Advanced Authentication and Intrusion Detection Technologies

Paul Dowland, Dr Steven Furnell, George Magklaras, Maria Papadaki, Prof Paul Reynolds, Philip Rodwell, Harjit Singh
Network Research Group, Department of Communication and Electronic Engineering, University of Plymouth, UK

Abstract

Security is a vital consideration in the age of modern networks and Internet-based communications, and represents an essential underpinning of emerging applications such as electronic commerce. Within this domain, the ability to ensure the authorised and correct use of systems is an area of significant challenge. The research to be presented is centred around the Intrusion Monitoring System, a conceptual architecture for real-time user authentication and supervision, which has been defined by an earlier project within the Network Research Group. The current research encompasses advanced authentication technologies, based upon biometric techniques and user behaviour profiling. These approaches improve considerably upon the traditional user name and password combination, which has been proven to be weak and susceptible to compromise. While enhanced authentication will combat external impostors and internal masqueraders, further research addresses methods of identifying system misuse originating from authorised users, whom independent surveys have established account for around 80% of computer abuse incidents. Another important consideration relates to methods of responding to suspected intrusions in a manner that will trap genuine impostors and misfeasors, without unduly disrupting legitimate user activity in cases where a false classification has occurred. The research considers the application of these authentication and intrusion detection approaches within both traditional desktop environments and third generation mobile networks.

The Intrusion Monitoring System architecture

The Intrusion Monitoring System (IMS) is the focus of security research in the Network Research Group. IMS is an architecture for intrusion monitoring and activity supervision, based around the concept of a centralised host handling the monitoring of a number of networked client systems. Intrusion detection is the system is based upon the comparison of current user activity against both historical profiles of 'normal' behaviour for legitimate users and intrusion specifications of recognised attack patterns. The architecture is comprised of a number of functional modules, addressing data collection and response on the client side and data analysis and recording at the host (as illustrated in the figure below).

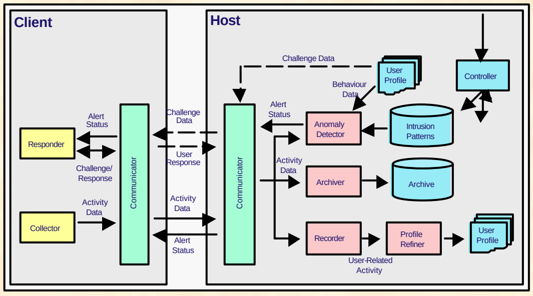

Figure 1: Intrusion Monitoring System architecture

Related Research Projects

The current IMS related research projects are listed below, a number of these involve collaboration and/or sponsorship from Orange Personal Communications Services.

1. User authentication and supervision in networked systems

This project concerns the investigation and evaluation of composite authentication techniques. The study recognises that a variety of authentication techniques are available which, when used in isolation, have known error rates in terms of false rejection and false acceptance. The research is focused upon the specification, implementation and evaluation of a composite authentication approach, in which a range of technologies are available and can be applied intelligently by the system as appropriate to the active user and their current task.

2. Behavioural profiling and intrusion detection systems using data mining

This project seeks to develop profiles of user behaviour by applying intelligent analysis techniques to system data collected in real-time during Windows NT sessions. The profile would represent a model of the legitimate users normal behaviour and could subsequently be utilised in a real-time supervision context to ensure that the activities of the user match those expected of the claimed identity. As such, the technique offers the potential to identify impostors and misusers within the system. This project contributes to the profiling aspect of the IMS architecture.

3. Generic approaches for intrusion specification and misuse detection

This project seeks to design and develop a generic intrusion specification language, which may then be used to specify intrusion characteristics in detection systems such as IMS. This work leads in to specific consideration of how to detect misfeasor attacks – that is, misuse of the system by a legitimate user. In terms of the IMS architecture, this project will contribute to the mechanisms utilised by the Anomaly Detector module.

4. Classifying and responding to network intrusions

This project seek to determine a comprehensive taxonomy of system-detectable intrusions and misuse, leading to the consideration of how the IMS system should respond to them. The work will involve design and practical evaluation of alternative response strategies, assessing factors such as the effectiveness against the nominated class(es) of intrusion and any negative effects that the response could have upon a legitimate user in a false rejection scenario.

5. Non-intrusive security for third generation mobile systems

This project highlights the need for improved methods of user authentication in future mobile systems such as the Universal Mobile Telecommunications System (UMTS). The work is focused upon an investigation of user-to-terminal and user-to-network forms of authentication for use in future mobile networks and devices.

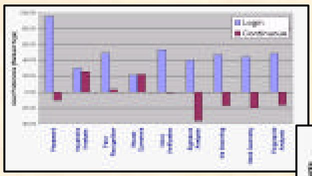

Figure 2: User Preference of Authentication and Supervision Methods (175 respondents)

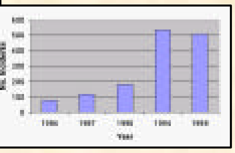

Figure 3: Reported Computer Crime Incidents (*source: Audit Commission*)

Authentication & Intrusion Detection Approaches

IDS techniques are based on the assumption that an intruder's behaviour will be different from that of a legitimate user. In order to detect this deviation from normal user behaviour, IDSs collect audit data such as system resource usage. Providing this continuous monitoring involves processing and analysing vast amount of audit data. Hence relying on human expertise is time consuming, knowledge intensive and infeasible past a certain volume of data. Therefore intelligent data analysis techniques are required to automate some of this process. The research is investigating techniques to automate some of the data analysis using Data Mining (DM) techniques and methodologies (figure 4 illustrates initial results).

