THE USE OF SIMULATION IN COMPUTER-BASED SECURITY SYSTEMS

Steven M. Furnell, Peter W. Sanders and Colin T. Stockel
Network Research Group
University of Plymouth
Plymouth, United Kingdom
E-mail : stevef@soc.plym.ac.uk

Keywords : Computer systems, Statistical analysis, Real-time simulation.

ABSTRACT

The aim of this paper is to examine the applicability of simulation techniques to the testing and evaluation of computer security systems. Attention is specifically focused upon a relatively new area of security, namely advanced user authentication and supervision systems that are able to detect intrusions in real-time, based upon the comparison of user activities to predetermined behaviour profiles. The discussion is supported by the examination of a prototype monitoring system, based upon a simulation of the real-time analysis of user's typing characteristics. The paper also considers a number of inherent problems in simulating the operation of a security system.

INTRODUCTION

Recent advances in the complexity of information systems, networking and telecommunications technologies have dictated an increasing requirement for more advanced security systems to safeguard against accidental and deliberate damage to systems and data.

Traditional approaches to user identity verification (principally passwords) can be considered increasingly inadequate as information system usage becomes an ever more routine part of society. The ability to utilise one system to access a multitude of others via global networks requires that user authentication be dependant upon more than just one (or a small series of) discrete judgement(s). In addition, it is desirable that mechanisms are incorporated that do not overburden the user with security responsibilities. However, even the more secure techniques available, such as the use of smart cards, require significant positive action on the part of users in order to be authenticated and may also be costly to implement on a large scale.

In light of such considerations it is increasingly desirable to redirect the focus of identity verification away from the user to being more of a system responsibility. An area of activity that supports this view is the development of advanced user authentication and supervision systems that aim to detect computer-based intrusions in real-time. These attempt to categorise various behavioural characteristics of legitimate users to form *profiles* of their normal system usage that can then be used as the basis for future identity verification and supervision (Lunt 1990; Bauer and Koblentz 1988).

However, such intrusion detection systems are, by definition, more complex than traditional means of authentication and access control and, as a result, the issue of effectively testing them may be considered problematic. Testing can no longer be regarded as being simply a question of determining whether a particular security measure can be easily broken or bypassed (Robertson 1992). It is also necessary to get a measure of *effectiveness* (i.e. how successfully can genuine intrusions be detected without mistakenly disrupting legitimate activity). In addition, testing cannot be effectively conducted by an individual or even a small team. The very nature of the concept requires that many genuine examples of user activity must be used as the basis for testing which, in turn, dictates that a reasonably large and diverse group of test subjects must be involved. However, it would be impractical (and probably undesirable) to introduce such a system into a "live" environment until it is known to work effectively, otherwise its presence could disrupt legitimate work (e.g. by causing the false rejection of valid users). There is also the consideration that the use (or simulation) of intrusion scenarios in an operational environment would

be a questionable proposition, as it could adversely affect system operation and potentially damage data.

SIMULATION IN SECURITY SYSTEM TESTING & EVALUATION

The considerations identified above highlight a significant requirement for off-line testing and evaluation of security systems, but in a context that will still provide a realistic measure of effectiveness.

An approach to the problem is to carry out the testing of such new security systems in a simulation environment, but using behavioural information taken from actual user sessions. In this way, data relating to user actions could be "recorded" from genuine sessions and then subsequently replayed, off-line, into the security system for analysis. This is illustrated in figure 1 below.

