A New Approach for Electronic Signature

Gianluca Lax, Francesco Buccafurri, Serena Nicolazzo, Antonino Nocera and Lidia Fotia
DIIES Department, University of Reggio Calabria, Reggio Calabria, Italy

Keywords: Electronic Signature, Digital Signature, Online Social Network, Twitter.

Abstract: There are many application contexts in which guaranteeing authenticity and integrity of documents is essential. In these cases, the typical solution relies on *digital signature*, which is based on the use of a PKI infrastructure and suitable devices (smart card or token USB). For several reasons, including certificate and device cost, many countries, such as the United States, the European Union, India, Brazil and Australia, have introduced the possibility to use simple generic *electronic signature*, which is less secure but reduces the drawbacks of digital signature.In this paper, we propose a new type of electronic signature that is based on the use of social networks. We formalize the proposal in a generic scenario and then, show a possible implementation on Twitter. Our proposal is proved to be secure, cheap and simple to adopt.

1 INTRODUCTION

Digital signature is a tool used in several contexts to exchange documents by guaranteeing their authenticity and integrity. As digitally signed documents have full legal validity, they can be used in e-commerce, e-government, dematerialization processes, and so on.

To be used in open environments like the Internet, digital signature needs a *public key infrastructure* to identify the signer. Public key infrastructure (PKI) (Kościelny et al., 2013; He et al., 2014) was designed to permit the binding between the subject and the public key by means of a digital certificate issued by the Certification Authority (CA). PKI relies on a hierarchical architecture and a strong trust-based model. In particular, a digital certificate includes a serial number (i.e. an identifier unique within the CA scope), the subject identity, the issuer identity, the validity period, the certificate policies of applicability, the usages for which the key has been authorized by the digital signature of the CA that issued the certificate. An advantage of PKI is that a smart card or similar device can store the user's certificate and corresponding private key.

The main drawback of digital signature is the need of having a public key infrastructure (PKI) and/or a physical device (typically a smart card or a token USB), or the need of securely storing a private key. This can increase the cost of this solution or reduce its usability.

Also the possibility of using remote signing services, such as HSM, does not help. Hardware Security Modules (HSMs) (Sustek, 2011; Mavrovouniotis and Ganley, 2014; Kim et al., 2014) are devices used for data encryption and decryption and host one or more cryptographic keys that respond to automated or manual commands. They safeguards and manages digital keys for strong authentication and have the capability to detect an attack on their surface and securely delete the sensitive content stored in their memory.

Due to the drawbacks derived from the use of digital signature, in several countries, such as the United States, the European Union, India, Brazil and Australia, the possibility to use simple generic *electronic signature* has been introduced. Differently from digital signature, electronic signature is a *weaker* way of signing documents, because it does not require any additional measure of security (in particular, a public key infrastructure and a physical device). No standard technology or implementation of electronic signature exists, so that proprietary software to generate and validate is used. The most important advantage of electronic signature is that it can be implemented more easily than digital signature, but accepting a lower level of security.

Electronic signatures can be used in closed domains where users agree on a signature protocol that (1) allows the identification of the signer, (2) creates a connection between signer and document and (3) detects any change to the document after the signature is applied. Clearly, the security of the protocol depends

Lax, G., Buccafurri, F., Nicolazzo, S., Nocera, A. and Fotia, L.
A New Approach for Electronic Signature.
DOI: 10.5220/0005743404400447
In *Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016)*, pages 440-447
ISBN: 978-989-758-167-0

on its implementation and must be evaluated.

In this paper, we propose a new approach for e-signature solutions that does not rely on a public key infrastructure or device or private keys, which are substituted by the use of social networks (Buccafurri et al., 2014c). Social networks have grown massively (Nocera and Ursino, 2012) and nowadays most of the people has at least an account in one of them (Buccafurri et al., 2013; Buccafurri et al., 2014d). In this paper, the social network is used as "device" enabling the generation of the signature and also as trusted-third-party allowing signature sharing. Our approach shows important characteristics of cheapness, usability, and, more importantly, security.

