RAID 98: First International Workshop on the Recent Advances in Intrusion Detection

Workshop report

Workshop held in Louvain-la-Neuve, Belgium on 14-16 September 1998

Marc Wilikens
Joint Research Centre
Institute for Systems Informatics and Safety
21020 Ispra (VA) – Italy
Tel: +39 332 789737, Fax: +39 332 789576
Marc.Wilikens@jrc.it

28/9/98

TABLE OF CONTENTS

1 Introduction

1.1 Background

Because of the increasing dependence that businesses and government agencies have on their computer networks, protecting these systems from intrusions is critical. A single intrusion of a computer network can result in the loss or unauthorised use of large amounts of information and can cause users to question the reliability of all the information on the network.

RAID'98 is the first in an anticipated annual series of international workshops that, quoted from the workshop announcement, aims to “bring together leading figures from academia, government, and industry to ponder the current state of intrusion detection technologies and paradigms from the research and commercial perspectives”.

RAID’98 was organised by IBM Research Labs of Zurich and was hosted by the University of Louvain-la-Neuve (UCL). It was held back-to-back with ESORICS ‘98, the 5th European Symposium on Research in Computer Security.

RAID’98 consisted of 8 paper sessions and two panel sessions. I presented a paper entitled “Dependability of large-scale infrastructures and challenges for intrusion detection” in session 3 chaired by Yves Deswarte from Laas. The paper was derived from the results of one of the industrial workshops organised in the frame of the European Dependability Initiative (DI) but with special emphasis on intrusion detection issues. It was also an occasion to promote the DI in this community prevalently from the security domain.

In addition, I participated to a panel on the last day on “Intrusion detection in the large” and a panel on the first day of ESORICS on “New challenges for research in Information System security”.

The following paper outlines the state-of-the-art research and challenges in intrusion detection based on the presentations and discussions held.

1.2 Definitions

An *intrusion* can be broadly defined as “any set of actions that attempt to compromise computing resources or the information handled by them”. They are deliberate in nature and include actions of individuals who are using a computer system without authorisation (e.g. cracker from outside the physical or logical perimeter of an organisation) or those who have legitimate access to the system but are abusing their privileges. Very often, the notion of *attack* is used or simply as a synonym for intrusion attempt or to differentiate between successful and unsuccessful attempts, a successful attack to be understood then as one leading to an intrusion.

Typically, intrusions take advantage of *system vulnerabilities* attributed to mis-configured systems, poorly engineered software, mismanaged systems, user neglect or to basic design flaws in for instance some internet protocols.

An *intrusion detection system (IDS)* is a tool that attempts to perform intrusion detection. IDS is a fast moving market with new players entering continuously.

Commercial tools range from the widely available anti-viruses, to enterprise tools (e.g. CISCO/Netranger), to NT centric (e.g. Internet Security Services/RealSecure) and to configurable freeware (e.g. Network Flight Recorder). In fact such tools only detect suspicious events and report the intrusion and/or attempt to the operator. They do not (yet) include decision making support for preventive or recovery actions once an intrusion has been detected.

1.3 General comments

130 participants attended RAID ’98, which is a success considering that it was the first of the series. Of the attendees, 40% were from the USA with a majority from large National Labs (Lawrence Berkeley, NIST, San Diego Super Computer Centre, etc), University Labs (Carnegie-Mellon, Purdue, MIT, Idaho, Univ. of New Mexico, etc) and IBM. European affiliations were evenly spread between Academia/Industry including amongst others Nokia, Sonera, LSE, Deutsche Telecom. As far as the presentations were concerned, there was a clear US dominance with 60% of the papers. This clearly reflects the technological advance of the US in this area which can be explained by the Defence interest and related funding. Noteworthy is also the relative share of East Asian papers (15%) from Hong Kong and Singapore on concrete implementations of IDS technology.

1.4 The changing security context

For better understanding its potential, the ID approach should be put in the context of a changing approach to security management in general. In a world keen to exploit open- ended communication infrastructures, to use evolutionary systems and to embrace mobility, striving for absolute security at any cost based on static design measures and the erection of security barriers similar to physical fences (e.g. firewalls) has become inappropriate. Instead, businesses strive for risk-based trade-offs between security and usability and for dynamic security adaptation to better respond to changes in threats, configuration and usage patterns of systems. In this context, IDS’s as operational responsive tools and combined with the necessary adaptive facilities will become more relevant in the future.

2 State-of-the-art and future challenges

Research into and development of automated Intrusion Detection Systems (IDS) has been under way for nearly 10 years. By now a number of systems have been deployed in the commercial or government arenas, but all are limited in what they do. The creativity of attackers and the ever-changing nature of the overall threat to targeted systems have contributed to the difficulty in effectively identifying intrusions. While the complexities of host computers are already making intrusion detection a difficult task, the increasing prevalence of distributed networked-based systems and insecure networks such as the Internet has greatly increased the need for intrusion detection.

The outcomes of the discussions were consolidated and organised in few issues that seemed best suited to reflect the challenges raised during the various presentations and discussions. These issues are i) Technology integration; ii) large-scale infrastructures and iii) global nature of the problem.

All organisations mentioned in the following chapters, refer to presentations made during the workshop.