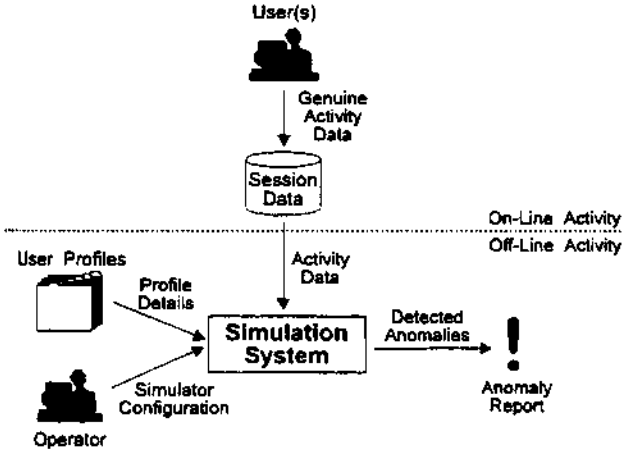

Fig. 1 : Simulation in security system testing

This approach has the advantage that testing can then occur away from any live operations, whilst still retaining the characteristics of genuine usage. In addition, the stored session data may be used to represent both legitimate users (when compared against the behaviour profile of their originator) and impostors (when compared against anyone else's profile). This latter point assumes that the profiled characteristics of any two users should not normally be similar enough to result in their behaviours being indistinguishable. However, whilst using genuine activities to represent impostors in this way would be sufficient to test the system from an identity verification viewpoint, it is unlikely that any examples of attempts to compromise system security would be observed. Therefore, in order to provide a comprehensive test of supervision, it is also desirable to introduce examples of deliberate intrusion attempts. A method by which these could be obtained would be to record the activities of professional "Tiger Teams" as they attempt to test security (Goldis 1989).

AN EXPERIMENTAL STUDY

This section describes the research teams implementation of a prototype intrusion monitoring application based on the concept of real-time keystroke analysis, highlighting areas in which simulation aspects were utilised (it should be noted that as the experimental study focuses upon a more specific aspect of intrusion monitoring than is discussed elsewhere in the paper, some of the points raised in other sections do not strictly apply to this system).

Keystroke analysis provides a behavioural biometric measurement based upon distinctive characteristics of the users typing styles. When used in the context of an intrusion monitoring application, the technique may be used to provide a continuous and transparent means of verifying user identities in conjunction with their normal system activity.

An experimental system, comprising three modules as listed below, was developed for the PC environment to allow an evaluation of the concept in practice :

- *Profiler*
  Accepts reference typing samples in order to create profiles for legitimate users.

- *Sampler*
  Accepts additional user typing samples and stores all keystrokes and associated timings for later use.

- *Monitor*
  Compares the typing samples against profiles to determine the effectiveness of the system, simulating the real-time entry of the sampled keystrokes.

These elements fit broadly into the structure that was presented in figure 1, with sample entry equating to the on-line activity and the monitor module representing the off-line security system simulation.

Tests were conducted involving 26 typists, with typing profiles being created based upon the average inter-keystroke times exhibited when entering specific character pairs (digraphs), with mean and standard deviation values being maintained for each pair. Subsequent supervision attempted to verify user identity by comparing incoming keystrokes against the relevant profiled values, with incompatible times being judged as invalid. If either the overall percentage or number of consecutive invalid keystrokes exceeded certain user-specific thresholds an impostor alert was raised.

The aim of the investigation was to establish the impostor false acceptance rate (FAR) with a false rejection rate (FRR) for valid users of 0%.

Uses of simulation elements

Simulation aspects were incorporated into the study in a number of ways :

- the use of stored user typing samples (including inter-keystroke timing data) to simulate the entry and analysis of keystrokes in real-time;

- the simulation of intrusion scenarios by using "non profile owner" typing samples as impostor inputs to the system. This allowed approximately 1300 impostor test cases to be derived from just 26 test subjects;

A further potential use of simulation that was identified (although not extensively explored) was the ability to generate simulated impostor typing samples based upon data from the initial user profiles. This process would work as follows. After selecting some text as the basis for the test sample, the character digraphs within it could be extracted and matched against the associated mean and standard deviation values held in the profile chosen to represent the "impostor". Using the upper and lower limits of the standard deviation from the mean to define a valid range, a random value could then be generated to represent the impostor's inter-keystroke time for that digraph. For example, if the text contained the digraph "TH" and this had been profiled with mean of 121ms and standard deviation of 47ms, a valid range would be defined as below :

74ms <---------- TH ----------> 168ms

So a typical inter-keystroke time generated by this impostor might be 106ms. This process would continue throughout the entire text to create an appropriate test sample simulation.