The analysis of protocol security shows that the proposed e-signature approach is able to guarantee document authenticity, document integrity and non-repudiation against attacks that an adversary can carry out.

The paper is organized as follows. In the next section, we discuss related work. In Section 3, we define the model and describe how to generate and verify a signature. In Section 4, we analyze the security of our solution. Section 5 shows an instantiation of the solution that uses Twitter as social network. Finally, in Section 6, we draw our conclusions and sketch possible future work.

2 RELATED WORKS

In this section, we survey the most relevant signature techniques proposed in the literature.

Conditional Signatures were originally introduced by Lee et al. (Lee and Kim, 2002) to implement fair exchange of digital signatures in untrusted environments and do not require the card to have a user interface or any special peripheral (like Clarke et al. (Clarke et al., 2002)).

Berta et al. (Berta et al., 2004) propose a method to generate, instead of an ordinary signature, a conditional signature such that it is guaranteed that the condition can not become true before a certain amount of time has passed. This should leave time for the user to move to a trusted terminal for checking the signatures generated by the card and to enforce that the conditions of the fake signatures can ever become true. Since this approach requires the smart card to know the current time but most smart cards have no internal clock, it could be acquired from a secure time servers as described in Berta et al. (Berta and Vajda, 2003). Moreover, this proposal requires the user to store every signed message, because this message has to be checked later by means of a trusted terminal. Since it may be infeasible for C to store large message, this problem can be solved by outsourcing the logging function to an external logserver. Therefore, even though the required hardware is the standard one, a trusted third party is required.

The drawback of conditional signature is to require a significant load for the user, who has to split the signature task into two phases, delaying the effective conclusion of the procedure at validation-time.

Weak signature was introduced by T. Rabin and Ben-Or (Rabin and Ben-Or, 1989; Rabin, 1994) to solve a problem (Verifiable Secret Sharing (Chor et al., 1985)) motivated by a question of general multiparty secure computation in the unconditional setting (network of untappable channels). They provide a form of authentication for which the on-line participation of a third party is needed.

Check vectors are related to work on authentication codes (Gilbert et al., 1974; Simmons, 1985) and on universal classes of hash functions (Carter and Wegman, 1977). The weak signature scheme relies on the presence of an on-line trusted server that participates in the creation of every signature, and also participates whenever a signed message holder wishes to prove to anyone that a signature is valid. This trusted server stores and retrieves information received from the signing agency and the message holder, and computes certain linear combinations of values it receives.

Using the idea of check vectors, T. Rabin (Rabin and Ben-Or, 1989) presents a weak signature scheme, called Information Checking Protocol. Consider that the intermediary wishes to have a message *s* signed by the dealer. In the first phase, the original message holder intermediary ends up with the "signed message" *s*, *y*, while a third party RCV ends up with the check information *a*, *b*. Anyone can determine the validity of the signature by asking RCV to reveal the check information. The signature is weak, because the assistance of this third party is needed to verify a signature.

Another signature scheme in the unconditional setting was introduced by Chaum and Roijakkers (Chaum and Roijakkers, 1991). It satisfies a stronger set of conditions than Rabin's Information Checking Protocol, at a great increase in communication cost.

Visual cryptography (Sharma and Srivastava, 2014; Shaji et al., 2014; Naor and Shamir, 1995) is a type of cryptographic scheme which can decode concealed images without any cryptographic computation. Naor et al. (Naor and Pinkas, 1997) suggest a number of transparency-based methods for visual authentication and identification, and give rigorous analysis of their security.

(Matsumoto, 1998) presents human-friendly identification schemes such that a human prover knowing a secret key in his brain is asked a visual question by a verifier, which then checks if an answer sent from the prover matches the question with respect to the key.

Ateniese et al. (Ateniese et al., 1996) propose a visual cryptography scheme for a set of participants to encode a secret image into many secondary images in such a way that any participant receives one secondary image and only qualified subsets of participants can "visually" recover the secret image, but non-qualified sets of participants have no information, in an information theoretical sense, on the original image. This scheme does not require the participants to perform any cryptographic computation.

The methods of visual cryptography can be broken by attacker exploiting human interaction. Moreover the user load can be considered very relevant.

