18

A comprehensive authentication and supervision architecture for networked multimedia systems

S.M.Furnell[†], H.M.Illingworth[†], S.K.Katsikas[‡], P.L.Reynolds[†] and P.W.Sanders[†]

[†] Network Research Group, School of Electronic, Communication and Electrical Engineering, University of Plymouth, Plymouth, United Kingdom.

[‡] Research Unit, University of the Aegean, 30 Voulgaroktonou Street, Athens, Greece

E-mail : stevef@pbs.plym.ac.uk, heleni@pbs.plym.ac.uk

Abstract

The paper identifies the need for improved user authentication and supervision techniques within local security domains. Whilst there are now appropriate standards for the security of inter-domain operations, authentication of the users within them is often still reliant upon measures that are open to compromise and which provide no safeguard against system misuse.

The discussion presents an overview of various potential authentication and supervision techniques (largely based upon a combination of physiological and behavioural biometrics), discussing the relative advantages and disadvantages of each from an implementation perspective.

The discussion then proceeds to consider how these approaches may be integrated into a comprehensive architecture for user and system supervision entitled IMS (Intrusion Monitoring System). The conceptual approach of this system is described, with details of the functional modules involved and the intended operation of the monitoring process.

The paper concludes by considering how the supervision approach would be integrated into a wider security framework, involving inter-domain operation and Trusted Third Party (TTP) certification.

Keywords

Authentication, Intrusion Detection, Biometrics, Trusted Third Party.

Communications and Multimedia Security Vol. 3 S. Katsikas (Ed.)

1 INTRODUCTION

As information technology systems assume ever more importance in the successful operation of modern organisations and societies, so the need for adequate means of ensuring authorised and correct use of facilities within and between systems becomes increasingly essential. Methods exist to enable the authentication of communicating parties between domains, along with the confidentiality, integrity and non-repudiation of transmitted data / messages (CCITT 1989). However, trust and certification between domains is only appropriate if adequate authentication can be performed within the individual systems involved.

In most traditional systems the principal means of user authentication is via the password. Whilst relatively acceptable in terms of ease of use and implementation, the weaknesses of passwords (e.g. vulnerability to compromise through poor selection and infrequent change) are well documented (Jobusch and Oldehoeft 1989). Even smart cards cannot provide a guarantee of user authentication, and systems may still be vulnerable to compromise in some circumstances (e.g. if the legitimate user leaves an active session unattended). In addition, smart cards do not provide any inherent protection against system misuse by authorised users. Finally, such an approach may be considered impractical as a compulsory measure due to the immediate financial burden associated with the installation of card readers and issuing of cards. As such, there is a need for other approaches to authentication, which do not sacrifice advantages such as ease of use.

2 APPROACHES TO AUTHENTICATION AND SUPERVISION

A number of methods may be appropriate to the above requirements, based upon a combination of physiological and behavioural biometric techniques. The principles behind these are described in the paragraphs that follow, along with an indication of their effectiveness where possible (note: effectiveness in this context relates to the False Acceptance and False Rejection Rates - FAR and FRR - associated with each measure). All of the characteristics would be assessed and held in a *profile* for each legitimate system user within the monitored domain.

- *Face Recognition*
  Face recognition is a physiological biometric technique that most people use every day in order to recognise others. Everyone has unique facial characteristics that distinguish them from others. Research into this area has proven to be successful, with authentication judgements made within 1.5 seconds and an error rate of 2.5% (Secure Computing 1995). There are several different methods for achieving this, including pattern recognition, neural networks, von der Malsburg's graph matching and isodensity maps.

  Additional hardware and software is required to enable face recognition to be used. A video camera with video-capture board, as well as appropriate software will be needed for each workstation to be monitored. At the present time, this would prove to be an expensive exercise, although with multimedia and video-conferencing becoming increasingly common, costs are likely to reduce.

With a small camera positioned on a monitor, users could be monitored continuously or perhaps periodically, to verify that the user logged-in is the legitimate owner of the account. This would provide stronger authentication than the current initial login methods.

- *Voice Recognition*

  Voice authentication techniques are already being used for physical access control, access to long distance telephone lines and voicemail. Voice authentication differs from speech recognition in that it tries to distinguish one person from another. It is not concerned with the words spoken but with their spectral content. On the other hand, speech recognition distinguishes one word from another and attempts to ignore speech characteristics.

  A typical system works by recording and storing the user's voiceprint. Once this has been done, a user speaks a password or phrase which is then compared to the stored voiceprint. If verified, the user gains access to the system. Some more advanced systems have the capability of adaptively updating the voiceprint records. This has the advantage of tracking any changes to a user's voice.

  As with face recognition, additional hardware and software will be required although both the complexity and cost of the hardware is much lower. This technique would most commonly find a role as an initial password verification tool and has limited potential for continuous monitoring. However, wider use would be possible if a subject routinely uses dictation tools or similar.

  Typical error rates for this technique are claimed to be an FRR of 1% and an FAR of as low as 0.0001% (Cope 1990).

- *Keystroke Analysis*

  Keystroke analysis refers to the verification of user identity through the monitoring and assessment of typing characteristics, based on the assumption that the difference in style between the legitimate user and an impostor is likely to be very marked. A number of factors may provide a basis for discrimination, including inter-keystroke times, keypress duration and typing error frequency.

