REMOTE HANDWRITTEN SIGNATURE AUTHENTICATION

Jarrod Trevathan
James Cook University
Townsville, Australia

Alan McCabe
James Cook University
Townsville, Australia

Keywords: Biometrics, authentication, client/server, handwritten signature, network security.

Abstract: This paper presents a secure real-time remote user authentication system based on dynamic handwritten signature verification. The system allows users to establish their identities to other parties in real-time via a trusted verification server. The system can be used to gain remote access to restricted content on a server or to verify a signature on a legal document. State of the art dynamic verification techniques are combined with proven cryptographic methods to develop a secure model for remote handwritten signature verification.

1 INTRODUCTION

Dynamic handwritten signature verification (HSV) is a computerised method of establishing a person's identity This is achieved by examining the characteristic way in which the person signs his/her name. The handwriting of the person is captured and digitised in real-time using a graphics tablet. The result is a series of values representing the person's handwritten signature. This is referred to as an "electronic signature". An electronic signature can be verified by comparing it with a reference set of the user's handwritten signature attributes.

Biometric security systems (including HSV) are typically used in simple, stand alone applications. However, this is now changing as the emphasis of computing shifts towards distributed systems where the qualities offered by a handwritten signature are highly desirable. This paper describes a system for performing HSV over a network.

This paper is organised as follows: Section 2 provides some background on HSV and the motivation for constructing a networked based HSV system. Section 3 presents a client/server model whereby a handwritten signature can be remotely verified. Section 4 examines the HSV algorithm. Section 5 discusses network security issues and its implications for HSV. Section 6 describes several protocols for remote HSV. Section 7 provides a security analysis of the proposed system. Section 8 gives some concluding remarks.

2 HSV

Handwritten signatures have long been used as proof of authorship of, or at least agreement with, the contents of a document (Schneier, 1994). Humans find signatures compelling as they offer authenticity, and prevent forgery, alteration, repudiation and reuse of the signed item (Schneier, 1996).

Despite the increasing popularity of other biometric authentication schemes such as retinal scanning and automated fingerprint identification, HSV is still regarded as one of the most reliable and natural methods of authenticating one's identity (Gupta and McCabe, 1997). There are a number of factors contributing to this including:

- high level of acceptability to the general public
- low cost of hardware compared to most other computerised schemes
- high level of reliability compared to most other schemes
- low error rate with little real deviation due to external factors

The growth of web based commerce and banking has been accompanied by a rise in new and innovative attacks of defrauding or impersonating legitimate users. Each year the costs associated with Internet and credit card fraud continue to accumulate. Much of this loss is attributed to ineffective user authentication protocols.

Trevathan J. and McCabe A. (2005).
REMOTE HANDWRITTEN SIGNATURE AUTHENTICATION.
In *Proceedings of the Second International Conference on e-Business and Telecommunication Networks*, pages 335-339
DOI: 10.5220/0001419203350339

A remote HSV system alleviates this problem by allowing a user to verify his/her identity on demand. For example, the user can verify his/her identity at the point of sale when using a credit card or can sign bids in an electronic auction. Similar systems involving fingerprinting and hand geometry have been proposed in (Techweb, 1998; Jain *et al.*, 1998). However, handwritten signatures are much more versatile.

Handwritten signatures are familiar to humans and have many network-based applications, which conventional biometric recognition systems are unable to effectively emulate. For example, remote HSV can be used to grant approval by "signing" a legal or consenting document such as a will or business contract without having to be physically present. Furthermore, remote HSV can allow a doctor's prescription to be authenticated at a pharmacy during sale to ensure the purchaser is the correct recipient of the medication.

Another application for remote HSV is where a client must authenticate themself to gain access to a database or file system under a server's control. In addition, the recipient of a business or personal email can use HSV to authenticate the sender.

While other biometric and cryptographic schemes can be used to accomplish the aforementioned tasks, HSV is clearly the most natural and least intrusive for humans. For example, people would prefer to sign their name rather than place their heads in a machine to photograph their retina or face. Furthermore, cryptographic methods often rely on people remembering large numbers. While these values can be placed in a smart card, cards can be lost or stolen and are inconvenient to carry. Furthermore, HSV cannot be subverted like other biometric systems. For example, it is almost impossible to get someone to sign their name under duress, whereas fingers, eyeballs and heads can be severed from a person's body and can be used to identify the dead (or maimed) person (as seen in action movies such as *Demolition Man* and *The Sixth Day*).