In this context, our paper proposes a lightweight protocol that allows us to know who created an electronic document and to ensure that this document has not been altered since that person created it. Differently from the above solutions (conditional signature and weak signature), our proposal does not rely on certification authority, asymmetric cryptography, or signature device.

3 A MODEL FOR E-SIGNATURE

In this section, we present the abstract model to realize e-signatures by social networks. We observe that this is the main added value w.r.t. the proposal described in (Buccafurri et al., 2014a), in which no theoretic model has been considered.

The main entities of our model are:

- a social network SN that supports the following features:
  1. the possibility to post textual information after authentication for registered users;
  2. the automatical notification about the post activity of other selected users;
  3. the possibility to search for an information posted by a user.

  Observe that the first characteristic is common to the most social networks, whereas the remaining ones are not supported by all social networks. Twitter is an example of social networks supporting these three features: indeed, users are notified about *tweets* coming from their *follows* and a search is done by *hashtags*.
- a company C, the environment in which this kind of signature has validity.
- the set of persons who can sign and verify a signature. In the following, we will denoted by S the signer of a document.

The model is composed of the following procedures:

- *Registration*. The procedure is carried out when a new person is added in such a way that he/she is enable to sign a document. In this phase, this person is identified and associated with a profile in the social network SN. Moreover, the company requires to be notified about any posting activity of this person in SN.

  Then, the person posts on SN the first message, say *registration message* of the type $\langle I, ID_S \rangle$, where I contains the real-life identity of S and ID_S is the identifier of S in the social network SN. This allows us to establish a trusted relationship between the external user account that pertains to the company and the registered Twitter account. For example, the email address of a user could be used as identifier to be associated with the Twitter account.

  The company is notified about this post and, in turn, posts the same message in its public space.
- *Signature.* This procedure is carried out by the signer S on the document D to be signed. Let ID_S be the identifier of S in the social network SN and h be a cryptographic hash function.

  This procedure is composed of two steps. In the first step, S posts on SN the *signature message* defined as $\langle h(D), ID_S \rangle$ (i.e., the document digest and his account identifier).

  In the second step, the company is notified about this post and, in turn, posts the same message $\langle h(D), ID_S \rangle$. We denoted the latter message posted by C as *confirmation* message.
- *Verification.* This procedure is used to check the validity of a signature. Let D be the document whose signature has to be verified. The protocol works as follow. First, the digest $h(D)$ is computed. Then, $h(D)$ is searched among the public information posted in the social network SN. If $h(D)$ is not found, then the signature on the document D is detected as invalid (i.e., either wrong or absent signature). Otherwise,

  we have two possibilities:
  1. Both a signature message and a confirmation message $\langle h(D), ID_S \rangle$ are found. In this case, the verification procedure returns that the signature on D is valid.
  2. Either a signature message or a confirmation message $\langle h(D), ID_S \rangle$ is found. In this case, the

verification procedure returns that an attack occurred. Section 4 is devoted to describe how to detect the type of attack and how to decide if the signature can be considered valid or not.

It is worth noting that, in case of multiple signers and, thus, of multiple signature messages found, the above verification is repeated for each signer, thus obtaining a result (valid, invalid or attack) for each signer.

- *Revocation.* This procedure is carried out to revoke the signature grant to a person (for example, in case of dismissal of an employee). We recall that in the registration procedure of a person, the company requires to be notified about any posting activity in SN of this person in such a way to generate the confirmation message for each signature message produced by this person. By the procedure of revocation, this notification is removed so that no confirmation message will be produced by the company. Consequently, any successive signature message posted by this person will not be confirmed by the company and, thus, the verification of this signature will fail.

The conceptual model underlying our proposal of e-signature requires message exchanges among the parties, message search in the social network, and enabling activity notification.

Clearly, how to technically implement these features is strongly related to the actually social network on which such a proposal is implemented, so that this aspect is not addressed in this section. However, in Section 5, we will instantiate our proposal on a real social network and these issues will be faced.

4 SECURITY ANALYSIS

In this section, we prove that the model defined above guarantees the security properties required for digital signature, which are document authenticity, document integrity and non-repudiation.

