Position Paper: On Approaches for Selecting Automated Personal Identification Mechanisms (APIMs) *

Anthony J. Palmer
Information Security Group, Royal Holloway, University of London
Egham, Surrey, United Kingdom
anthony.palmer@rhul.ac.uk

ABSTRACT

We contend that ASMSA (Approach for Selecting the Most Suitable APIM) [31], which incorporates stakeholder participation and systematic decision-making processes, is the optimum methodology to select the most suitable APIM for a given context.

1. INTRODUCTION

We observed an interesting debate at SOUPS 2007 between the proponents and the audience regarding the use of a gaze-based PIN entry solution for identifying cardholders withdrawing money from cash machines [24]. As with many of these types of debate about digital identification, the technical proposal was defended well and the audience identified vulnerabilities, e.g. environmental lighting impacting accuracy, and issues, e.g. exclusion of poorly sighted customers. It was recognised, by many present, that evaluation criteria for APIMs would not only assist these debates but also the actual selection of the most suitable human identification mechanism for a particular context.

Automated Personal identification, as defined in this paper, applies to all of the various methods that computer systems use to establish the identity of individual [42], which include user authentication, biometric verification and biometric identification solution types. Organisations introduce APIMs to manage their business risks associated with information assets, e.g. payment card transactions, or to open new service delivery channels, e.g. eGovernment services to citizens, cost effectively [5]. Conversely, users want to perform their tasks quickly and easily, preferably without cumbersome or intrusive identification routines [1].

Ineffective APIMs impact upon organisations and their user communities, as evidenced by [36], resulting in unacceptable risks and societal issues. Poorly designed APIMs are exploited through vulnerabilities ranging from technological deficiencies as identified by [34] to inappropriate or inadvertent user actions, as noted by [28]. Unreliable APIMs may also adversely impact critical life-threatening situations, as a consequence of inappropriate user authentication controls in health information systems [18].

It seems expedient, therefore, to establish methodologies which can determine the most suitable APIM for a given context in order to minimise vulnerabilities, costs and address user community issues in terms of acceptability, accessibility and usability. We argue that APIMs should be selected using a participative design approach [29], by engaging all relevant stakeholders, including the user community, and systematic decision processes.

1.1 Selection Approaches Practised

Commercial methodologies for Identity Management (IdM) [7] concentrate on the protection of organisation's interests, i.e. corporate employee or customer identification and access control to assets.

These IdM methodologies [13, 14] are based on capability maturity modelling [23, 41], which focuses on organisational processes for asset protection and legal compliance rather than ascertaining the optimal solution to identify users in the community with their respective tasks. It appears that IdM methodologies do not give sufficient regard to community acceptance, accessibility and usability in these enterprise identification contexts.

Additionally, evidence confirms that organisation's primary objectives are not being met as fraudulent activity continues to increase [8], which suggests that some APIM implementations may not be suitable and approaches currently practised may need reconsideration.

For some heterogeneous identification contexts, e.g. national eID Cards, there is reliance on the competencies of experts (i.e. no systematic methodology) and, in some contexts, the use of pilot exercises to trial alternative solutions [27] rather than devoting effort to document objectives and requirements [38]. For example, the Belgian eID Card Programme commenced over a decade ago, employed a pilot exercise, and may be considered to be the most mature eID Card implementation in the EU; however, as a key component to the Belgian eGovernment's initiative, it has serious vulnerabilities [39] and remains under utilized by its citizens [26].

1.2 Towards Participative Approaches

Broad heuristics for assessing biometric solutions [20] and high-level frameworks for evaluating the properties of IdMs [21] exist; however, we consider that more emphasis needs to be placed on the relevant stakeholders', including the intended user community, aims and objectives surrounding the context's human identification challenge. Importantly, there is now recognition [20] that more attention needs to be paid to problem analysis in this space, in order to avoid unintended and counter-productive side effects of selecting unsuitable APIMs, by undertaking assessments from alter-

(EuroSOUPS) 2010, November 24, 2010, Newcastle, UK.

native perspectives.

Generic approaches, as proposed by [35, 3], evaluate the organisational values of enterprise IdM Systems, which are based upon the balanced business scorecard method. Return on Security Investment (ROSI) evaluations can, it is claimed [11], provide both tangible and intangible measurement of security controls; however, we consider risk and control values for organisations do not address acceptability issues [37], usability issues [19, 10, 1], accessibility issues [33] or assess the impact upon society [4].

Efforts to determine the suitability of APIM using quantitative methods [32, 37], with evaluation criteria may be applied heuristically to some contexts. Nevertheless, we consider that the suitability of an APIM, which can impact a large or diverse user community and involve many complexities, is better determined by applying a qualitative methodology. We also consider that these complexities should form the attributes in an evaluation framework, to model the relationships between the differentiating factors. We also consider that a selection method must accommodate mixed data types. We acknowledge, however, that some processes, such as the ordering of preferences, are quantitative tasks.

