized user(s), but it does not provide privacy and anonymity of participants. The reason for that is that identities of users are represented as Distinguished Names (DN) contained in their X.509 certificates. Therefore, to achieve *privacy* and *anonymity*, DNs of users must be replaced with pseudonyms. This cannot be done inside X.509 certificates, as that would make them noncompliant to many standards. Therefore, in the BIX System, the ideas from Bitcoin are used as a solution for this problem [24]: users' public keys are used as their anonymous identifiers. Therefore, when creating a "cross encapsulation" package, users' public keys should be used instead of X.509 certificates.

Anonymous identities included in each encapsulated object are at the same time used as identifiers of all users who are authorized to access the specific document. Protected documents are uploaded and available at some document-sharing server. Therefore, because users have their own public keys, these public keys contained in each section of the "cross encapsulated" document are at the same time used as search attributes to identify documents accessible to the particular user. To retrieve documents for which she is authorized, the user submits her public key to the Secure Archive server. The server searches through the collection of protected documents stored at the server and displays the list of those that, in the section with anonymous identifiers, contain the provided public key.

With this scheme, recipients of documents cannot identify and verify the identities of associated users authorized to share the document, as they are all anonymous. They can only verify that there is a person who is authorized to access the document.

For instance, in a simplified case of two-person transactions—such as bids at auctions, submissions of tenders, and submissions of research papers—the recipient can verify that there exists a legitimate person as the creator of the document but cannot establish the identity of that person. That is exactly the requirement for anonymous sharing of documents.

5. The Role of BIX Proxy Servers

From the description of the design of the BIX System, it may seem that transaction partners and other legal parties on the Internet have simply "transferred" trust from various security service providers to the BIX Proxy Servers. Those servers receive and redirect secure e-mails and IMs, perform initial authentication, and so forth. It may seem that these servers learn much about users and their transactions, so they may show themselves to be a new type of trusted third party.

But, with the described approach and design solutions for handling identities, this is not the case. Depending on the type of services selected by users (security, privacy, or authenticity), BIX Proxy Servers cannot obtain any information about users and their transactions. In the designed security architecture, they simply act as "resource dispatchers" passing protected resources between users and various security and application services providers. Protection even against BIX Proxy Servers is based on special selection of user identities, as follows.

If only *security* is selected by users, this is provided using a combination of secret and public key cryptography. In that case, user identifiers are their X.509 certificates. They contain explicit user identification attributes (user DN), so when a certificate is submitted to the BIX Proxy Server in the authentication protocol [28], the server learns about that user's identity. But that is not a problem, as only security for users and their resources is required. Their content is hidden from BIX Proxy Servers using cryptographic protection.

If, in addition to security, users also select *privacy*, then X.509 certificates cannot be used. In this case, alternative, specially designed certificates must be used, based on the concept of Attribute Certificates [29]. In the original standard, these certificates are used to manage user roles for access control and authorization services. In the BIX System described in this paper, instead of role attributes, BIX Identifiers (10-digit random numbers) are used. Such new types of anonymity certificates are called *BIX Certificates*. These are used for distribution and validation of public keys, but without revealing real identities of their owners. With such certificates, users' public keys can still be distributed to their transaction partners, but identities of users are hidden even from BIX Proxy Servers.

Finally, if users want to perform transactions with full *anonymity*, then certificates cannot be used as identifiers. In this case, the BIX System uses users' public keys. These keys

provide full anonymity, as they do in the Bitcoin system [24]. A sophisticated analysis of various Bitcoin system resources to break anonymity is very complicated, so this solution may be considered as reasonably strong.

With the elimination of certificates, user identification and authentication cannot be performed. That is acceptable here, as the system provides anonymity. However, user credentials were used not only for identification and authentication, but also as identifiers of various encrypted resources designated to specific users, such as e-mail letters, instant messages, or documents. But public keys can also be used as anonymous identifiers. Resources (protected IM or e-mail letters) in this case cannot be delivered directly to users using their identifiers, as users are anonymous.

To solve this problem, two new distribution protocols have been designed: for protected IMs and e-mail letters, the identity of the (mobile or PC) station from which the user logged into a BIX Server is used ("station signatures"). With this approach, protected IMs and e-mail letters can be correctly delivered to the authorized recipients based on their station identity. For anonymous payments, the system uses another distribution protocol—distributed community protocol, which is equivalent to the blockchain in the Bitcoin system. Finally, the format of "cross encapsulated" documents does not contain certificates, but users' public keys. These keys can be used to search for documents targeted to the specific user.