In our analysis, our (realistic) assumptions are:

1. the cryptographic hash function h withstands all known types of attacks in such a way that *pre-image*, *second pre-image* and *collision* resistance are assured;
2. the social network SN is a trusted party;
3. the information posted by the users on the social network cannot be compromise.

In our threat model, the attacker is either the company, or a signer, or a third person. We do not consider the collusion between company and signer as this is meaningless (indeed, in a typical scenario this does not give them any advantage – they could agree to obtain the same result without carry out any attack).

Now, we analyze the security properties of our proposal with respect to several attacks (Lax et al., 2015).

Document Authenticity. A document is authentic if it has been signed by the claimed signer. In our solution, once a signature is verified valid for a signer S, the personal information of S (name, surname, etc.) can be found in the *registration message* posted by both the signer and the company. This allows us to associate a document signature with a real-life identity.

An attack on document authenticity is carried out in different ways (we consider only the most significant cases):

- The adversary creates a fake account on SN by using the personal information of a victim. However, because the registration protocol has not been done, the company is not notified of signatures produced by this fake account so that no confirmation messages will be generated. Consequently, a signature done by the adversary is not considered valid.
- The adversary adds or corrupts an already posted signature message and the corresponding confirmation message by substituting $h(D)$ with $h(D')$, where D' is a new document, in such a way that it appears a valid signature of the victim on D'. However, an external adversary cannot modify posted message due to Assumption 2. Moreover, whenever the adversary is the company, it is able to modify only the confirmation message, not the signature (Assumption 2). Therefore the attack fails.

Document Integrity. This property ensures that any modification of the binary representation of the document done after the signature is detected. This property is guaranteed by the presence of the document digest $h(D)$ both in the signature message and the confirmation message. Any change to the document after the signature results in the change of the digest, which, thus, will be different from $h(D)$.

- An attack on document integrity would success only if the attacker is able to modify the signed document yet keeping its digest equal to $h(D)$. However, this is unfeasible thanks to Assumption 1, which guarantees that the cryptographic hash function has pre-image resistance.
- Another possibility of attack is that the digest of the document is modified in the signature

or/and the confirmation message. In this case, an external attacker cannot modify such messages thank to assumption 2. If the signer or the company can act as attacker, the modification of only one of such messages is possible, so that the signature is not considered valid. Moreover, the mismatch between signature and confirmation message is used to detect this attack.

Non-repudiation. This property assures that the real signer cannot challenge the authorship or validity of the signature. In this case, the attacker is clearly the signer.

- A first possibility of attack is to claim that the signature message has been produced by someone else who violated his/her account. Assumption 1 assures that this is unfeasible, so that repudiation is not admitted.
- The signer deletes the signature message from the posted information. As a consequence, now only the confirmation message for that signature is found. The signature is not considered valid, however a warning for a possible (repudiation) attack is raised.

Document Immutability. This property requires that the content shown by the signed document cannot change after the signature. It is worth noting that this property is different from the document integrity discussed above, because document integrity refers to changes in the bits composing the document. In contrast, document immutability is related to the possibility for documents of having an ambiguous presentation depending on system or external parameters (Alsaid and Mitchell, 2005). The typical case is that of digital documents containing macros or JavaScript, which establish what should be displayed on the basis of some conditions (for example, a date). Clearly, this does not produce any change on the bits of the signature, so that document integrity property is satisfied.

As done for digital signature, this attack is contrasted by forcing that signed document cannot contain dynamic content. Interestingly, the presence of dynamic content can be detected, so that a signature done on a non-static document is considered not valid.

5 AN INSTANTIATION OF THE MODEL

In this section, we show an application of our proposal in a real-life case, and discuss the requirements of the real social network to use as underlying layer.

The scenario considered is that of a university that needs an e-signature procedure for internal documents (learning plans, exam results, travel reimbursement requests, and so on).

In this case, the actors are the university, which plays the role of the company `C` of our model, and its students and employees, who compose the set of persons who can sign and verify a signature.

The social network `SN` underlying the proposal should:

1. allow registered users to post textual information after authentication;
2. allow users to be automatically notified about the post activity of other selected users;
3. allow for the search for an information posted by a user.