We consider that striking the right balance between stakeholders' objectives is key to the selection of the most suitable APIM in any context. As with other information security systems, achieving this goal requires collaborative and transparent processes together with, crucially, user participation [12]. A systematic evaluation approach not only helps communication between interested stakeholders but also provides evidence to justify to others the reasonableness of the proposed decisions [17].

All APIMs have vulnerabilities, costs and issues [30] and inevitably, organisational decisions may demand some trade-offs; however, stakeholders' preferences and requirements should still be established before the various identification solutions are even evaluated [9]. Equally, rectifying an APIM implementation may not always be an easy course to pursue. Essentially, stakeholders, particularly the APIM owners, need to determine whether the APIM is the most suitable by establishing a complete set of requirements or Key Performance Indicators. These requirements are essential for evaluation purposes. Quality models, with comprehensive evaluation criteria, not only facilitates better informed and, therefore, rational decision-making, but also improves a project's success rate [2].

2. THE ASMSA METHODOLOGY

We have introduced ASMSA[31], comprising of systematic decision-making and stakeholder consultation processes, to capture and reconcile all objectives and requirements in a given context.

ASMSA's evaluation framework models the Strategic Aims, Operational Requirements and Solutions' Attributes perspectives using established criteria to evaluate APIMs [30]. Its three-stage selection method draws on Multi-Stakeholder Processes (MSPs), as described by [22], as a means to help reconcile the stakeholders' objectives and incentives for the introduction of the APIM. ASMSA's selection method also uses a Multi-Objective Multi-Criteria (MOMC) technique, which, according to [16], explicitly recognises the existence of many points of view and more than one set of qualities in a decision process.

Stakeholder objectives, within policy and constraints, are established and reconciled, which help to inform operational requirements for the APIM. These requirements describe the functionality, performance and assurance testing schemes for the APIM as a discrete application, e.g. verifying the holder of an ePassport, or one that forms part of a transaction, e.g. Internet banking. Candidate solutions are then compared against these stated requirements. They are also assessed in terms of adequacy of their information security architecture, reliability, accessibility and usability.

3. SUMMARY

Criteria for evaluating APIMs, developed over the decades from various perspectives [40, 15, 33], have been consolidated [30]; however, methodologies established for selecting APIMs require theoretical and practical validation.

Effort is now required to validate the efficacy of ASMSA against other methodologies and current practices, using the criteria below proposed by [25], which could be applied for enterprise, federated and heterogeneous identification context types:

1. Execution time required;
2. Size of problem considered (dimensionality and proportionality);
3. Accuracy of selection in respect to optimal decision variables and/or objective function;
4. Simplicity in use;
5. Simplicity of computer program to execute algorithms and processes; and
6. Capable of application to real world problems.

We anticipate that some methodologies may be more appropriate than others in certain circumstances. Essentially, the development of a mature attitude towards digital identity is needed by all stakeholders to enable enterprises and society to then take full advantage of digital identification technologies [6].

4. REFERENCES

[1] A. Adams and A. Sasse. Users are not the enemy: Why users compromise security mechanisms and how to take remedial actions. In L. Cranor and S. Garfinkel, editors, *Security & Usability*, pages 639–649. O'Reilly Media, Inc, California,USA, 2005.

[2] A. Al-Khouri. Using Quality Models to Evaluate National ID Systems:the Case of the UAE. *International Journal of Social Sciences*, 1(2):117–130, 2007.

[3] N. Alush-Aben. IDMology: Coherent Identity Management Methodology. Technical report, ID Focus, 2005.

[4] R. Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems Second Edition*. Wiley Publishing, Inc, Indionapolis, USA, 2008.

[5] R. Anderson and T. Moore. The economics of information security: A survey and open questions, 2007.

[6] D. Birch. Victorian values: Politicians and the public incorrectly see security and privacy as opposites. *Information Security Technical Report*, 14:143–145, 2009.

[7] BT Identity Management. Identity Management Quick Start Service. Technical report, British Telecommunications plc, 2006.

[8] CIFAS The UK's Fraud Prevention Service. Identity fraud levels continue to rise. Technical report, 2010.

[9] Common Criteria Biometric Evaluation Methodolgy Working Group. Common methodology for information technology security evaluation - biometric evaluation supplement. Technical report, Common Criteria Interpretation Management Board, 2002.

[10] L. Coventry. Usable biometrics. In L. Cranor and S. Garfinkel, editors, *Security & Usability*, pages 175–197. O'Reilly Media, Inc, California,USA, 2005.

[11] L. Dadayan. Measuring Return on Government IT Investments. Proceedings of the 13th European Conference on Information Technology Evaluation, 2006.

