USign—A Security Enhanced Electronic Consent Model

Yanyan Li, *IEEE Student Member*, Mengjun Xie, *IEEE Member*, and Jiang Bian, *IEEE Member*

***Abstract*—Electronic consent becomes increasingly popular in the healthcare sector given the many benefits it provides. However, security concerns, e.g., how to verify the identity of a person who is remotely accessing the electronic consent system in a secure and user-friendly manner, also arise along with the popularity of electronic consent. Unfortunately, existing electronic consent systems do not pay sufficient attention to those issues. They mainly rely on conventional password based authentication to verify the identity of an electronic consent user, which is far from being sufficient given that identity theft threat is real and significant in reality. In this paper, we present a security enhanced electronic consent model called USign. USign enhances the identity protection and authentication for electronic consent systems by leveraging handwritten signatures everyone is familiar with and mobile computing technologies that are becoming ubiquitous. We developed a prototype of USign and conducted preliminary evaluation on accuracy and usability of signature verification. Our experimental results show the feasibility of the proposed model.**

I. Introduction

Electronic consent (eConsent) can significantly improve the efficiency and quality of the informed consent process, which is time-consuming and burdensome. For example, electronic consent can help recruit more subjects and meanwhile save time and money in clinical trials [12]. Therefore, many healthcare providers such as the nationwide VA hospital system have started the transition to an electronic consent and electronic signature process for consenting hospital procedures.

However, security and privacy concerns, e.g., how to assure the security and privacy of the data of electronic consent users in a secure and user-friendly manner, also arise along with the popularity of eConsent. Unfortunately, existing electronic consent systems such as eConsent Trial Project [2] do not pay sufficient attention to those issues. They mainly rely on conventional password based authentication to verify the identity of a user being consented, which is far from being sufficient given that identity theft threat is real and significant in reality. So far, little attention has been paid to the security assurance of electronic consent while the majority of the research efforts on electronic consent are focused on improving participant comprehension of the consent using multimedia and mobile computing technologies.

Yanyan Li is with the University of Arkansas at Little Rock, Little Rock, AR 72204 USA (e-mail: yxli5@ualr.edu).

Mengjun Xie is with the University of Arkansas at Little Rock, Little Rock, AR 72204 USA (e-mail: mxxie@ualr.edu).

Jiang Bian is with the University of Arkansas for Medical Sciences, Little Rock, AR 72205 USA (e-mail: jbian@uams.edu).

Similar to current paper-based consenting procedure, handwritten signatures are also collected in many electronic consent systems. However, in those systems, a user' signatures, which are collected either directly through touch screen or indirectly through digital scan of handwritten signatures, are only preserved for archival purpose instead of being used for verifying the identity of the signer.

Leveraging the fact that handwritten signature is an effective behavioral biometric and the technological trend that smartphones (and tablets) become ubiquitous, we propose a security enhanced electronic consent model called USign. USign takes the signature a user supplies through her smartphone/tablet along with her password to verify the user's identity. Signatures effectively become another authentication factor besides password in a user-friendly manner. Different from common smartphone-based two-factor authentication methods that essentially verify the device, USign verifies the person. USign can also be combined with common two-factor authentication schemes to further enhance the authentication security.

We developed a proof-of-concept prototype of USign that consists of an Android app for collecting user signatures and a server application for hosting the consent forms and verifying the user identities. We conducted preliminary evaluation on the accuracy and usability of the signature verification. Our experimental results show the feasibility of the proposed model.

The rest of this paper is organized as follows. Section II briefly describes related work. Section III presents the design and implementation of USign, particularly the signature verification component. Section IV evaluates the proposed system in terms of its accuracy and usability. Section V concludes this paper.

II. Related Work

A. Electronic Consent

One possible solution to improving the efficiency and quality of the consent process is electronic consent. Electronic means is generally eco-friendly, streamlined, readily available, cost-efficient, and provider and consumer friendly.