3 REMOTE HSV

3.1 The Model

Figure 1 presents a client/server model for performing remote HSV. The main components of the system include:

- A set of clients $C = \{c_1, c_2, ..., c_n\}$ who each possess a unique handwritten signature h; h_i denotes the signature corresponding to c_i, $1 \leq i \leq n$;
- A *trusted* server S to which clients can make requests for verification. The server contains a verification algorithm V, and secure reference database;

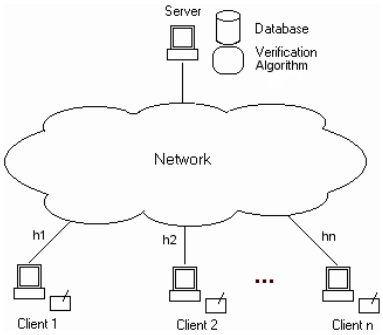

Figure 1: Remote Handwritten Signature Verification

- A network providing a bi-directional communication link between each client and the server.

A client, c_i, provides a signature for verification (in which case he/she is trying to establish or "prove" his/her identity). Alternately, c_i can be the recipient of the verification results (in which case the server sends them the verified identity of the signer).

The server, S, verifies signatures presented on the client's behalf. The verification algorithm can be updated on the server and hence technology may be improved without requiring any changes to the client software. Furthermore, having the verification software on the server removes the bias that would exist if a client also contained the same software. For example, there is a possibility that malicious users may tamper with or simulate the verification algorithm.

The database is used to store handwritten signature reference files, client information and security logs.

The verification algorithm, V, makes a binary decision to ascertain whether the client is genuine. The algorithm must be able to successfully authenticate legitimate signatures and identify forgeries. An outline of the verification algorithm is presented in Section 4.

The network links clients to the server. This network is assumed to be insecure and any information passing through it can be tampered with. Section 5 discusses network security and its implications for HSV.

3.2 Stages in Verification

There are two main stages in a remote HSV system (Figure 2):

- Registration - Add users to the system. Update signature profiles;
- Verification - Verify an electronic signature.

Registration is required in order to add new users to the scheme. This must generally occur in some form of supervised environment where the potential user must prove his/her identity through traditional means

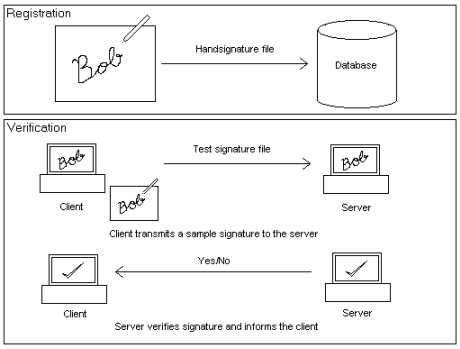

Figure 2: Registration and Verification Phases

such as a birth certificate, driver license, etc. If successful, a reference file is created for the registered user. This involves storing samples of the user's signature in a secure database. The user is provided with a unique identifier (number or name) and any additional information pertinent to the verification procedure.

Unlike other biometric systems, an individual's signature tends to change over time due to various factors such as age and health (Gupta and McCabe, 1997). Therefore, the registration stage requires a method to update a user's reference file when needed after his/her initial registration.

During verification an algorithm is run on a client's electronic signature. The electronic signature is compared with the client's reference file. The server logs the outcome and notifies the client.

4 VERIFICATION ALGORITHM

This section contains a brief description of the verification algorithm used in the scheme. Further details can be found in (McCabe, 1997; McCabe, 2004).

The dynamic HSV approach consists of two separate phases: conversion and comparison. The conversion phase involves tracing the path of the signature. It then examines several static and dynamic details of the handwriting such as shape, spacing, velocity, acceleration and timing details. These details are converted into a string of characters (different characters are used to represent different levels of velocity, acceleration etc. and different aspects of shape, timing etc.). The end result of this process is a string of several hundred characters in length which attempts to characterise the handwritten signature.

