TEMPLATE FREE BIOMETRIC E-BANKING AUTHENTICATION

More Trustworthy or False Trail?

Tim French, Marc Conrad
Department of Computer Science and Technology, University of Bedfordshire, Luton LU1 3JU, England

Raymond Brown

Keywords: Identity, user authentication, e-banking, template free biometrics.

Abstract: Identity management is an area that has proved challenging for many e-service providers such as e-banks. The problem is how to authenticate on-line consumers at the initial point of registration and also how to re-authenticate on-line customers each time they wish to access e-banking services. Hitherto, e-banks have adopted several different technological approaches to user authentication. These include traditional user passwords, as well as one-time passwords that necessitate the user operating a specialist device. In order to more fully conceptualise the area it is proposed that e-banks should classify the available and emerging using that we call a "Sign Based Identity Management" approach. One emergent solution is considered in more detail: namely template free biometric authentication. Our contribution suggests that the hitherto neglected area of biometric user authentication for e-banking may not only be more robust than existing whilst also meeting many of the requirements (security, usability, strong trust model, less vulnerable to replay attacks) of existing methods.

1 INTRODUCTION

E-banking providers have deployed a range of techniques to handle on-line user authentication. The use of user passwords being ubiquitous and chip-and-pin cards (with passwords) is commonplace. Biometric techniques have hitherto tended to have been dismissed too often by the banking industry as a whole as being inherently too vulnerable to replay attacks or loss of identity templates leading to an unacceptable risk of loss of identity (Venkatraman and Delpachitra, 2008). There may also deeper organisational cultural reasons for the lack of adoption of biometrics within banking more generally to due to a risk aversion culture and technological conservatism (Constanzo 2006). For example the guidance issued by relevant authorities such as the Federal Finance Examinations Council (*http://www.ffiec.gov*) tends to stress the importance of risk management and the increasing dangers of identity theft in relation to tried and tested methods, rather than promoting the adoption of novel methods. This has led to a culture of conservativism in terms of adopting new technologies, despite the rise in criminal abuse. For example, the FSA (Financial Services Authority) recently identify a worrying rise in online banking fraud losses totalling some £21.4m during the six month to June 2008, a 185% rise compared to 2007 (Financial Crime Newsletter, 2007). Similarly, a recent IBM report (IBM Internet Security Systems X-Force®, 2008) identifies USA and UK based e-banking fraud as one of the fastest growing area of on-line crime. Phishing attacks for example are targeted mainly at USA and UK based e-banks (88%), with a further 8% targeted at financial payment sites. This is due to the high economic return of investment for criminals. Traditional well tried and trusted methods of operating secure e-banking predominate. However the rise of e-crime may force e-banking providers to consider new approaches. Later, we identify a novel variant *template free (voice based) biometric* as offering an alternative for e-bank authentication both at the initial customer e-banking enrolment stage and also beyond enrolment for users on a regular day-to-day basis. The main potential

French T., Brown R. and Conrad M.
TEMPLATE FREE BIOMETRIC E-BANKING AUTHENTICATION - More Trustworthy or False Trail?.
DOI: 10.5220/0003267801110116
In *Proceedings of the Twelfth International Conference on Informatics and Semiotics in Organisations (ICISO 2010)*, page
ISBN: 978-989-8425-26-3

advantage is that (unlike traditional biometric methods) there is no need to generate a client template from a presented biometric. The method is still emerging from the research literature and has not been specifically tailored for e-banking use. Rather, limited trials and test-beds have demonstrated proof-of-concept results using voice speech samples (Wisse, 2006). The semiotic paradigm has offered little support for identity management. Only Wisse (Athan and Howells, 2009) has offered a theoretical extension to Peirce's triadic model of semiosis to take into account the additional complexities of mapping a biological identity to virtual identities. We go on to ground our contribution within a semiotic analytic approach to trusted authentication. This can be seen as a natural extension to a generic semiotic account of an E-trust framework most recently articulated within French (French, 2009).

2 IDENTITY MANAGEMENT: A SEMIOTIC ANALYSIS

Previously one of us has suggested that a novel trust ladder a novel and tailored variant of Stamper's well known semiotic ladder (Stamper, 1973) can prove to be invaluable conceptual tool to clarify matters of trust and security issues in the context of e-bank web-site design as well as in the context of SSL/TLS client-server exchanges (Bacharach and Gambetta, 1997).

Semiotic trust ladder
Social world, organisational trust: Beliefs and reputation. Trust as expectations *Organisational trust, social capital*
Pragmatics of trust: Goals, intentions, trusted negotiations, trusted communications *e-service consumption & provision*
Semantics of trust: Meanings, truth/falsehood, validity *e.g. deception and mimicry on a web-site home-page*
Syntactics of trust: Formalisms, tangible security, trusted access to data, files, software *e.g. PKI, X.509 certificates*
Empiric trust: Cryptographic ciphers, entropy, channel capacity, *e.g. RSA*

Figure 1: A "Universal" e-service semiotic trust ladder.

