Pascal van Eck

In the wake of major accounting scandals at Enron, Ahold and Parmalat, companies – particularly in the US – must better substantiate all financial and accounting disclosure information. This requires an effective control framework.

For Pascal van Eck, the time is ripe to develop intrusion detection systems that speak the language of policy makers.

Secure technology from a business perspective

'Intrusion detection systems stand guard at the gates, looking out for suspicious traffic. This is no easy task, as major organisations can produce millions of reports each day. We always tend to think that the danger comes from outside, but the problem is not limited to the global attacks that take advantage of commonly known Windows vulnerabilities. Scandals like Enron demonstrate that you also need to look within the organisation. With the Sarbanes-Oxley Act, which is also known as SOX, the US government has dramatically tightened the rules governing financial accounting standards. As a result, the CEO must not only approve and sign off on the correctness of all financial transactions, but the company must also have a highly effective control framework in place. In this regard, the timing of our Integrated Policy-based Intrusion Detection project couldn't be better.'

'Traditional approaches to intrusion detection have so far focused on technical measures, involving the development of a set of rules and traffic monitoring based on network addresses and keywords. Reporting is filled with technical jargon. A growing organisational issue is where to place the individuals working in this field. Should they be placed close to system management? Or would it be better to place them near management and the auditing or internal accounting department? For this reason, we are taking a comprehensive approach. We want all technical decisions to be rooted in policy.

Moreover, the reports generated should be based on aggregate results derived from the information obtained and be easy for management to understand. Ideally, the entire process will be automated, as this will facilitate the integration of intrusion detection into corporate operations and management cycles.'

'This can be compared to the fairly simple system I use at home, which produces no more than 20 reports a day. If, for example, I don't permit online banking transactions involving more than 1,000 euros to be effected without approving them first, I would be very concerned about any reports indicating that such a transaction occurred without my knowledge. I would want to be informed of this as quickly as possible, preferably in real time.

This technical alarm must be programmed in accordance with the "policy" I have established for online banking payments. Making this translation in real time is not easy at all, it it is nonetheless our goal.'

'Overseeing the millions of reports generated might be possible if you could see them individually. To date, no one has seriously attempted to identify the patterns in these reports. This is another "impossibility" we want to investigate. The system sees that someone has submitted a claim, which is not suspicious. Several hours later, the system sees that someone has approved the claim. Again, this is not suspicious. However, it would be suspicious if the same person submits and approves the claim. This brings us back to the need to view it from the organisation's perspective.'

'Mobility complicates matters. One of the organisations we looked at processes information of such a highly sensitive nature that the programmers were not permitted to view the live data. The tests we conducted involved random data sets instead. We have had the means to distinguish between production and test environment for ten years already. In the meantime, WLAN technology has made wireless connections possible, enabling more and more people to work remotely. Is the system still watertight?

Or can users, who log into the domain to which they have access, also gain access to sensitive data simply by remaining logged in and moving to another computer? If you take a purely technical approach to this type of problem, you may not even be aware that it exists. The organisation in question, however, was made aware of its existence after we created a gap in the system to highlight it.

'While many claim that SOX is yet another example of American overkill and that it is not needed in Europe, the law applies to all international companies listed on the American Stock Exchange, even if they have their headquarters outside the States. Moreover, the European Commission has announced that it is developing similar legislation. This makes this research project exceptionally relevant, and that is a big motivation for me. After talking to people in the banking industry, who generally do not focus on technological issues, we are left to translate the information they provide into algorithms and services. As part of the larger ISTRICE security project, we have developed effective collaborative relationships with other groups. Some are more technically oriented, while others focus more on the organisational aspects of information systems. This has proven quite effective.'

'Mobility complicates matters. One of the organisations we looked at processes information of such a highly sensitive nature that the programmers were not permitted to view the live data.'

CTIT progress report 2005-2006