In order to compare two signatures it is possible to use any one of a number of existing string distance algorithms to determine the level to which the signatures differ. In (McCabe, 1997) several string distance algorithms were implemented and experimented with. The *Wagner-Fischer* algorithm (described in (Stephen, 1994)) proved to be the most successful.

In order to create a reference, a user of the system is asked to provide five reference signatures on registration. The strings are extracted from each of the reference signatures, each signature is compared to one another and details of the common types and average levels of variation are recorded. When a test signature is processed, it is compared to the reference and a figure for the overall difference is calculated. If this figure is below the threshold the test signature is accepted as genuine, otherwise rejected as a forgery.

5 NETWORK SECURITY

In a network environment the signature data is at risk from eavesdropping, interception, modification, fabrication and disruption. Measures such as encryption, *digital* signatures and time stamping, are needed to provide protection against these threats. This section examines network security requirements for the HSV scheme presented in this paper.

A client is provided with an initial session key, k_i, during registration. This allows encrypted communication with the server using any off-the-shelf symmetric cryptosystem. Key updates are performed using Diffie-Hellman key exchange (Diffie and Hellman, 1976).

The results of verification are signed using a digital signature (not to be confused with handwritten or electronic signatures). S publishes a public key S_{ku}. This enables S to sign the results of verification using the private key S_{kr}. Anybody can verify the signature using S_{ku}. This can be achieved using RSA (Rivest *et al.*, 1978) or ElGamal (ElGamal, 1985) signatures.

Time stamping is required to prevent an interceptor from resending captured messages. A time stamp is appended to the handwritten signature data before encryption. When a message is received, its time stamp is examined to determine how old the message is and if it has been previously received. This presents a unique problem to HSV as any captured electronic signature could be reused indefinitely. A remedy stated in (McCabe, 2000), is to use a signed password (rather than a signature) to verify a user. This enables compromised handwritten passwords to be changed, rather than handwritten signatures.

S logs all information regarding verification. Users can access these logs in accordance with S's policies.

Table 1: Registration Protocol

User		S
	$\xrightarrow{ID,r,c_{ku}}$	
	$\xleftarrow{r,s}$	
	$\xrightarrow{s,ref_{h_i}}$	
	$\xleftarrow{t,k_i}$	

Table 2: Client/Server Verification Protocol

c_i		S
	$\xrightarrow{t,r,h_i}$	
	$\xleftarrow{t,r,V(h_i),S_{kr}(t,r,V(h_i))}$	

Table 3: One to One Verification Protocol

c_i		S
	$\xrightarrow{t,r,h_i,t_{c_j}}$	
c_j		S
	$\xleftarrow{t_{c_i},r,V(h_i),S_{kr}(t_{c_i},r,V(h_i))}$	

Table 4: Multiple Verification Protocol

$t_{c_{i_{list}}}$		S
	$\xrightarrow{t,r,h_i,t_{c_{j_{list}}}}$	
$t_{c_{j_{list}}}$		S
	$\xleftarrow{t_{c_{i_{list}}},r,V(h_i),S_{kr}(t_{c_i},r,V(h_i))}$	

6 REMOTE HSV PROTOCOLS

An electronic signature (and the results of verification) is more binding and versatile than other biometric authentication schemes. This gives rise to many possible authentication scenarios. This section describes the setup and registration of the scheme and authentication protocols for performing verification.

Setup - S sets up the system, publishes a public key, S_{ku}, and keeps private key, S_{kr}, secret.

Registration - A user must register with S. This protocol is shown in Table 1. A user first obtains S_{ku} in order to encrypt information sent to S. A user submits a request to S with proof of identity, ID, a random number, r, and the user's public key, c_{ku}. S acknowledges this request, returns r and another random number, s (encrypted using c_{ku}). The user generates a signature reference file, ref_{h_i}. S saves ref_{h_i} and issues the new client with a certificate, t, and an initial session key, k_i.