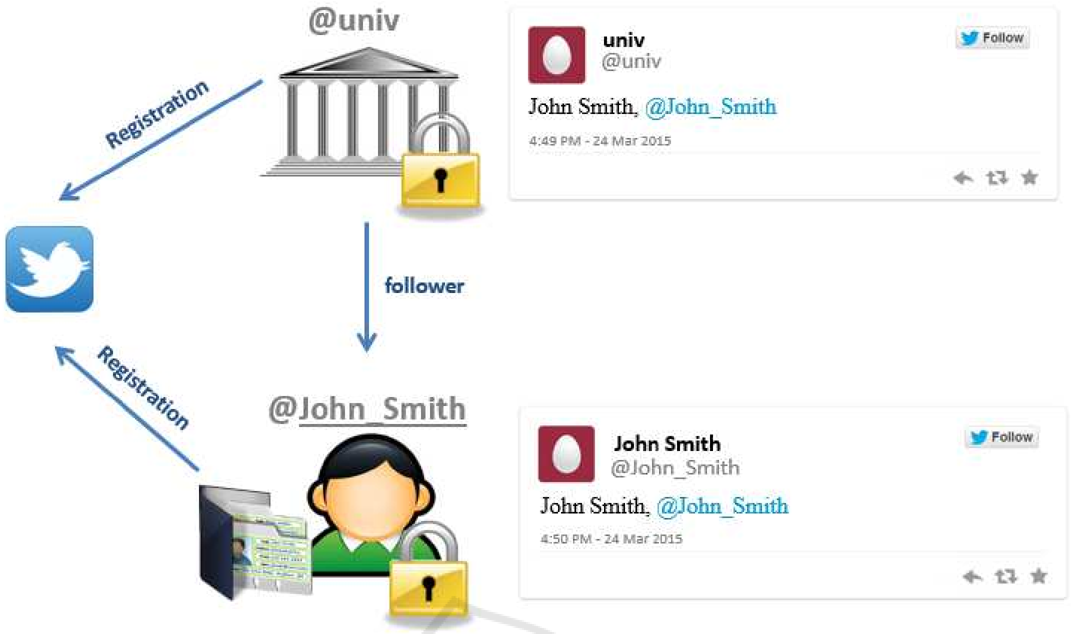
Among all social networks, Twitter is one of the most famous complying such requirements. Indeed, (1) registered users can post textual information, named *tweet*, and they must be authenticate to post anything; (2) users can add friendship relations with other users in such a way to be automatically notified about their tweets, and (3) Twitter supports textual search among tweets by means of a mechanism based on *hashtags*. Concerning this aspect, in Twitter people use the hashtag symbol # before a relevant keyword or phrase (no spaces) to categorize their tweets by keywords. Moreover, hashtags are indexed to make it easier to find a conversation about a topic.

In the implementation of our solution, the first step is the registration. Each student and employee is identified and associated with a profile in Twitter. Also the university has its Twitter profile, and adds a *follow* relationship towards registered students and employees, in such a way that the university account receives their tweets. Assume that `@univ` is the account of the university in Twitter (we recall that a Twitter screen-name starts with the symbol @ and represents the unique Twitter identifier for a given user).

Each registered student and employee posts the *registration message* on Twitter: an example of this message for the user John Smith is ⟨John Smith, @John_Smith⟩, where the first item is the real-life identity of the user, whereas the second item is his identifier on Twitter. The university account receives this tweet and, in turn, posts the same information in its public space.

A snapshot of the publication of the registration message on Twitter is illustrated in Figure 1.

Consider now the instantiation of the signature procedure. When an employee or a student, say John Smith, needs to sign a document *D*, first the digest of *D* is computed by SHA-256,



John Smith, @John_Smith

John Smith, @John_Smith

Figure 1: An instantiation of the registration procedure.

which is considered robust against all known attacks. Then, he posts on Twitter the *signature message* ⟨#5WKm+A0+9X51DtyLKxaB6myoC6uHrbZ+Oc+ZKFuRFMY, @John_Smith⟩, where the first item is the *base64* representation of the document digest. Observe that the digest of the document is hashtagged (see the symbol # at the beginning): this results in the indexing of this tweet in such a way to be found in case of search.