Electronic consent can provide a number of benefits and greater protection to participants. In some cases, electronic consent facilitates remote consent thereby giving researchers greater access to rural populations that may otherwise be underrepresented. There is a body of literature that shows that the use of video, audio, and other media improves participant comprehension of the details of a study. For example, the eConsent Trial project [2] launched by the Office of the National Coordinator for Health IT aims to identify effective and innovative ways to capture patient consent and help

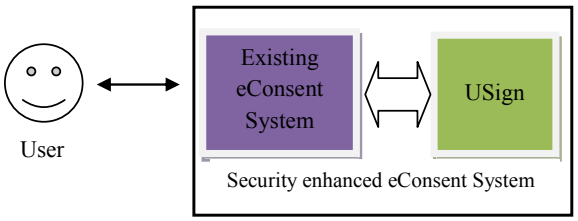

Figure 1. USign-based eConsent system model

patients understand the consequences of their choices. However, clearly, the captured signature is only used as a record, and no verification is implemented in that tool.

B. *Electronic Signature*

Electronic signature and its application in healthcare can be dated back to 1997 when the FDA promulgated 21 CFR Part 11 [1] to permit and encourage the use of electronic signature, which is a signature legally binding equivalent of the individual's handwritten signature. Commercial software, e.g., DocuSign [3] and e-SignLive [4], has been widely adopted to collect electronic signatures for online transactions and consenting. However, the signatures used by those software programs usually are not real ones, i.e., handwritten signatures. Instead, a user chooses a style from predefined signature styles and based on the selected style the system will generate a "signature" that appears to be handwritten. Therefore, these types of signatures are not behavioral biometric and cannot be used for verifying a signer's identity.

C. *Signature Verification*

Signatures are commonly accepted for authentication of individuals; and the signature verification process has been widely studied. A variety of approaches have been proposed to recognize and verify electronic signatures including dynamic time warping (DTW) [13], Hidden Markov Model (HMM) [14], Neural Networks [15], etc. A fine-tuned signature verification system can achieve high accuracy (or low error rate) [6], which makes signature-assisted authentication system effective and accurate in practice.

III. USIGN SYSTEM

USign is unique in that it is not aimed to be another standalone full-fledged eConsent system. Instead, USign is focused on the security enhancement realized through signature verification. USign is designed as an independent security assurance system that can interface with existing eConsent systems which are mainly focused on consent presentation and participant comprehension.

Figure 1 shows the proposed security enhanced eConsent system model in which USign delegates the function of user identity verification during user login, document signing and so on while an existing eConsent system focuses on other consenting procedures. Users of the new eConsent system will benefit from stronger security assurance while maintaining almost the same user experience.

As USign is aimed to enhance eConsent security through signature verification, we first present the system design specific to signature verification and then describe the algorithm for signature verification in the remaining part of this section.

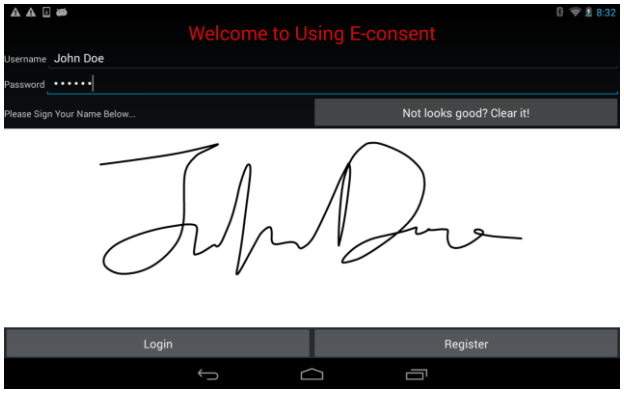

Figure 2. A Snapshot of the login screen of the USign client app

A. *System Design*

We have developed a proof-of-concept USign prototype system that is focused on the signature-based security enhancement. The prototype system follows standard client-server model. We implemented our client as a mobile application running on Android devices. Figure 2 shows the login interface of the client application running on an ASUS Nexus 7. The server part is deployed on Tomcat v7.0 and uses MySQL as the storage database. Regarding identity verification, the client application is used to interact with user (e.g., collecting user signatures) and the server is responsible for all the computation in signature verification. All communications between client and server are encrypted through standard HTTP over SSL/TLS.