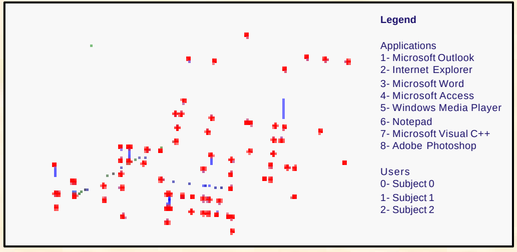

Figure 4: Graphical representation of applications run by users(IMS - Behavioural Profiling)

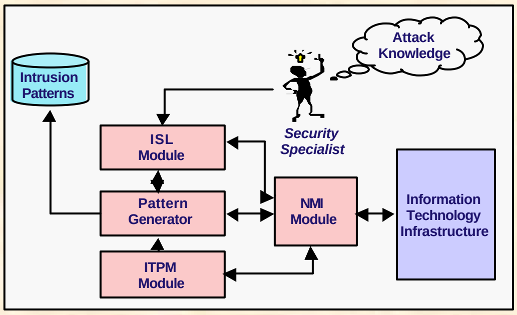

Figure 5: Functional Modules of an Intrusion Specification Language

ISL module The Intrusion Specification Language module, responsible for describing intrusions in a standardized, system independent manner. Used by the security specialist/architect.

Pattern generator module It converts the ISL descriptions into system-specific patterns. It also performs optimised pattern matching functions that are essential for real-time intrusion detection.

ITPM module The Insider Threat Prediction Model tries to sense the level of sophistication of a legitimate user. It can then estimate the probability that a particular user will misuse the infrastructure. This is an experimental/new approach of tackling the insider IT misuse problem.

NMI module The Network Management Integration module is responsible for utilising network management protocols in order to collect information and co-ordinate selected IDS responses from a variety of IT infrastructure components.

Information Technology Infrastructure The set of computer hardware, software and telecommunication components that perform a useful function inside an organisation.

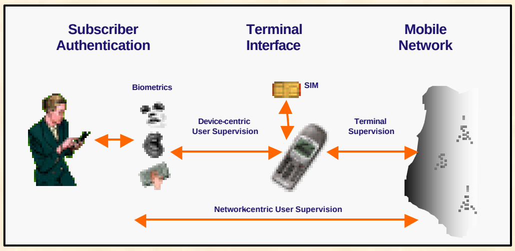
Subscriber Authentication
Terminal Interface
Mobile Network
Biometrics
SIM
Device-centric User Supervision
Terminal Supervision
Network-centric User Supervision

Figure 6: Supervision in a Mobile Environment

Summary

The techniques under investigation represent a considerable departure from traditional methods of authentication and access control, and aim to provide an added level of protection for IT systems. Modern society is increasingly dependent upon IT infrastructures. At the same time, surveys from bodies such as the Audit Commission and the FBI are reporting increased levels of computer crime and abuse (originating from both outside the organisation and from within). In view of these factors, the additional safeguards provided by advanced security techniques will become ever more necessary. As the research has identified, the techniques are relevant to both traditional networked PC environments, as well as other scenarios such as third generation mobile systems.

Dowland, P.S, Furnell, S.M, Illingworth, H.M. and Reynolds, P.L. 1999. "Computer Crime and Abuse: A Survey of Public Attitudes and Awareness", *Computers & Security*, vol. 18, no. 8, pp715-726.

Dowland, P. and Furnell, S 2000. "Enhancing Operating System Authentication Techniques", *Proceedings of the Second International Network Conference (INC 2000)*, Plymouth, UK, 3-6 July 2000, pp253-261.

Furnell, S.M, Illingworth, H.M, Katsikas, S.K, Reynolds, P.L. and P.W.Sanders. 1997. "A comprehensive authentication and supervision architecture for networked multimedia systems", *Proceedings of IFIP CMS'97*, Athens, Greece, 22-23 September 1997, pp227-238.

Furnell, S.M. and Dowland, P.S. 2000. "A conceptual architecture for real-time intrusion monitoring", *Information Management & Computer Security*, vol. 8, no. 2, pp65-74.

Furnell, S.M, Dowland, P.S, Illingworth, H.M. and P.L.Reynolds. 2000. "Authentication and supervision: A survey of user attitudes", *Computers & Security*, vol. 19, no. 6, pp529-539.

Papadaki, M. 2000. *A Taxonomy of I.T. System Intrusions.* M.Sc. Thesis, University of Plymouth, Plymouth, UK.

Rodwell, P.M, Furnell, S.M. and Reynolds, P.L. 2000. "Non-intrusive security requirements for third generation mobile systems", *Proceedings of PG Net 2000– 1st Annual Postgraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*, Liverpool, UK, 19-20 June 2000, pp7-12.

http://ted.see.plym.ac.uk/nrg