To make the sample even more realistic, the simulation could also take into account the maximum percentage of invalid keystrokes that the "impostor" would generate against his / her own profile (given that profiles also maintain this value, for use as an authentication threshold). To this end, a further random element could be introduced by generating an appropriate proportion of keystroke times in the test sample *incompatible* with the host profile.

Once generated, these simulated test samples could be used as a realistic means of testing the false acceptance rates against other user profiles (thus allowing a much more comprehensive test of the systems impostor detection effectiveness without requiring any further test subject involvement). It should be noted, of course, that these artificial samples would only be useful as "impostor" attempts. They could not be used to test legitimate user performance as the creation process would always ensure that they were compatible with the host profile.

The desirability of using such artificially created samples has previously been identified by other research in this area (Brown and Rogers 1993), but in the more limited context of user name entry. The technique was not used to contribute to the results from our study that are described below, but would have been particularly useful had insufficient genuine test subjects been available to participate.

Results and discussion

The results obtained provided a number of useful indications regarding the effectiveness of keystroke analysis as an intrusion detection technique. From the 1300 impostor cases that were used, a FAR of 15% was observed (which can be regarded as a "worst case" figure given that no false rejections occurred). Although this value is somewhat high, it should be remembered that keystroke analysis could be implemented as just one aspect of a more comprehensive intrusion monitoring system and, therefore, other factors could also be introduced that would compensate for the currently undetected cases. Of the detected cases, 49% were due to the percentage of invalid keystrokes observed, whilst the other 51% were due to consecutive invalid keystrokes entered by the impostors.

Given that impostor detection was achieved in the majority of cases, the other important consideration was how quickly it occurred (i.e. how many keystrokes would the impostor have been able to enter before detection). This issue was also addressed by the study, and the results observed are shown in figure 2. This indicates the proportion of detections that occurred within each of five distinct keystroke ranges (based around 40 character blocks - equivalent to half a standard line of text).

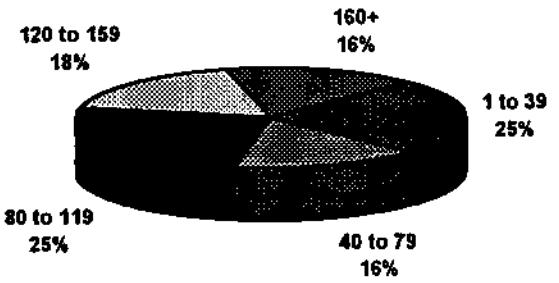

Fig. 2 : Keystrokes before impostor detection

It can be seen from this that the vast majority of impostors would be detected within 160 keystrokes. This result was also considered reasonably encouraging, although it is acknowledged that if intruders were of a particularly malicious nature, then they would possibly require somewhat less than 160 keystrokes in order to cause significant damage.

The experimental study itself would have been considerably more difficult to conduct had the simulation element not been involved. With the test samples being obtained and stored, the study only required that subjects were available for a maximum of around an hour (much less with the faster typists). If the testing had had to be conducted in real-time, on an individual basis, it would have entailed repeated test sample entry and increased the subject availability requirements to such an extent as to make a large test group impractical. In addition, the prototype authentication system would need to have been installed on individual user systems - potentially disrupting their normal activities.

A further point is that the simulation-based environment provided the ability to re-mount the experiment after re-configuration of various aspects of the system (e.g. user authentication thresholds, the number of recent keystrokes monitored, valid inter-keystroke ranges). This facility was used to allow the optimum monitoring configuration to be established.

Finally, the establishment of a "worst case" FAR rating would not have been possible outside of a simulation environment. The ability to specifically configure the system allowed an FRR of 0% to be ensured, with successful impostor performance then being observed at this level. Conversely, the simulation could have been used to determine the level of false rejections with a guaranteed FAR of 0% (however, this approach was not pursued as rejection of legitimate users would be extremely undesirable in the context of a continuous monitoring system).