  Keystroke analysis may be implemented in two ways - termed the static and dynamic verification strategies. In the static scenario, authentication is based upon entry of a known text string, such as a username and password. The information would be entered as usual, but the system would also analyse the way in which it was typed. By contrast, dynamic analysis is based upon any arbitrary keyboard input, allowing greater scope for continuous user supervision. Both approaches have been subject to a number of experimental studies and typical measures of effectiveness are 0.5% FAR and 3.1% FRR for the static approach (Bleha et al. 1990) and 15% FAR and 0% FRR for the dynamic approach (Furnell et al. 1996).

- *Mouse Dynamics*

  Mouse dynamics is a new area of research which involves monitoring characteristics of mouse usage. Current research is looking at measurements of speed and acceleration in order to distinguish one person from another. These measurements may be taken without the need for any physical changes to the current mouse design and require only minimal software changes. These measurements can be taken when a user makes a selection from a pull-down menu, moves the pointer or uses the mouse in other ways.

  Mouse dynamics monitoring is limited to Graphical User Interface (GUI) environments where mouse usage is greatest. A recent exploratory study gave an average error (FAR/FRR combined) of between 14% and 39% (Barrelle et al. 1996), indicating

that the technique requires further refinement before it is comparable with some of the other approaches.

- *Behaviour monitoring*
  This technique is based upon the monitoring of the users interaction with the system. It is founded on the premise that everyone has their own characteristic or preferred way of doing things when using a system. As such, behaviour monitoring may actually encompass a number of further profiled characteristics, some examples of which are given in Table 1 below.

Table 1 Potential characteristics for behavioural profiling

Characteristic	*Description*
Access Time	Time(s) between which subjects typically access IT systems. In some cases there may be a detectable correlation between access time and application usage, allowing a continuous measure.
Access Location	May be approached from two perspectives : monitoring the location(s) from which subjects typically access IT systems OR monitoring which subjects normally access from any given terminal / port.
OS Command Usage	Type and frequency of operating system commands used.
Application Use	Type and frequency of application systems used.
User Interaction	Monitoring of the method(s) by which a subject commonly interacts with the system / applications (e.g. keyboard or mouse, commands or menus).
Resource Usage	Statistics of typical usage of system resources (e.g. CPU, memory, disk) associated with each subject.
Access Violations	Tracking of the number of access violations (e.g. to files, data, applications, devices) made by a user / process during a session.

Individual behaviour profiles would need to be developed using data collected over a reasonably long time period, in order to establish what constitutes "normal" behaviour for each legitimate user.

Effectiveness in this case would depend upon the exact combination of characteristics being monitored and, as such, it is not possible to give a general figure. The approach is a key element of a number of intrusion detection systems, including IDES (Lunt 1990) and SecureNet (Androutsopoulos et al. 1994).

It is acknowledged that there are a number of other biometric authentication measures that may also be technically feasible, including fingerprint analysis, hand geometry or signature recognition. However, these are considered to offer less potential for transparent or continuous integration into the supervision system, given that they require more specific actions on the part of the user. In addition, the required hardware in each of these cases would not be a likely "standard" feature of any system (multimedia or otherwise) and would, therefore, represent an additional expense. The perceived advantages and disadvantages of the chosen approaches are presented in Table 2.

Table 2 Advantages and disadvantages of authentication / supervision approaches

Method	*Advantages*	*Disadvantages*
Face Recognition	• Low error rates • Continuous monitoring	• Requires extra hardware • Complexity and cost • Restricted number of users due to database size and complexity • Will not detect insider attacks
Voice Recognition	• Low error rates • Most mature technology of the techniques discussed	• Requires extra hardware • Complex • Generally restricted to initial login • Will not detect insider attacks
Keystroke Analysis	• Continuous monitoring • Low cost • Works with existing systems requiring no extra hardware	• Experimental technology • Will not detect insider attacks • For continuous monitoring, can only be used in keyboard-intensive applications (e.g. word-processing)
Mouse Dynamics	• Continuous monitoring • Low cost • Works with existing systems requiring no extra hardware	• New technology • Will not detect insider attacks • For continuous monitoring, can only be used in GUI-based applications
Behaviour Monitoring	• Continuous monitoring • Detects insider attacks • Low cost • Works with existing systems requiring no extra hardware	• New technology

It is possible to categorise the techniques into different groups, according to the general strength and reliability of the authentication / supervision measures that they deliver. As such, they can be seen to reside at different "confidence levels", as illustrated in Figure 1 below (note that, for simplicity, the measures are split into just three levels, although there could conceivably be more in practice).

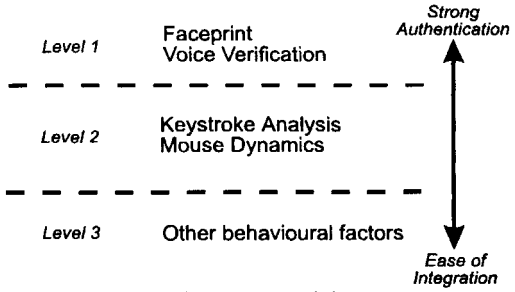

Figure 1 Comparison of the authentication / supervision measures.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.