Next, the university account receives this tweet and, in turn, posts the same tweet in its public space as *confirmation* message.

A snapshot of the result of the signature procedure on Twitter is illustrated in Figure 2, where the tweet posted by the signer and that posted by the university are reported.

Consider now the procedure used to check the validity of a signature. When a user has to check the signature on a document D, the digest $h(D)$ is computed. Then, the hashtag $\#h(D)$ is searched on Twitter.

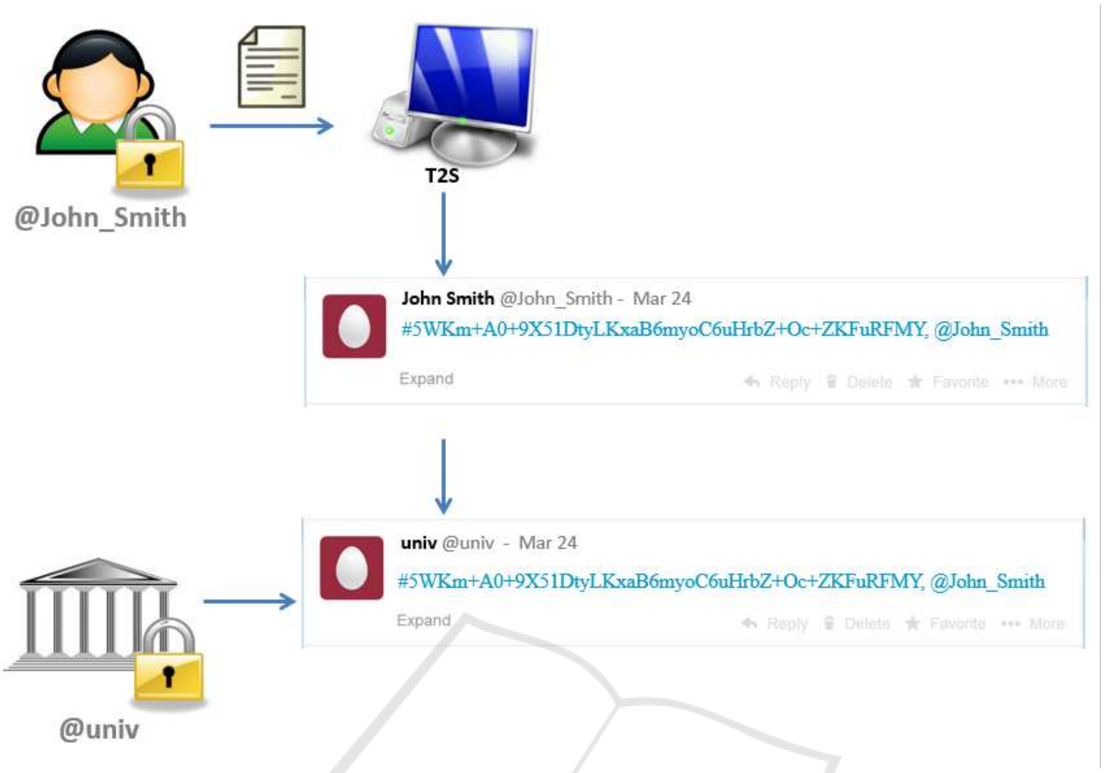
If no tweet is found, then the document is considered never signed. If a pair of equal tweets ⟨signature message, confirmation message⟩, the first posted by a user S, the second posted by @univ is found, and if @univ follows the Twitter account of S, then D is considered signed by S. Finally, if a signature message without the corresponding confirmation message is found or if a confirmation message without the corresponding signature message is found, the verification procedure notifies a possible attack and the type, according to the security analysis provided in Section 4.

Finally, consider the revocation procedure. When it is necessary to revoke the permission of signature to a student or an employee, then the following relation from @univ to the Twitter account of such a person is removed. Then, @univ will be not notified about any tweet posted by this person and no confirmation message will be produced. Consequently, if this person tries to sign a document, the signature verification procedure will fail (no confirmation message for this person is found).