A more detailed description of this study, the methods involved and the results obtained can be found in (Furnell 1995).

POTENTIAL PROBLEMS OF SECURITY SYSTEM SIMULATION

Even with simulated environments and intrusions there are still a number of considerations that complicate the issue of security testing. A principal point here is that many successful intrusions / system security breaches result from scenarios that were either unanticipated or overlooked by system designers. This is evidenced by the details of known abuse cases (Audit Commission 1990) and also by the fact that, despite the many controls that are present in existing systems, around half of the detected cases of computer abuse are only discovered by chance (Audit Commission 1994).

In addition, there may be difficulties associated with simulating the security environments. Keystroke analysis is quite a trivial example in this respect, whereas most other potential candidates for behaviour profiling (e.g. usage of operating system commands and applications) would require more complex simulation environments and would also demand that profiles were developed over a longer period than in the study described.

Finally, there are a number of important aspects that the approach (as discussed) cannot address. These include issues such as the systems compatibility with other applications, processing overheads that may be incurred in a live environment and acceptability to end-users. As a result, there is still a need for system evaluation in the context of a live "pilot" study, but with the major question of effectiveness having largely been answered.

CONCLUSIONS

The provision of effective security still remains a key issue in the implementation of information systems. Whilst information technology has already affected most aspects of society (e.g. government, healthcare, policing and commerce), this has largely occurred in the context of "closed" systems. As formerly independent domains merge and share common global networks, the requirement for adequate security will increase still further.

It is hoped that this paper has served to highlight how simulation techniques may have a useful role to play in the security field, targeting an approach to protection that is considered appropriate to the perceived needs of future systems.

Our own study served to demonstrate various areas in which simulation could be involved in a practical context and proved how it could vastly improve the ease of testing in this type of system (with the results of the evaluation indicating the significant potential of keystroke analysis as an intrusion monitoring / user supervision technique).

As information systems advance, it is envisaged that intrusion monitoring systems at this level and beyond will become increasingly more attractive. As such, the use of simulation approaches similar to that discussed will be ever more appropriate.

REFERENCES

Audit Commission. 1990. *Survey of Computer Fraud & Abuse : Supplement*. The Audit Commission for Local Authorities and the National Health Service in England and Wales.

Audit Commission. 1994. *Opportunity Makes a Thief - An Analysis of Computer Abuse*. HMSO, HMSO Publications Centre, London, UK.

Bauer, D.S. and M.E.Koblentz. 1988. "NIDX - A real-time intrusion detection expert system", In *Proceedings of Summer USENIX '88* (San Francisco, USA, June 20-24), 261-273.

Brown, M. and S.J.Rogers. 1993. "User identification via keystroke characteristics of typed names using neural networks", *International Journal of Man-Machine Studies* 39: 999-1014.

Goldis, P.D. 1989. "Questions and answers about Tiger Teams (organizational security measures)", *EDPACS* 17, no.4: 1-10.

Furnell, S.M. 1995. "Data Security in European Healthcare Information Systems", PhD Thesis. School of Electronic, Communication and Electrical Engineering, University of Plymouth, UK.

Lunt, T.F. 1990. "IDES: An Intelligent System for Detecting Intruders", In *Proceedings of the Symposium: Computer Security, Threat and Countermeasures* (Rome, Italy, Nov.).

Robertson, B. 1992. "The testing of secure systems", In *Proceedings of SECURICOM 92 - 10th Worldwide Congress on Computer & Communications, Security & Protection* (Paris, France, March 18-20), 131-146.

BIOGRAPHY

Steven Furnell graduated from the School of Computing, University of Plymouth with a first class honours degree in *Computing & Informatics* in July 1992. Since August of that year he has been a post-graduate research student in the University's Network Research Group undertaking a PhD programme. The project is entitled "*Data Security in European Healthcare Information Systems*" and, in addition to addressing intrusion monitoring issues, has also involved the development of security guidelines for European healthcare establishments. The research is being supervised by Peter Sanders and Colin Stockel.