6. Implementation and Deployment

At the time of writing this paper, research and design of the BIX System have been completed and the system is in a beta test of the prototype implementation. Two applications with security and privacy have already been implemented: a secure e-mail system and a secure documents management system. Implementation of Secure Instant Messages is in progress.

The system is accessible at https://www.bixsystem.com/.

In closing, it is important to emphasize that registration procedure for users and all registration data are performed locally, at users' (PC or mobile) workstations. User registration data are encapsulated into a strong encryption "envelope." In the concept of the described system, this is called a *BIX ID Card*. Registration data does not exist anywhere in the BIX System except at a user's secure tokens (smart cards, mobile phones, or USB sticks). With this approach, user identification data and security credentials cannot be hacked, stolen, impersonated, profiled, or tracked.

Protection and use of user's personal data that are under full user control and consent are the topic of our current research [30]. Results will be reported soon in forthcoming papers. With this final component of our overall BIX System, the system will provide full security, privacy, and anonymity for all users, their data, and transactions on the Internet.

7. Proof of the Concept and Its Correctness

In this section we formally prove that the described concept and system are correct; that is, we validate the claim that the system provides security, privacy, and anonymity. The criteria for the verification procedure are described in Table 3. According to that table, it must be shown that user identities, metadata of her transactions, and the content of transactions are not accessible or disclosed to any party except the transaction partner. Exchange of e-mail letters is used for this purpose, as the analysis and proof of correctness for the other two applications, Secure Instant Messages or Secure Sharing of Documents, are equivalent.

In an e-mail letter user identities are all e-mail addresses specified in the header of the message: `From:` sender, `To:` recipients, `CC:` recipients, and `BCC:` recipients. As specified in Section 4.1, random numbers as pseudonyms are used as e-mail addresses. Real e-mail addresses are known only to the BIX Proxy Server. Therefore, the requirements in line 1 of Table 3 are satisfied, as parties who receive e-mails cannot recognize the sender or any other recipient of the letter.

Metadata for e-mail letters are attributes in the header and IP location of the station from which the letter has been sent. But, because the sender submits the letter to the BIX Proxy Server, only the BIX Proxy Server knows the location of the sending station. Thus, the requirements in line 2 of Table 3 are also satisfied.

Finally, the content of the e-mail letter is its body, attachments, and its subject. These are encrypted using random secret key, enveloped with the recipient's public key. So they are accessible only to the designated recipient. This meets the requirements in line 3 of Table 3.

In addition to these considerations and analysis, it may be suggested that a very good proof of the correctness and feasibility of the described system is its operational instance, available at the URL https://www.bixsystem.com/.

A final potential issue of correctness may be the possibility of security, privacy, or anonymity violations by the BIX Server itself. Assuming that the code has been tested and verified for correctness, this possibility may be caused only by infected or corrupted software. But this possibility is effectively eliminated by two methods. First, the core software modules of the server are themselves encrypted, and, second, each instance of the server is hosted in a highly secure cloud environment.

In case the highest level of assurance is needed, the system may be extended with smart cards issued to users. In this case, all of a user's sensitive data and security credentials are stored in the user's smart card. With this version, instead of using a standard web GUI with SSL protection, the system upon access by the user sends a software servlet into the user's browser environment. This is code that is dynamically downloaded and activated in the browser's local environment. Upon presentation of the correct PIN by the user, the servlet activates a smart card that performs all required crypto functions.

8. Conclusions and Future Work

The results of this research have created the initial version of the concept of the Web Portal that supports three types of security services, protection, privacy, and anonymity, for three types of Internet applications, e-mail, files sharing, and instant messages. The results represent an initial version of

an innovative concept of security infrastructure and secure applications based on the use of combined security, privacy, and anonymity technologies. At the same time, these results have opened some new topics and challenging problems that will be addressed in the next research phase. Some of the important extensions of the current Web Portal as well as innovative research problems and targeted solutions are listed below.

8.1. Anonymizing Mobile Network and Protocols. The current version of the BIX Portal is based on and supports only web-based applications. Each client is linked to the Portal using standard browsers. The Portal hides user locations, but this concept and protocols also must be extended with solutions for *anonymity of locations* when using mobile applications, not mobile browsers. It is well known that almost all smart phones and mobile applications collect data about user locations. Thus, some effective solution for anonymity of user locations when using mobile technologies and applications is needed.