As shown in Figure 2, a user needs to provide his/her signature besides his/her username and password in order to log into the prototype system. We believe that the behavioral biometric of handwritten signature will enhance the authentication assurance as it is directly linked to the user besides being a second authentication factor. If the provided signature does not match with the signatures that the system has, the user will not be able to log into the system even if the username and password are correct.

Our prototype system uses signature for both registration and login. In the registration phase, a user needs to submit a specified number of signatures into the system. The first half of the signatures are used as the reference signatures and the rest are used as the training signatures. For the signature obtained in the login process, its normalization value will be calculated and compared with the separating boundary. If the value is less than the boundary value, its corresponding signature will be regarded authentic and the login succeeds.

B. *Signature Verification*

We apply Dynamic Time Warping (DTW) method to signature verification due to its reported high accuracy and good performance. Figure 3 shows the workflow of the user identity verification, which is performed through the DTW method. The major steps of the process include: data acquisition, preprocessing, feature selection, pairwise

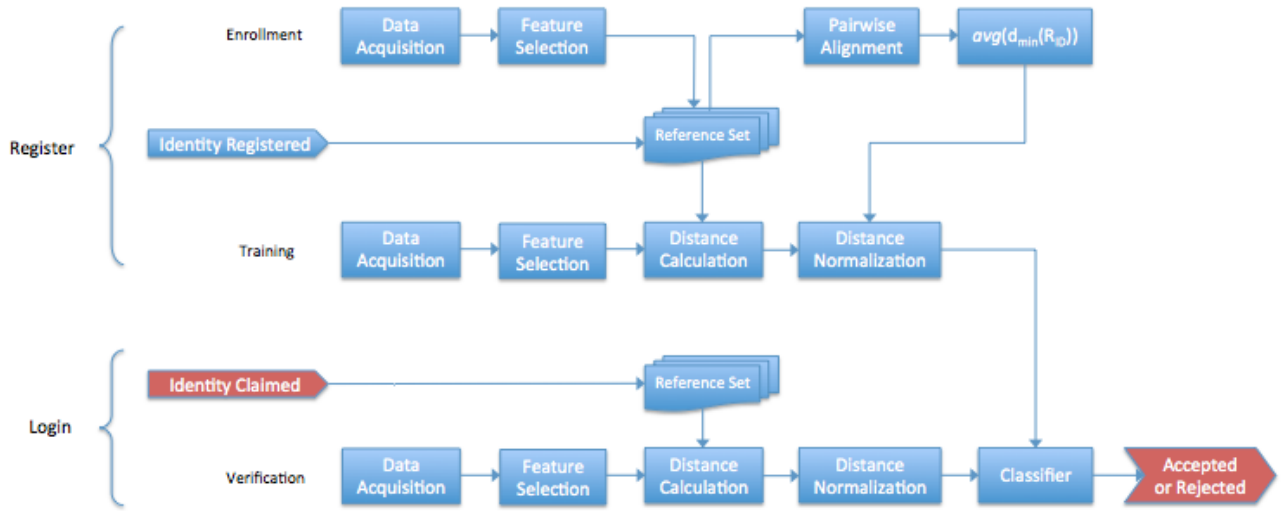

Figure 3. The workflow of user authentication through signature verification

alignment, distance normalization and verification. We briefly describe each step below.

In the Data Acquisition step, users' signature data are obtained, e.g., through either smartphones or tablets. The collected data contains a number of characteristics such as coordinates, timestamp, pressure information, writing angles and so on. After being collected, the signature data may be preprocessed (or normalized) to eliminate noises introduced during signature capturing device (e.g., rotate or adjust the signatures to a standardized angle or a fixed size [7][8]). Considering that preprocessing can cause information loss [6], our current system does not include this step.