2.1 Integration of technologies and paradigms

Related to the technological approach of Intrusion Detection Systems (IDS’s), three categories are identified:

2.1.1 Modelling: Misuse or anomaly detection

In the *misuse detection* model, detection is performed by looking for specific patterns or sequences of events representing previous intrusions (i.e. looking for the “signature” of the intrusion). It is a knowledge-based technique and only known intrusions can be detected. This is the more traditional ID technique which is usually applied in for instance the anti-virus tools.

In the *anomaly detection* model, detection is performed by detecting changes in the patterns of utilisation or behaviour of the system. It is performed by building a model that contains metrics derived from normal system operation and flagging as intrusive any observed metrics that have a significant statistical deviation from the model. The approach is behaviour-based and as such should be able detect previously unknown intrusions. It is an R&D area in which currently innovative modelling paradigms are explored which are inspired from biological systems. Pioneers in this area are the University of New Mexico with seminal work based on the way natural immune systems distinguish between “self” from “non-self”. The main challenge with this approach, like for every behaviour-based technique, is to model the “normal” behaviour of a process. This can be done by learning the activity of the process in a real environment. Another approach, advocated by IBM research, consists in describing the sequences of audit events (patterns) generated by typical UNIX processes. Another method developed by Nokia is based on Kohonen Self Organising Maps (SOM) and was also presented at the workshop.

2.1.2 Analysis: Off-line vs. real-time

Another, more conventional classification divides IDS’s into systems which operate after the event and rely on analysis of logs and audit trails for preventive action and those that attempt real-time monitoring in the hope that precursor signs of abnormal activity give indication that corrective action is possible before real damage occurs.

2.1.3 Deployment: host or network

Intrusion monitoring can either be sited at the computer system which is the putative target or placed on a network level where traffic can be evaluated or where information aggregated from various hosts can give insight in co-ordinated attack scenarios.

2.1.4 Challenges

- Most of the individual techniques are more suitable for local event monitoring and analysis. Globally co-ordinated attack strategies require integration of methods and aggregation of disparate information sources. The critical issue lies in defining the high-level communication protocol to allow different methods of IDS to contribute to the intrusion detection process.

- IDS methods must be better integrated with exiting network management systems if their widespread adoption in Industry is to be guaranteed. One reason is that this should facilitate their maintenance/upgrades and a more coherent audit/log data management.
- IDS is one mechanism to respond to new business dependability/survivability needs. It is as yet unclear how to integrate IDS with other dependability mechanisms (e.g. fault tolerance, recovery mechanisms) in a wider information risk and security policy context.

2.2 Large-scale infrastructures

Intrusion detection for emerging large-scale distributed systems (e.g. global companies and virtual enterprise networks) faces a variety of difficult challenges. The most important ones can be summarised as:

- Variety of attack scenarios: The anatomy of an intrusion is composed of increasingly complex attack scenarios. An attack scenario consists in a logical sequence of actions that are applied for reaching a particular strategic goal (e.g. getting confidential information). These actions are typically applied on different hosts in a network and by using a variety of tools. Moreover, a variety of different attack scenarios are possible to reach the same goal. There is a need for dynamically linking local individual events to global attack strategies in order to provide pro-active and adaptive intrusion monitoring. In his presentation, Huang from the Boeing Company proposed an augmented goal tree method for modelling intrusion intentions. Intrusion intentions are understood as high-level platform independent attack strategies that manifest in large permutations of low level system/network events.
- Volume, volatility and noisiness of data generated by ID systems: IDS techniques so far concentrate on local event monitoring. Important new issues in the large-scale network context are information exchange, work division and co-ordination amongst various IDS's. An emerging architectural approach is based on autonomous local IDS agents performing event processing coupled with co-operative global problem resolution. However, the degree of autonomy of agents is subject to debate and research. Purdue University has been working on their AAFID, the Autonomous Agents for Intrusion Detection. However at the present stage, the system does not yet exploit the real mobility and autonomy aspects of agents.
- Performance in complex infrastructures: Large distributed networks of systems need scalable IDS approaches for which performance is becoming an important attribute. This includes issues of timeliness of local event monitoring and communication of contextual data between nodes as well as of trust relationships between the nodes.

2.3 Global nature

How intrusions can exploit global communications infrastructures has been illustrated by the USAF Rome Labs experience. Relevant issues of global nature that were discussed at the workshop include:

- Incident data and reporting: CERT operated by SEI/CMU is a well known and public incident reporting system. They were not represented at RAID ’98. Various commercial initiatives in incident handling are also being set up as a service to businesses. IBM presented the Real-Time Intrusion Detection System set up in the frame of their ERS (Emergency Response Service). IDLE (Intrusion Data Library Enterprise) is a joint SRI/Chalmers effort for database format based on the XML language. Forums and mechanisms are necessary for sharing data and experiences. These should allow a better quantification of the intrusion risks.
- Standards for characterising intrusions: There is still confusion about terminology in the areas of attacks, intrusions and vulnerabilities. This hinders data sharing. Moreover, there is a need for better characterising these issues in order to support IDS requirements, implementation and evaluation processes and to support evidence collection for law enforcement investigations and legal proceedings. Related to the latter, the London School of Economics (LSE) has made interesting work. Also standardisation bodies are working on intrusion detection frameworks. Initiatives from IETF, ISO-SC27 (IT Security) were reported on the workshop. DARPA’s CIDF (Common Intrusion Detection Framework) was mentioned in informal discussions.