For each of the layers of the semiotic trust ladder (a close variant of Stamper's famous ladder) an exemplar security/trust aspect is indicated. Clearly the development of a semiotics of security and trust forms a much larger research agenda. This task lies outside the scope of the present paper, though this paper forms a minor contribution to this research agenda. Indeed, that the ladder may prove to be useful in the analysis and classification of e-banking user authentication methods and hence establish a kind of taxonomy of identity management that we coin as *Sign Based Identity Management* (SBIM). SBIM is intended to reveal the inherent characteristics and vulnerabilities of well known user authentication methods used by e-banks and seek to map these to the various layers of the semiotic trust ladder. The trust ladder is reproduced as Figure 1 above.

We suggest that the ladder may prove to be useful in the analysis and classification of e-banking user authentication methods and hence establish a kind of taxonomy of identity management. SBIM is intended to reveal the inherent characteristics and vulnerabilities of well known user authentication methods used by e-banks and seek to map these to the various layers of the semiotic trust ladder.

Tables 1 and 2 that follow present a tentative mapping of key user authentication methods to signs and signal exchanges and known vulnerabilities. This mapping effectively re-factors authentication in terms of the signs and signals being exchanged. It can be seen in Table 1 below that traditional methods suffer from well known weaknesses of social engineering whilst the low adoption of one-time passwords suggests user resistance to adoption. Credentials such as smart cards and chip-and-pin cards suffer from problems of 'cloning' and also offer the possibility of a user presenting such credentials under duress. It has recently been suggested that the optimal (future) method of initial registration identity verification in an EU context may be the use of EU ID cards (Naumann, 2009). Such credentials may be relatively easy to clone. Table 1, contains an entry marked 'template free' biometrics. We later seek to demonstrate applicability to e-banking user registration and site usage through the use of a use case based overview, with supportive mathematical underpinning. SBIM's "added value" is to seek to reveal clearly that every method has known weaknesses and that these are related to the nature of the signs being exchanged at various levels of the trust ladder.

Table 1: User authentication methods compared.

Method	***Signs presented***	***Vulnerabilities***	***UK adoption by e-banks?***
Passwords	Alphanumeric strings (PIN codes)	Shoulder surfing; social engineering	Ubiquitous
Password generated token devices: (Key-fobs) as part of 2 factor authentication	User password (as above) + Key fob generates unique numeric codes every 30 secs.	Counteracts M-in-M attacks but user adoption requires use of specialist devices. Shelf-life typically < 3 yrs	Barclays UK
Visual passwords	User clicks on hot-spots within images / or clicks on one or more arrays of images	Shoulder surfing; poor scalability for e-banking	None
Smart card	Stored encrypted public/private keys	Card cloning	Commonplace
USB Token (as initial part of two factor password based authentication)	Stored user signed digital certs. as part of PKI	Tamper resistant but needs USB port; can be lost by user leading to loss of service availability	Used in USA but not adopted in UK
EU ID Card	As above plus potential for stored biometrics	No ID card available yet across EU. Loss of card. Card cloning.	None
Biometrics	Extract of salient features e.g from voice (template)	Loss of template leads to loss of identity! Specialist devices needed at client end	None (methods are relatively mature and scale well)
Template free biometrics	Salient features generate keys from e.g. voice biometric	May not be scalable?	None still emergent stage

Table 2: Mapping of password user authentication to the trust ladder.

Password	***Trust ladder layer***	***Risk of compromise?***
Password selection and usage	*Social level* determines password strength / social engineering leads to weaknesses /shoulder surfing in internet café etc	***High***
Active attacks	*Pragmatic* level Brute force attack, DDNOS attacks	***Medium***
Phishing attacks (fake web-site)	*Semantic* level Consumers log on to fake site and re-enter password due to lure of fake surface level signs.	***High*** *IBM report*
Key space	*Syntactic* level Can be re-issued	***Medium*** Reissuance involves manual interaction with e-banking human agent to re-establish security. Some possibility for interception and/or abuse.
Ciphers/crypto	*Empiric* level	***Very low*** *Private key only. Mathematically secure through use of hash functions*

Table 3: Mapping of voice template free biometric user authentication to the trust ladder.

Voice template free biometric	*Trust ladder layer*	*Risk of compromise?*
Voice presented by phone	***Social level*** Replay via social engineering	***Low***
Active Attacks	***Pragmatic*** Goals of system re-directed by inherent vulnerability exploits	*Medium*
Phishing attacks	***Semantic level*** Biometric could be stolen but cannot be matched to key pairs unless the secret proprietary algorithm is compromised.	***Low*** *IBM report*
Key space	**Syntactic level** Cannot be reissued if compromised	***Low*** Template free mechanism guarantees that the map from biometric feature to key space can be adapted if necessary.
Ciphers/crypto	***Empiric level*** Digital signal exchange and verification	***V. Low*** Private / public keys generated dynamically and not stored at client end. Unbreakable.

