User Unique Identifcation

Terry Jones
Mike Newberry
Jennifer Seberry

Basser Department of Computer Science
University Of Sydney

Traditionally, users have been authenticated by asking them to provide some form of password. This password has been stored securely in the computer and used to check the identity of the user at various times, such as when they first log on. However such authentication only proves that the challenged user knows the password — it doesn't identify the user. This has often been a security problem in time-shared computer installations, when unauthorised users (the proverbial "hackers") have obtained the passwords of valid users and used these to penetrate the site's security.

This has led to much work to identify users uniquely by more secure means, such as fingerprints. Such measures all try to identify a user by checking some attribute of the person. In what follows we will discuss various identification schemes based upon work done at the University of Sydney.

1. Type-Signatures

The idea of a *type-signature* is one such approach, first proposed by Terry Jones [Jones1985]. It incorporates a statistical measure of the typing style of the user.

1.1 Type-signature Password Systems

In December 1986 we commenced testing the concept of the type-signature[1]. Over the next two months several mini password systems, based around this concept, were developed and installed by Mike Newberry on various machines to test them under different conditions (all of these machines were DEC VAX 11/780's running various forms of UNIX). These systems checked both the type-signature and the password when a user attempted to log-on. The type-signatures were allowed to change over time as users became more proficient with their passwords. Facilities were also established for accounts to be owned by more than one person. The results from these test systems were that valid users were able to log-on 89% of the time, while intruders, once they were told an account's password, could log-on only 43% of the time. It should be noted that in a real system the second figure would be smaller as intruders would have no way of knowing whether they they possessed the correct password, until they guessed the correct typing style. These results are further discussed in [Newberry and Seberry 1987].

A type-signature system would be proof against the common password attacks. For example, attempts to exhaustively test every possible password, either manually or by machine, would be unlikely to succeed, as intruders would be unable to determine whether or not they had chosen the correct password, and had used the wrong type-signature, or had simply entered the wrong password. Certainly attempts to exhaustively

1. This was funded by a grant from ATERB.

try each password combination by machine would fail, as the manner with which a computer entered a password to another computer, would be very different from the manner with which a human would. Thus most attacks via modems would be unsuccessful.

1.2 A Super-shell

An obvious extension of the type-signature idea, is that of an operating system capable of checking the type-signature of a user for each command that was issued to it. Such an idea is being pursued by Mike Newberry in his honours thesis [Newberry1987].

1.3 Other Effects

Since both applications of type-signatures described above measure the way a person types they can be effective in detecting disorders such as RSI[2]. In the trials of the password system, one user developed RSI, and was unable to log-on, because her typing style had changed. Similiar results are anticipated for any event that altered the way a person typed, such as intoxication. This was anticiapted in [Jones1985].

2. Unix Style

Initial experiments performed by Mike Newberry, suggest that it is possible to use the commands issued by a user as a measure of their identity. For example, a new computer user would use very different commands to a more experienced user. Such a system is being developed using artificial intelligence and expert systems technology, and when completed will be capable of learning what kinds of commands are typical for a given user, and using this information to identify an intruder. Such a system could be used when a staff member was suspicious of the identity of a particular user, early versions being be too cpu intensive to be run in the background continuously.

3. Summary

In any area where it is critical that users be identified correctly, the above measures provide much greater security than just a password system — even if all passwords became public knowledge, an intruder would have less then a 50/50 chance of successful entry.

For more information contact:

Professor Jennifer Seberry
Department of Computer Science
University of New South Wales
Australian Defence Force Academy
Canberra ACT 2600
(062) 688184

---

2. Repetition Strain Injury

References

Jones1985. Terry Jones, *Secrecy and Authentication*, Unpublished honours thesis, University of Sydney (1985).

Newberry1987. Mike Newberry, *User Unique Identification*, Thesis in preparation, University of Sydney (1987).

Newberry and Seberry 1987. Mike Newberry and Jennifer Seberry, *Experience of Using a Type Signature Password System for User Authentication in a Heavily Used Computing Environment*, Unpublished Paper, University of Sydney (1987).