8.2. Concept of Personal Security Proxies. Current solutions do not provide complete privacy and anonymity of users with respect to the BIX Portal itself. The Portal stores protected users' documents, so it must have the full trust of users with respect to their availability and correct operations. In the current version of the architecture, BIX Portals can sometimes also be used as ASPs, that is, as third parties. The solution for this problem is to use a new category of servers, called *Personal Security Proxies*. These proxies will be designed and implemented as client applications and will replace the handling of all data and functions in the current version of the BIX Portal. This approach will be based on the concept of blockchain-distributed public ledger, so personal Portals will be clients to the servers in the ledger's distributed network [31].

8.3. Personal Services Using Java Applets. An important component of Personal Security Proxies will be the code stored and executed in Javacard chips—applets. The identification applet will be compliant with the PIV standard. Other applets will perform full crypto operations with e-mails, documents, or instant messages. Finally, an applet for anonymous payments based on virtual currencies will also be created. Such a system will provide truly end-to-end encryption, as all crypto operations will be performed locally, at the users' workstations, using Javacard chips and a collection of applets.

8.4. Peer-to-Peer (P2P) Protocols. The introduction of Personal Security Proxies opens the possibility of performing transactions as pure *peer-to-peer transactions*. Such transactions do not need or use third parties. It is well known that such transactions are much more efficient than transactions using third parties and complex infrastructures, as they are performed instantaneously between the transaction parties. However, it is also well known that security for such transactions is much more difficult to achieve as there are no third parties involved. This category of transactions is usually called "*community transactions*" and their verification mechanism is the concept of a distributed public ledger.

8.5. Distributed Community Applications. The concept of Personal Security Proxies and use of different types of public ledgers as the protocol for validating community transactions open the possibility of designing and implementing a completely new category of applications, called *community* or *peer-to-peer applications*. Current examples and ideas include distributed file sharing systems, proof of presence, and voting schemes. The scope and functionality of such applications are much broader than those of the applications described in this paper. These new applications represent an interesting challenge for future research.

Competing Interests

The authors declare that they have no competing interests.

References

[1] Washington Post, "Saving the internet," August 2014.

[2] World Economic Forum, "*Why Internet Security Matters*," https://agenda.weforum.org/2015/01/why-internet-security-matters/.

[3] D. E. Denning, "Field encryption and authentication," in *Advances in Cryptology: Proceedings of Crypto 83*, D. Chaum, Ed., pp. 231–247, Springer, New York, NY, USA, 1984.

[4] D. E. Denning, "Cryptographic checksums for multilevel database security," in *Proceedings of the Symposium on Security and Privacy*, p. 52, 1984.

[5] Internet Engineering Task Force (IETF), "System for cross-domain identity management: definitions, overview, concepts, and requirements," Tech. Rep. RFC 7642, Internet Engineering Task Force (IETF), 2015.

[6] U. T. Mattsson, "A practical implementation of transparent encryption and separation of duties in enterprise databases: protection against external and internal attacks on databases," in *Proceedings of the 7th IEEE International Conference on E-Commerce Technology (CEC '05)*, pp. 559–565, Munich, Germany, July 2005.

[7] D. Ron and A. Shamir, "Quantitative analysis of the full Bitcoin graph," in *Proceedings of the Financial Crypto Conference*, Okinawa, Japan, 2013.

[8] J. Clark and A. Essex, "CommitCoin: carbon dating commitments with bitcoin," in *Financial Cryptography and Data Security: 16th International Conference, FC 2012, Kralendijk, Bonaire, Februray 27-March 2, 2012, Revised Selected Papers*, vol. 7397 of *Lecture Notes in Computer Science*, pp. 390–398, Springer, Berlin, Germany, 2012.

[9] D.-R. Tsai, A. Y. Chang, S.-C. Chung, and Y. S. Li, "A proxy-based real-time protection mechanism for social networking sites," in *Proceedings of the IEEE International Carnahan Conference on Security Technology (ICCST '10)*, pp. 30–34, IEEE, San Jose, Calif, USA, October 2010.