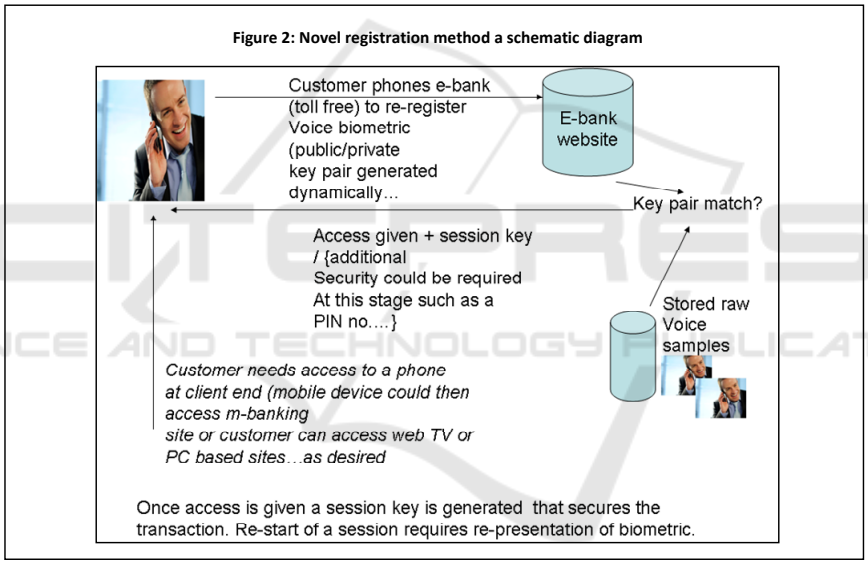

Figure 2: Novel registration method a schematic diagram.

Tables 2 and 3 show how passwords present a relatively high risk of compromise as compared to template free biometrics, when examined in terms of their vulnerabilities. This is because any adversary would typically need to mimic genuine signs at multiple layers of system and user abstraction, making the task potentially harder. Passwords offer more vulnerable layers (higher risk) than biometrics.

- In the context of e-banking the system dynamics are: large scalability, high-volume, high accuracy and reliability. The analysis presented earlier suggests that e-banks should consider supplementing their use of passwords and/or smart cards with a template free biometric approach. Organizations are using or actively considering multi-factor authentication techniques, despite increased management overheads (Chiasson, 2008).

3 VOICE BASED TEMPLATE FREE USER AUTHENTICATION AND E-BANKING

3.1 Overview

The traditional procedure for opening an on-line

bank account (enrolment) typically involves the customer entering a high-street branch and presenting evidence of ID, a copy of their signature and evidence of domicile.

The bank often checks the credit score of the customer, and after these checks are made the customer is mapped to one or more accounts. Later, the customer receives bank credentials (e.g. card, passwords etc.) that enable transactions to be made on-line. A variation of the above process involves the initial capture of information from an on-line customer, followed by verification of identity (off-line) and issuance of credentials to the customer so that the account can be activates and operated on-line.

Atah and Howells (Athan and Howells, 2009) claim to have developed a so called *template free authentication* system. Here the encryption key is devised directly from the measured features. It should be noted that a simple hash algorithm would not be appropriate in this situation as even a small change in the recorded features would imply a completely different hashed value. The algorithm uses voice features, normalizes them and produces data which is *discretised*. The use of voice based template free biometric would typically involve an initial visit to a branch followed by seamless on-line usage. Thus the initial workload of enrolment would be somewhat higher than the traditional method. This (recording) would need to be accompanied by manual ID document presentation as in the traditional method for additional security reasons.

The e-banking customer presents a voice biometric, by means of any voice enabled IP connected device. To avoid replay attacks a daily 'passphrase' could be embedded within their free voice text entry.

3.3 Empiric Level: A Novel Centred Discretisation Approach

In an e-banking context it is always the case that an e-bank needs to verify that the presented credential matches the stored credential. The most vulnerable situation is that of an e-bank storing the clear text voice sample (as shown in Figure 2). In this case if the sample is stolen a person's identity is also stolen. A better case is when the e-bank stores only a hashed value of a voice sample. In this case loss would not result in a loss of identity due to the difficulty of reversing such hash functions. The difficulty of generating a unique hash value from differing presented voice samples generated by the customer remains problematic. Our solution is based upon *centred discretisation* techniques. These techniques retain the advantages of template free biometric method (no potential loss of identity if the discretised samples are stolen) whilst enhancing the practicability of an e-bank correctly matching the hashed values of the presented credential to the stored credential. We suggest that centred discretisation provides a potentially more stable approach, as depicted schematically in Figure 3 below.