Finally, it is worth noting that the use of Twitter as social network produces an interesting side effect, that is the timestamp of the signature generation. Observe that this is a feature usually not required in digital signature, and typically provided not for free by a trusted third party. This is another characteristic that makes our proposal more interesting also from the cost point of view.

6 DISCUSSION AND CONCLUSIONS

The need of guaranteeing authenticity and integrity of digital documents is high in many application contexts, such as e-commerce and e-government. The tool typically used for this purpose relies on digital signature, which provides high security standards.



John Smith @John_Smith - Mar 24
#5WKm+A0+9X51DtyLKxaB6myoC6uHrbZ+Oc+ZKFuRFMY, @John_Smith

univ @univ - Mar 24
#5WKm+A0+9X51DtyLKxaB6myoC6uHrbZ+Oc+ZKFuRFMY, @John_Smith

Figure 2: An instantiation of the signature procedure.

However, due to some drawbacks of digital-signature-based solutions, the request of more simple and cheap solutions is growing.

The concept of electronic signature has been introduced in many country to simplify and make more effective the process of dematerialization of documents and transactions, both in the public sector and in business.

In this paper, we presented a new form of electronic signature which overcomes the drawbacks of digital signature. Our approach is based on the use of social networks to share the information necessary to sign and verify a signature. Thus, a first advantage is related to the user-friendliness, as people are well disposed to work in an environment they well know (i.e., social network). The fact that, in our solution no private key or PKI infrastructure has to be managed, is a great advantage. From this point of view, our proposal overcomes other solutions such as those using PKI technology within OpenSSL.

The security analysis of the approach showed that it is able to guarantee authenticity, integrity and non-repudiation, and to be resistant against a large number of attacks, which are also detected (Buccafurri et al., 2014b; Buccafurri et al., 2015).

The effectiveness of our proposal has been shown by describing an instantiation of our generic approach in a scenario related to an university, where the social network considered is Twitter.

ACKNOWLEDGEMENTS

This work has been partially supported by the TENACE PRIN Project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research and by the Program “Programma Operativo Nazionale Ricerca e Competitività” 2007-2013, Distretto Tecnologico CyberSecurity funded by the Italian Ministry of Education, University and Research.

REFERENCES

Alsaid, A. and Mitchell, C. J. (2005). Dynamic content attacks on digital signatures. *Information Management & Computer Security*, 13(4):328–336.

Ateniese, G., Blundo, C., De Santis, A., and Stinson, D. R. (1996). Constructions and bounds for visual cryptography. In *Automata, Languages and Programming*, pages 416–428. Springer.

Berta, I. Z., Buttyán, L., and Vajda, I. (2004). Mitigating the untrusted terminal problem using conditional signatures. In *Information Technology: Coding and Com-*

puting, 2004. Proceedings. ITCC 2004. International Conference on, volume 1, pages 12–16. IEEE.

Berta, I. Z. and Vajda, I. (2003). Documents from malicious terminals. In *Microtechnologies for the New Millennium 2003*, pages 325–336. International Society for Optics and Photonics.

Buccafurri, F., Fotia, L., and Lax, G. (2014a). Social signature: Signing by tweeting. In *Electronic Government and the Information Systems Perspective*, pages 1–14. Springer.

Buccafurri, F., Lax, G., Nicolazzo, S., and Nocera, A. (2014b). A Privacy-Preserving Solution for Tracking People in Critical Environments. In *Proc. of the International Workshop on Computers, Software & Applications (COMPSAC'14)*, pages 146–151, Västerås, Sweden. IEEE Computer Society.

Buccafurri, F., Lax, G., Nicolazzo, S., and Nocera, A. (2014c). A model to support multi-social-network applications. In *On the Move to Meaningful Internet Systems: OTM 2014 Conferences*, pages 639–656. Springer.

Buccafurri, F., Lax, G., Nicolazzo, S., and Nocera, A. (2015). Accountability-preserving anonymous delivery of cloud services. In *Trust, Privacy and Security in Digital Business*, pages 124–135. Springer.

