

Panel: Intrusion Detection in the Large

RAID'98 Workshop

September 16, 1998.

Panel objectives

The main objective of the panel was to discuss the problems and possible solutions related to doing intrusion detection in large systems. It ended up, however, being a much more general and wide-ranging discussion about many issues that, although particularly important in large installations, are relevant for Intrusion Detection systems deployed in installations of any size and type.

Panel participants

- **Deborah Frincke** (University of Idaho, USA) — Moderator.
- **Karl Levitt** (UC Davis, USA).
- **Michel Miqueu** (CNES, France).
- **Jean-Jacques Quisquater** (UCL, Belgium).
- **Marc Wilikens** (Institute for Systems, Informatics and Safety, Italy).
- **Kevin Ziese** (Cisco/Wheelgroup, USA).

Issues presented and discussed

The format of the presentations by the panelists was very informal. In fact, few of them had a formal presentation.

Quisquater started the panel by stating that to be able to tackle the problem of doing Intrusion Detection in the Large, where many of the components are mobile, we need reference points that are both mobile and secure. He asked whether it would be useful, for example, to use smart cards for Intrusion Detection. Smart cards could

be used to store traces and other useful information. In fact, smart cards could possibly interact with their environment to get other useful information. This creates new problems, because now we need to do also Intrusion Detection in very small systems. As he called it, we need to do “Intrusion Detection in the large in the small.” This issue was not touched again in the course of the panel.

Miqueu talked from the perspective of the “real world” as a representative of CNES, the French Space Agency, where they use Intrusion Detection systems in their production systems. Early-on, their work requirements brought the need for security policies and plans, and Intrusion Detection was one of the needs they determined. He mentioned the problem of evaluating Intrusion Detection systems in the real world, and a common problem seems to be that it is difficult to find people with the necessary expertise to do those evaluations. He thinks that some important needs for an Intrusion Detection system are the ability to provide a timely reaction, to provide evidence, and to identify suspicious activity before a more serious attack occurs. He thinks that real-world experiences is difficult to obtain, and that this will be one of the major problems to remain to be solved. Other problems he sees for the future are the need to reduce the overhead imposed by Intrusion Detection systems, and the need to integrate them with other products, such as network management systems and other system administration tools. Network and system administrators are already too overloaded with work, so we cannot expect them to learn yet another language, another system, to be able to do intrusion detection.

Wilikens tried to identify the main issues related to Intrusion Detection that were mentioned in the workshop, but in the context of large scale systems. He identified three main issues:

- Large scale infrastructures. Apart from the traditional problems associated with large scale and distributed systems, there is the problem of the constant evolution of attack patterns. Thus, systems are needed that are not only scalable and easy to use, but also evolutionary so as to be able to adapt to new attacks.
- Integration. There is a need to integrate multiple Intrusion Detection techniques and architectures (such as anomaly detection, misuse detection, host-based and network-based systems) in order to provide real business solutions. He also repeated the importance of having the Intrusion Detection systems integrated with other tools that are already used in the networks. Thus, interoperability is a big concern.
- Global nature of the problem. It is very important to have standards for characterization, storage and exchange of data about attacks intrusions, vulnerability and evidence.

At this point the panel was opened to questions from the audience. The first questions focused on the problem of integrating Intrusion Detection systems as part of network management. One of the main issues was the problem of how to control the guard, this is, the system administrators, who may become “your worse enemy” because they know how the internal mechanisms work, they know what intrusion signatures are being looked for, etc. The other issue was whether the current Intrusion Detection systems are looking for the right things, this is, the real problems, or only for things that the developers think they can detect. To these points, Kevin Ziese answered that it is important that people start using and believing in these tools in order for them to evolve. There are many technical problems to solve, including usability, data visualization and performance problems.

The issue of the insider threat was reiterated by Marc Dacier (IBM Zurich Laboratory). He stressed that the security community will always be interested in finding a solution that may jointly tackle the internal and external problems. However, there are also the issues of service and integration of Intrusion Detection inside a network.