Client/Server Verification - To begin the verification process the client c_i must first establish a connection with the server S (see Table 2). All information is encrypted using k_i. c_i transmits his/her handwritten signature, h_i, to S. Given h_i, the verification algorithm either returns a $true$ or $false$ value indicating the success of the verification, that is, $V(h_i) = true$ means that the signature has been accepted as authentic or $V(h_i) = false$ meaning that the signature was rejected as a forgery. S signs this information using S_{kr}.

One to One Verification - One to one verification involves two clients c_i and c_j, $i \neq j$. Client c_j wants to establish the identity of c_i. c_i provides h_i and the id of the intended recipient, t_{c_j}, to S. S performs $V(h_i)$ and forwards the result and the id of the signer, t_{c_i}, to c_j. This process is shown in Table 3.

Multiple Client Verification - Multiple client verification allows a set of clients to verify themselves to another set of clients. For example, two signatures may be required to perform a transaction on a jointly held bank account. Another situation is where a group of t out of n clients must authenticate themselves. For example, 2 out of 3 CEO's must be authenticated to provide consent on a business contract or 6 out of 10 Senator's votes are needed to pass a bill. This is reminiscent of cryptographic secret sharing schemes. The general protocol is shown in Table 4, where $t_{c_{i_{list}}}, t_{c_{j_{list}}}, i \neq j$ denote sets of clients.

7 SECURITY ANALYSIS

This section provides a security analysis of the proposed system. As stated in Section 2, HSV is a superior form of biometric authentication system as it cannot be subverted in the same manner as fingerprinting, retinal scanning and facial recognition setups. The security of the verification algorithm is based on the HSV methods described in (McCabe, 1997) (see Section 4).

The network security of the scheme is dependent on the underlying cryptographic protocols. All information sent between the clients and the Server is encrypted and digitally signed, therefore it cannot be modified. Key updates can be performed at any time. Timestamping prevents signature data, or the results of verification from being replayed. The Server signs the results of verification, therefore anyone can verify that the handsignature was legitimately accepted or

rejected. The Server retains logs of all transactions. In the case of a dispute (repudiation of a signature, etc.) the logs can be used to resolve the problem.

8 CONCLUSION

This paper describes a system for conducting dynamic handwritten signature verification across a network. A user is able to establish his/her identity in real-time for the purposes of commerce, indication of intent or simply to ensure the identity of communicating parties. The scheme allows complex authentication scenarios to occur between users of the system. The system is more natural/less intrusive to humans, and has a larger application area than other biometric techniques. Security of the scheme is based on the strength of the HSV methods of (McCabe, 1997; McCabe, 2004) and the underlying cryptographic measures.

REFERENCES

Diffie, W. and Hellman, M.E. (1976). New Directions in Cryptography. *IEEE Transactions on Information Theory*, 22, 644-654.

ElGamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory* 31, pp. 469-472.

Gupta, G. and McCabe, A. (1997). A Review of Dynamic Handwritten Signature Verification. Computer Science Department, James Cook University.

Jain, A., Prabhakar, S. and Ross A. (1998). Biometrics-Based Web Access. *Technical Report TR98-33*, Michigan State University.

McCabe, A. (2000). Markov Modelling of Simple Directional Features for Efficient and Effective Handwriting Verification. R. Mizoguchi and J. Slaney (Eds.). PRICAI 2000, LNAI 1886, p. 801.

McCabe, A. (1997). Implementation and Analysis of a Handwritten Signature Verification Technique. *Honours Thesis*, James Cook University.

McCabe, A. (2004). Cooperating Statistical Models for Handwritten Signature Verification. *PhD Thesis*, James Cook University.

Rivest, R., Shamir, A. and Adleman, L. (1978) A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21 (2), pp. 120-126.

Techweb. (1998). Net-Based Fingerprint Security Arrives, http://www.techweb.com/wire/story/TWB19980206S0006

Schneier, B. (1994). A Primer on Authentication and Digital Signatures, *Computer Security Journal*, v 10, n. 2, pp. 63-71.

Schneier, B. (1996). *Applied Cryptography*. J. 2nd Edition, Wiley and Sons, Inc. USA.

Stephen, G. (1994). String Searching Algorithms. *World Scientific*, Lecture notes in Computing - Vol. 3.