Buccafurri, F., Lax, G., Nicolazzo, S., Nocera, A., and Ursino, D. (2013). Measuring betweenness centrality in social internetworking scenarios. In *On the Move to Meaningful Internet Systems: OTM 2013 Workshops*, pages 666–673. Springer.

Buccafurri, F., Lax, G., Nicolazzo, S., Nocera, A., and Ursino, D. (2014d). Driving global team formation in social networks to obtain diversity. In *Web Engineering*, pages 410–419. Springer.

Carter, J. L. and Wegman, M. N. (1977). Universal classes of hash functions. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 106–112. ACM.

Chaum, D. and Roijakkers, S. (1991). Unconditionally-secure digital signatures. In *Advances in Cryptology-CRYPT090*, pages 206–214. Springer.

Chor, B., Goldwasser, S., Micali, S., and Awerbuch, B. (1985). Verifiable secret sharing and achieving simultaneity in the presence of faults. In *Foundations of Computer Science, 1985., 26th Annual Symposium on*, pages 383–395. IEEE.

Clarke, D., Gassend, B., Kotwal, T., Burnside, M., Van Dijk, M., Devadas, S., and Rivest, R. (2002). The untrusted computer problem and camera-based authentication. In *Pervasive Computing*, pages 114–124. Springer.

Gilbert, E. N., MacWilliams, F. J., and Sloane, N. J. (1974). Codes which detect deception. *Bell System Technical Journal*, 53(3):405–424.

He, D., Chan, S.-C., Zhang, Y., Guizani, M., Chen, C., and Bu, J. (2014). An enhanced public key infrastructure to secure smart grid wireless communication networks. *Network, IEEE*, 28(1):10–16.

Kim, D., Jeon, Y., and Kim, J. (2014). A secure channel establishment method on a hardware security module. In *Information and Communication Technology Convergence (ICTC), 2014 International Conference on*, pages 555–556. IEEE.

Kościelny, C., Kurkowski, M., and Srebrny, M. (2013). Public key infrastructure. In *Modern Cryptography Primer*, pages 175–191. Springer.

Lax, G., Buccafurri, F., and Caminiti, G. (2015). Digital document signing: Vulnerabilities and solutions. *Information Security Journal: A Global Perspective*, pages 1–14.

Lee, B. and Kim, K. (2002). Fair exchange of digital signatures using conditional signature. In *Symposium on Cryptography and Information Security*, pages 179–184.

Matsumoto, T. (1998). Human–computer cryptography: An attempt. *Journal of Computer Security*, 6(3):129–149.

Mavrovouniotis, S. and Ganley, M. (2014). Hardware security modules. In *Secure Smart Embedded Devices, Platforms and Applications*, pages 383–405. Springer.

Naor, M. and Pinkas, B. (1997). Visual authentication and identification. In *Advances in Cryptology-CRYPTO'97*, pages 322–336. Springer.

Naor, M. and Shamir, A. (1995). Visual cryptography. In *Advances in CryptologyEUROCRYPT'94*, pages 1–12. Springer.

Nocera, A. and Ursino, D. (2012). PHIS: a system for scouting potential hubs and for favoring their "growth" in a Social Internetworking Scenario. *Knowledge-Based Systems*, 36:288–299. Elsevier.

Rabin, T. (1994). Robust sharing of secrets when the dealer is honest or cheating. *Journal of the ACM (JACM)*, 41(6):1089–1109.

Rabin, T. and Ben-Or, M. (1989). Verifiable secret sharing and multiparty protocols with honest majority. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 73–85. ACM.

Shaji, S. et al. (2014). Anti phishing approach using visual cryptography and iris recognition. *IJRCCT*, 3(3):088–092.

Sharma, A. and Srivastava, D. K. (2014). A comprehensive view on encryption techniques of visual cryptography? *International Journal of Recent Research and Review*, 7(2).

Simmons, G. J. (1985). Authentication theory/coding theory. In *Advances in Cryptology*, pages 411–431. Springer.

Sustek, L. (2011). Hardware security module. In *Encyclopedia of Cryptography and Security*, pages 535–538. Springer.