Minòs: Extended User Authentication

Michael Newberry

Centre for Computer Security Research
Department of Computer Science
University College
The University of New South Wales
Australian Defence Force Academy
Canberra. ACT. 2600

ABSTRACT

Minòs is a preprocessor for commands issued to the UNIX operating system. It uses information about how a user is working to continually authenticate them. Minòs learns with the user as they develop new habits with the computer. This paper describes in detail the plans for Minòs, and their realisation to date.

1 Introduction

This way I went, descending from the first
into the second circle, that holds less space
but much more pain — stinging the soul to wailing.

There stands Minòs grotesquely, and he snarls,
examining the the guilty at the entrance;
he judges and dispatches, tail in coils.

By this I mean that when the evil soul
appears before him, it confesses all,
and he, who is the expert judge of sins,
knows to what place in Hell the soul belongs;
the times he wraps his tail around himself
tells just how far the sinner must go down.
The damned keep crowding up in front of him:
they pass along to judgement one by one;
they speak, they hear, and then are hurled below. [2], p. 109

1Michael Newberry is supported in part by the Australian Telecommunications and Electronics Research Board
In Dante's Hell, Minős was the magistrate to the damned. He examined the actions of those condemned, and accordingly assigned each a place for eternity. Unlike Dante's magistrate, computers frequently assess the character of users from their words, not from their actions. The idea of using the behaviour of a user as a guide to their identity has found little application in computer security. This paper describes the Minős system, developed by the author since 1987. This Minős uses information about how a user operates a computer, to identify breaches in security.

There have been three other efforts at analysing user actions in order to identify intrusions (these are summarised in [11], p. 378). Denning's Intrusion Detection System uses elaborate database techniques to monitor computer resource usage (see [3] for the theoretical model). To date it has used "connect time, shift of login, and location of login" ([6], p. 63) as detection metrics. Its emphasis has been on identifying an intruder from exceptional behaviour. A similar approach is reported in [4]. There, the authors looked for features that were typical of intruder sessions, in order to detect future intrusions. Their emphasis was on identifying typical "intruder behaviour". A different approach was used in [12]. Here, the author developed models of typical user behaviour, and then identified potential intrusions from their deviation from this behaviour. The emphasis was on modelling the user, and identifying intruders by their deviation from the user's normal behaviour, rather than seeking characteristic intruder behaviours. This is also the approach used by the computer system Minős.

Minős acts as a filter between the user and the operating system (in this case UNIX\(^2\)). Minős continually examines the actions of the user, looking for uncharacteristic behaviours that may indicate an intruder at work. Upon finding such behaviour, Minős will be capable of a variety of responses, depending on the individual site's requirements (see [8], p. 171).

Minős is capable of using many metrics to identify users. It is planned to use four in the current implementation:

- The user's choice of commands
- The user's sequencing of commands
- The user's location in the computer (That is, which directories/folders are accessed by a user)
- The way a user types (This is measured by examining the intervals between the keystrokes of the user)

\(^2\)UNIX is a trademark of AT&T Bell Laboratories