[12] R. Dean and J. Hoskins. Identity Management: Back to the user. *Network Security*, pages 4–7, December 2007.

[13] Department of Finance and Regulation. Identity Management for Australian Government Employees Framework (IMAGE). Technical report, Australian Government, 2008.

[14] P. Englebert. 5 keys to a successful identity and access management implementation. Technical report, CA Services Global Security Practice, December 2007.

[15] V. Fak. Computer verification of human users identity: a theoretical model and some evaluation criteria. *Computers & Security*, 10:626–36, 1991.

[16] B. Farbey and A. Finkelstein. Evaluation in Software Engineering: ROI, but more than ROI, 2001.

[17] R. Feeney, H. Raiffa, and R. Meyer. *Decisions with Multiple Objectives: Preferences and Value Trade-offs.* Cambridge University Press, 1993.

[18] A. Ferreira, R. Cruz-Correia, L. Antunes, and D. Chadwick. Access control: how can it improve patients' healthcare? *Studies in Health Technology and Informatics*, 127:65–76, 2007.

[19] S. Furnell. Making security usable: Are things improving? *Computers & Security*, 26:434–443, 2007.

[20] J. Grijpink. Identity fraud and biometrics –An assessment model for the use of biometrics. *Computer Law & Security*, 22:316–319, 2006.

[21] M. Guel. A framework for choosing your next generation authentication / authorisation system. *Information Security Technical Report*, 7:63–78, 2002.

[22] M. Hemmati. *Multi-stakeholder processes for governance and sustainability: beyond deadlock and conflict.* Earthscan Publications, London, UK, 2002.

[23] J. Hughes. An Identity Management Maturity Model. *Information Security Bulletin*, 11:99–105, April 2006.

[24] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd. Reducing shoulder-surfing by using gaze-based password entry. In *Symposium on Usable Privacy and Security (SOUPS)*, 2007.

[25] Y. Lai and C. Hwang. *Fuzzy Multiple Objective Decision Making: Methods and Applications.* Springer-Verlag, Berlin, 1994.

[26] J. Lapon, V. Naessens, B. Verdegem, P. Verhaeghe, and B. De Decker. Building Advanced Applications with the Belgian eID. *Security and Communications Networks*, 2010.

[27] MiSense Trial Members Group. Summary report: Biometrically enabled access control trial at Heathrow Airport 2007. Technical report, 2007.

[28] K. Mitnik, L. Simon, and W. Simon. *The art of deception: controlling the human element of security.* John Wiley & Sons, Inc, 2002.

[29] E. Mumford. A socio-technical approach to systems design. *Requirements Engineering*, 5:125–133, 2000.

[30] A. Palmer. Criteria to Evaluate Automated Personal Identification Mechanisms. *Computers & Security*, 27:260–284, November December 2008.

[31] A. Palmer. Approach for Selecting the Most Suitable Automated Personal Identification Mechanism (ASMSA). *Computers & Security*, 29:785–806, October 2010.

[32] K. Renaud. Quantifying the Quality of Web Authentication Mechanisms –A Usability Perspective. *Journal of Web Engineering*, 3(2):95–123, 2004.

[33] K. Renaud. Evaluating authentication mechanisms. In L. Cranor and S. Garfinkel, editors, *Security & Usability*, pages 103–128. O'Reilly Media, Inc, California,USA, 2005.

[34] C. Roberts. Biometric attack vectors and defenses. *Computers & Security*, 26:14–25, 2007.

[35] D. Royer and M. Meints. Enterprise Identity Management - Towards a Decision Support Framework based on the Balanced Business Card Approach. *Business & Information Systems Engineering*, 3:245–253, 2009.

[36] Synovate. 2006 Identity Theft Survey Report. Technical report, US Federal Trade Commission, November 2007.

[37] D. Toledano, R. Pozo, A. Trapote, and L. Gomez. Usability evaluation of multi-modal biometric verification systems. *Interacting with Computers*, 18:1101–1122, 2006.

[38] United Kingdom Biometrics Working Group. Use of Biometrics for Identification and Authentication - Advice on Product Selection. Technical report, UK Government-Office of the e-Envoy, 2002.

[39] P. Verhaeghe, J. Lapon, V. Naessens, B. De Decker, K. Verslype, and G. Nigusse. Security and Privacy Threats of the Belgian Electronic Identity Card and Middleware. 2007.

[40] G. Warfel. *Identification Technologies: Computer, Optical and Chemical Aids to Personal ID.* Charles Thomas, Springfield, Illinois, USA, 1979.

[41] P. Windley. *Digital Identity.* O'Reilly, Sebastopol, 2005.

[42] J. Young and D. Raphael. Automated Personal Identification. Technical report, Stanford Research Institute, 1974.