In the Feature Selection step, we use the difference of x (and y) coordinates between two consecutive points, i.e., Δx (and Δy) as the signature features based on the study by Kholmatov and Yanikoglu [6]. We did not include features seen in other studies such as pressure, azimuth and altitude as on one hand we want to optimize performance and on the other hand there are studies showing that those features are not effective in signature verification [9][10].

In the Pairwise Alignment step, we calculate the DTW distances of all the reference signatures through pairwise comparison. A matrix is first created to record all the calculated distance values, as shown in Figure 4. Then we calculate the minimum distance for each row and derive the average minimum value based on these minimum values. The obtained $avg(d_{min})$ is then used as the base in the next step (Distance Normalization). As $avg(d_{min})$ is per user, the final result in this step is $avg(d_{min}(R_{ID}))$, where R_{ID} represents a user. Note that this step is only applicable to reference signatures.

In the Distance Normalization step, a separating boundary distinguishing genuine signatures from forged ones is derived based on the normalized value. This step consists of three sub-steps. First, the minimum DTW distance between all genuine training signatures and the corresponding reference signatures is calculated. Then, the minimum distance is divided by $avg(d_{min}(R_{ID}))$. In this way, we obtain a normalized value for every genuine training signature. Similarity, we can

	Ref Sig 1	Ref Sig 2	Ref Sig 3	
Ref Sig 1	d_{11}	d_{12}	d_{13}	d_{1min}
Ref Sig 2	d_{21}	d_{22}	d_{23}	d_{2min}
Ref Sig 3	d_{31}	d_{32}	d_{33}	d_{3min}

$avg(d_{min})$

Figure 4. Pairwise alignment process for reference signatures

also obtain a normalized value for every forged training signature. Afterwards, a linear classifier can be used to classify all the normalized values and find the separating boundary that differentiates all genuine signatures from forged ones. The boundary is used to verify the authenticity of the login signature acquired in the next phase.

In the Verification step, a user signature will go through all the aforementioned steps, including distance calculation and normalization. After the normalization step, the normalized value of the login signature will be compared with the separating boundary. If the normalized value is smaller than the boundary value, then the signature is regarded authentic. Otherwise, it is considered as a forgery signature and can't be used for login or document signing.

IV. System Evaluation

A. Experiment Methodology

To evaluate our signature verification algorithm, we use the Task1 dataset from the first international signature verification competition (SVC2004) as our data source (available at http:// www.cse.ust.hk/svc2004/download.html), which has been extensively used in the evaluation of many different verification algorithms.

The data set contains 40 writers' signatures, and there exist 40 signatures for each writer. Among them, the first 20 are genuine signatures and the rest are forgery signatures. We choose 12 genuine signatures from each writer as the reference signatures, which are used for calculating the $avg(d_{min})$ of genuine signatures. Then, 2 genuine signatures

and 2 forgery signatures for each writer are used to derive the separating boundary. The remaining 6 genuine signatures and 18 forgery signatures are used for testing, from which the false rejection rate (FRR) and false acceptance rate (FAR) are derived, respectively. Table 1 shows the information of the dataset for evaluating our verification method.

Table 1 Data Source

Data Set	Type	Each User	Total Size
Reference	Genuine	12	480
Training	Genuine/Forgery	4	160
Test 1	Genuine	6	240
Test 2	Forgery	18	720

B. *Error Rate*

Equal Error Rate (EER) is usually the most important metric for evaluating a signature verification method. It is obtained from the condition where FAR is equal to FRR. For the DTW method, the error rate is closely related to the separating boundary, which is a user-independent value.

Table 2 FRR and FAR of the DTW Method

Separating Boundary	FRR	FAR
1.20	11.7%	4.2%
1.25	5.83%	5.4%
1.30	4.17%	7.2%
1.35	4.17%	10.3%

Table 2 shows the relation between separating boundary and the corresponding FRR and FAR. We can see that when the separating boundary is set to 1.25, FRR and FAR are quite close to each other. The EER for this DTW method with the given data source is close to 5.6%.