Table 4: a risk analysis of the template free method.

Semiotic trust ladder	***Vulnerabilities of template free method***
Social world, organisational trust: Beliefs and reputation. Trust as expectations *Organisational trust, social capital*	Adoption may be limited by consumer fears concerning possible misuse of presented voice biometric
Pragmatics of trust: Goals, intentions, trusted negotiations, trusted communications *e-service consumption & provision*	Customers are adverse to adopting biometric methods in general for e-finance in the UK. Past track record of introduction (for ATM's) failed due to user (over engineering) reactions.
Semantics of trust: Meanings, truth/falsehood, validity *e.g. deception and mimicry on a web-site*	Robust algorithms needed to ensure robustness to replay attacks, user forced under duress to submit biometric by adversary etc.
Syntactics of trust: Formalisms, tangible security, trusted access to data, files, software *e.g. PKI, X.509 certificates*	No trusted standard (yet) developed unlike other systems that are ANSI certified.
Empiric trust: Cryptographic ciphers, entropy, channel capacity	Template free discretisation of continuous data may constitute a problem of matching stability.

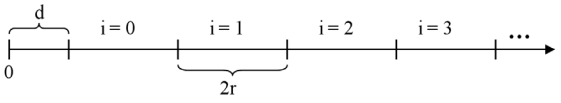

Figure 3: Continuous line (0..∞) divided into segments of length 2*r* (adapted from (14).

The centred discretisation algorithm is discussed in (Chiasson, 2008), in the context of *graphical* passwords. We have adapted the method so as to match the needs of e-banking voice verification.

4 CONCLUSIONS

The adoption of novel user authentication technologies by e-banks is a complex affair. From a semiotic analytic viewpoint barriers and vulnerabilities exist at several layers of the trust ladder not only at the tangible security layer. Whilst the template free approach offers the future prospect of a generally more robust solution to e-banking user authentication, concerns remain, particularly as to the reaction of on-line customers and with respect to the ease with which unique bit strings can be generated within a fault free context from presented samples. Future work includes an e-banking provider survey and initial exploratory partnerships with one or more UK e-banks, so as to seek active support for the adoption of voice based template free biometrics. Before adoption, enhancements such as the centred discretisation method will be needed and scaled to meet the demands of security, trust and user acceptance of such novel technologies. Existing technologies are weak and liable to abuse by criminals. To simply maintain the *status quo* may not prove viable.

REFERENCES

Venkatraman, S. and Delpachitra, I. (2008) Biometrics in banking security: a case study. *Journal of Information Management and Computer Security*,6 (4), 415-430.

Costanzo, C. (2006). Suddenly, biometric ID doesn't seem like science fiction, *American Banker*,

Vol. 171 No. 107, pp. 6-11.

Financial Crime Newsletter (2007). Special edition from the Financial Crime Sector Team

Issue No.8, August 2007 *Authentication and Safeguarding of Customer Identity*, FSA Publications.

IBM Internet Security Systems X-Force® 2008 Trend & Risk Report, Available as a PDF from: http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf

Wisse, P. (2006). Semiotics of Identity Management. Prima Vera Working Paper Series,

University of Amsterdam, Working Paper 200602.

Atah, J., Howells, G. (2009). Mapping of Information in Voice Features for use in an Efficient Template - Free Biometric Security System, International Conference on Information Security and Privacy (ISP-09), Orlando, Florida, USA.

French, T. (2009). Towards an E-service Trust Framework: Trust as a Semiotic Phenomenon, PhD Thesis, School of Systems Engineering, Reading University, UK.

Bacharach, M. & Gambetta, D. (1997). Trust in Signs. In: Cook, K.S. (Ed.). Trust in Society. Russell Sage Foundation. New York, 148–184, 1997.

Clayton. (2005) Who'd phish from the summit of Kilimanjaro? Procs. 9th International Conference FC 2005, Roseau, The Commonwealth of Dominica, February 28-March 3rd 2005, Vol. 3570 of LCNS,91-92, Springer-Verlag.

Clayton. (2005). Insecure real-World Authentication Protocols (or why Phishing is so Profitable).Procs. 13th International Workshop on Security Protocols, Cambridge, UK.

Wu, M. (2006). Fighting Phishing at the User Interface. PhD Thesis. MIT, August 2006.

Stamper, R. K. Information in Business and Administrative systems. New York: Wiley, 1973.

Naumann, I. (2009) (Ed.) 'Privacy and Security Risks when Authenticating on the Internet with European eID Cards', ENISA Risk Assessment Report.

Chiasson, S., *et al.,* (2008).Centered Discretization with Application to Graphical Passwords, in USENIX Usability, Psychology, and Security (UPSEC). 2008.