Fighting the insider threat may prove to be extremely complicated and also directly related to the environment

of the organization. For example, Michael Erlinger (Harvey Mudd College) stated that there is no point of its college to tackle the threat coming from the students. The important factor, continued Erlinger, is that each individual needs to focus and identify its own problems and then choose the appropriate solutions. Following on Erlinger’s train of thought, Ziese affirmed that each organization needs to establish its own risk model. After having done so, it would be possible to customize and integrate Intrusion Detection inside the network. Moreover, he reiterated the importance of having efficient and effective visualization mechanisms for the activity of the networks and possible intrusions.

Another question was about the fact that most Intrusion Detection systems are put “on the border” of the networks. What about Intrusion Detection inside the network? Also, is Intrusion Detection a service that companies can provide, or it can only be a product that is packaged and sold? To this, Miqueu responded that Intrusion Detection is needed inside the network because we need protection against the insider threat, but it needs to be integrated with the rest of it to be useful. Ziese mentioned that Intrusion Detection systems were traditionally put “on the border” because they were considered “a bump in the road,” and not an integrated product. To avoid this problem, Intrusion Detection needs to be able to integrate with other products and mechanisms, and for this, interoperability is crucial. Efforts such as the CIDF (Common Intrusion Detection Framework) project represent steps in the right direction.

Ziese followed his idea of the need for interoperability by answering another question: within an enterprise, there are products from multiple vendors, there are different applications and many networks, and attacks can be performed on any level. This problem can be solved, remarked Ziese, by using different products for detecting and protecting different things, but they need to be able to communicate or exchange data to be able to provide a really useful solution.

The panel identified another dilemma for the Intrusion Detection research community: striking the right balance between customization and automatic update (vendor setting) of Intrusion signatures. The fact is that system administrators do not have the time to create their own signatures. However, as every environment presents its own specific problems and characteristics, it is important that

Intrusion Detection systems provide the ability to customize signatures. Nevertheless, it will always be the vendors' effort to provide constant updates to signatures to its clients. Basically, Intrusion Detection systems need efficient service and maintenance.

Another member of the audience raised a question about the efficiency of Intrusion Detection systems. They may generate too many alarms. In fact, it seems that Tripwire continues to be one of the most used tools for doing Intrusion Detection. Karl Levitt remarked that Tripwire is a host-based tool that cannot see what happens in the network. As such, both him and Ziese concluded, it is only one more hammer in the toolbox. It needs to be orchestrated with other tools. And again, interoperability makes it much easier for this to happen.

The session ended with a small debate on the importance of data. Levitt stressed the importance of having data in order to develop and test Intrusion Detection techniques and systems. However, the research community has great difficulty in collecting data concerning internal problems, and in fact we do not know what data is needed. Being the internal threat extremely important, Levitt has invited the community to try to find a solution to the availability of data. Marc Dacier confirmed that there is cooperation between some research efforts in different organizations, but none in the field of data exchange. This is a common problem, because organizations do not like to release information about their security problems.

Panel summary

One issue that was repeated many times was the need for interoperability of Intrusion Detection systems and security tools in general. Efforts such as the CIDF project help in that respect, but much more work is needed. Since it is impossible to build a single tool that detects and protects against every possible problem, it will not be until all our different tools can communicate that really integrated solutions will be possible.

Another important issue was the questioning of the efficacy of the existing Intrusion Detection systems. Are they looking for the right things? Can they really be useful in detecting real problems without overloading the operator with useless data (particularly in large systems)? To this, part of the solution seems to be working on the usability

issues of the systems, as well as on the data visualization problems.

Very related to the previous issue, and also a big source of discussion, was the question of who has to provide the signatures for intrusions: the vendor or the users? It seems that the most appropriate solution would be to find a balance between the two extremes. Most of the responsibility lies with the vendor (who has to provide reasonably complete and up-to-date sets of signatures), but the user must also be able to add or modify signatures in order to customize the Intrusion Detection system to his own needs, or to react immediately to new problems that are detected.

One last big issue was the problems with data exchange. Data is needed for research, but nobody wants to share their data. This is a big problem, and organizations, both in research and in industry, need to work together and try to find solutions to this problem. The issue of interoperability shows up here again, because having a common format for the presentation of data would make it much easier for the necessary exchanges to happen.

Scribes for the panel: Thomas Daniels, Patrik D'haeseleer, Donald Tobin, Lorenzo Valeri and Diego Zamboni.