C. *System usability*

In order to evaluate the usability of the proposed USign system, we recruited 10 students to test this system and asked them four questions after their tests. The four questions are as follows:

- Question 1: Is this eConsent system easy to use?
- Question 2: Would you like to use it in the future?
- Question 3: Do you feel comfortable and secure using your signature to login the system?
- Question 4: Do you have some concerns regarding it?

Table 3 Evaluation Result

Questions	# of Yes	# of No
Question 1	8	2
Question 2	9	1
Question 3	9	1
Question 4	2	8

Table 3 shows their responses, from which we can see most participants have positive impression of this system. At the same time two students did express their concerns. One asked "would it be possible that somebody forges my signature to log into the system"; the other expressed the concern on the troublesome registration. We readily acknowledge that these concerns are reasonable. Our system requires training signatures from the user in the registration stage, which affects user experience for certain people. Although signature forgery is difficult it is still possible. We plan to conduct more extensive usability evaluation in a larger scale to understand those user concerns we may not be aware of and at the same time to further improve the system usability based on the evaluation feedback.

V. CONCLUSION

In this paper, we present a security enhanced electronic consent model, USign, for strengthening the identity protection and authentication for electronic consent systems. We developed a prototype of USign and conducted preliminary evaluation on system accuracy and usability. Our evaluation results show the feasibility of the proposed model.

REFERENCES

[1] FDA, U. (21). CFR Part 11 Electronic Records; Electronic Signatures.

[2] Marchesini, K. (2013). eConsent Trial Project Overview. http://www.healthit.gov/sites/default/files/econsent_project_overview_hitpc_010813.pdf

[3] Retrieved from https://www.docusign.com/

[4] Retrieved from http://www.silanis.com/

[5] Yeung, D. Y., Chang, H., Xiong, Y., George, S., Kashi, R., Matsumoto, T., Rigoll, G. (2004). SVC2004: First international signature verification competition. In Biometric Authentication (pp. 16-22). Springer Berlin Heidelberg.

[6] Kholmatov, A., Yanikoglu, B. (2005). Identity authentication using improved online signature verification method. Pattern recognition letters, 26(15), 2400-2408.

[7] Jain, A. K., Griess, F. D., Connell, S. D. (2002). On-line signature verification. Pattern recognition, 35(12), 2963-2972.

[8] Xuhua, Y., Furuhashi, T., Obata, K., Uchikawa, Y. Constructing a high performance signature verification system using a GA method. In Proceedings of the Second New Zealand International Two-Stream Conference on Artificial Neural Networks and Expert Systems, pp. 170-173, IEEE.

[9] Lei, H., Govindaraju, V. (2005). A comparative study on the consistency of features in on-line signature verification. Pattern Recognition Letters, 26(15), 2483-2489.

[10] Nanni, L., Lumini, A. (2008). A novel local on-line signature verification system. Pattern Recognition Letters, 29(5), 559-568.

[11] Aloul, F., Zahidi, S., El-Hajj, W. (2009, May). Two factor authentication using mobile phones. In Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on (pp. 641-644). IEEE.

[12] Sanderson, IC, Obeid, JS, Madathil, KC, Gerken, K, Fryar, K, Rugg, D, Alstad, CE, Alexander, R, Brady, KT, Gramopadhye, AK, Moskowitz, J (2013). Managing clinical research permissions electronically: A novel approach to enhancing recruitment and managing consents. Clinic Trials, 10, 4:604-11.

[13] Martens, R., Claesen, L. (1996, August). On-line signature verification by dynamic time-warping. In Pattern Recognition, 1996., Proceedings of the 13th International Conference on (Vol. 3, pp. 38-42). IEEE.

[14] Yang, L., Widjaja, B. K., Prasad, R. (1995). Application of hidden Markov models for signature verification. Pattern recognition, 28(2), 161-170.

[15] Baltzakis, H., Papamarkos, N. (2001). A new signature verification technique based on a two-stage neural network classifier. Engineering applications of Artificial intelligence, 14(1), 95-103.