[10] R. C. Jammalamadaka, T. W. van der Horst, S. Mehrotra, K. E. Seamons, and N. Venkasubramanian, "Delegate: a proxy based architecture for secure website access from an untrusted machine," in *Proceedings of the 22nd Annual Computer Security Applications Conference (ACSAC '06)*, pp. 57–66, Miami Beach, Fla, USA, December 2006.

[11] J. Wu and Z. Huang, "Proxy-based web service security," in *Proceedings of the IEEE Asia-Pacific Services Computing Conference (APSCC '08)*, pp. 1282–1288, Yilan, Taiwan, December 2008.

[12] A. Dowling and J. G. Keating, "A proxy-based security architecture for Internet applications in an extranet environment," *Journal of Systems and Software*, vol. 58, no. 2, pp. 107–118, 2001.

[13] J. Shao, G. Wei, Y. Ling, and M. Xie, "Identity-based conditional proxy re-encryption," in *Proceedings of the IEEE International Conference on Communications (ICC '11)*, pp. 1–5, Kyoto, Japan, June 2011.

[14] J. Liu, M. D. Ryan, and L. Chen, "Balancing societal security and individual privacy: accountable escrow system," in *Proceedings of the 27th IEEE Computer Security Foundations Symposium (CSF '14)*, pp. 427–440, IEEE, Vienna, Austria, July 2014.

[15] A. Acquisti and H. College, *The Economics of Personal Data and the Economics of Privacy*, OECD Privacy Guidelines, 2010.

[16] J. Turow, The Digital Marketing Transformation: How Consumer Privacy Fits into the Equation, https://www.truste.com/resources/pioneers-and-mavericks/joseph-turow/.

[17] P. Franco, *Understanding Bitcoin: Cryptography, Engineering, and Economics*, Wiley Finance Series, John Wiley & Sons, 2015.

[18] TOR Project, https://www.torproject.org/.

[19] F. Reid and M. Harrigan, *An Analysis of Anonymity in the Bitcoin System*, Clique Research Cluster, University College Dublin, Dublin, Ireland, 2012.

[20] J. Camenish, A. Lehmann, and G. Neven, "Electronic identities need private credentials," *IEEE Computer and Reliability Societies*, vol. 10, no. 1, pp. 80–83, 2012.

[21] A. Jøsang, M. A. Zomai, and S. Suriadi, "Usability and privacy in identity management architectures," in *Proceedings of the 5th Australasian Symposium on ACSW Frontiers (ACSW '07)*, vol. 68, pp. 143–152, Darlinghurst, Australia, 2007.

[22] J. Vossaert, J. Lapon, B. De Decker, and V. Naessens, "User-centric identity management using trusted modules," in *Public Key Infrastructures, Services and Applications*, J. Camenisch and C. Lambrinoudakis, Eds., vol. 6711 of *Lecture Notes in Computer Science*, pp. 155–170, Springer, Berlin, Germany, 2011.

[23] IETF, Secure/Multipurpose Internet Mail Extensions (S/MIME), Version 3.1, Message Specifications, https://www.ietf.org/rfc/rfc3851.

[24] 2009, https://en.bitcoin.it/wiki.

[25] D. Chaum, "Blind signature system," in *Advances in Cryptology: Proceedings of Crypto 83*, D. Chaum, Ed., p. 153, Springer, 1984.

[26] I. Kounelis, S. Muftic, and J. Loschner, "Secure and privacy-enhanced e-mail system based on the concept of proxies," in *Proceedings of the 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO '10)*, pp. 1405–1410, IEEE, Opatija, Croatia, May 2014.

[27] TOR Project, "*TOR Browser*," https://www.torproject.org/projects/torbrowser.html.en.

[28] M. Mumtaz, S. Muftic, and N. Bin Abdullah, "Strong authentication protocol based on Java Crypto chips," in *Proceedings of the 5th IEEE International Conference on IT Convergence and Security (ICITCS '15)*, Kuala Lumpur, Malaysia, August 2015.

[29] IETF, "*An Internet Attribute Certificate Profile for Authorization*," RFC 3281, https://www.ietf.org/rfc/rfc3281.txt.

[30] I. Nai Fovino, R. Neisse, R. Rana, and S. Muftic, "Electronic soft identities (e-IDs)," JRC Technical Report, 2014.

[31] S. Muftic, "BIX certificates: cryptographic tokens fro anonymous transactions based on certificate public ledger," *LEDGER Journal*, vol. 1, no. 1, 2016, http://www.ledgerjournal.org/ojs/index.php/ledger.