SLAC-PUB-8060
February, 1999

Intrusion Detection and Physics

Robert Cowles, Computer Security Officer

Stanford Linear Accelerator Center
Stanford University
Stanford, California 94309

rdc@slac.stanford.edu

Work supported by Department of Energy contract DE-AC03-76SF00515

Intrusion Detection & Response II Workshop

San Diego, CA

12-13 February 1999

What’s Different?

Research environments, especially in High Energy Physics (HEP) have a tradition of being very open. The very size of the experimental collaborations involving software development, hardware design and implementation from teams all around the world require incredible amounts of open discussion and collaboration with as few barriers as possible.

Physicists consider themselves very capable and expert users of technology, and certainly their success at wringing results from huge, multi-billion dollar particle accelerators lends credence to that belief. These are highly intelligent, creative people who tend to enjoy playing with the latest software releases (beta) and in solving puzzles (how do I get around this restriction?). Once these users have found ways around restrictions or become used to certain software "features", it can be extremely difficult and politically dangerous to (re)impose barriers which might delay large projects.

Physics & Computer Security

The standard reaction to computer security policies is to ignore them and see how much can be done before someone makes an issue of it. This is the "Huh? What policy?" approach and can be used with great success since no once can really expect them to read any information published with a bureaucratic content higher than 0.1%.

Another successful approach is used when the policy is implemented with technical barriers, say TCP/IP port blocking. In this circumstance it is assumed any solution they find allowing them to bypass the restriction must be OK, or you would have prevented it from happening. Here the security policies are treated like any other problem they need to solve in their daily work, and clearly anything that works is fair game.

If all else fails, the security restrictions are pointed to as "the reason" work cannot proceed. If you try to work with the user and find out what problem they are really trying to solve, you find the real problem is "you" and the solution is to take your policies which needless get in the way and peddle them to a bank -- some place else where they would be appreciated.

Computer Security as related to Physics is certainly not mechanics. It is much more like thermodynamics: there is what seems like a lot of random motion, and the governing rules are (1) You can’t win; and (2) You can’t even break even.

Security Activity

Typical security activities at SLAC include dealing with four to five minor incidents per month. Typical incidents involve cleaning "warez" from anonymous ftp incoming areas and dealing with cases where a user's password has been compromised (usually sniffed at another site) and an IRC bot has been installed.

While there is a large variation, the cleanup and reporting activity including contacting the user involved and doing some education can easily add up to between four and sixteen hours per incident.

Incident on 2 June 1998

On June 2, SLAC experienced a major incident. The result was more than 25 machines with root compromises and more than 50 user accounts were used by the intruders. The intruders also had access to more than 40 other sites for further "exploration." In order to assess the damage and clean up the systems, SLAC dropped off the Internet with respect to interactive services for a one week period (incoming web access and bi-directional email was still allowed). It did serve to focus a lot of attention on computer security issues.

Management Priorities

Lab management set forth the following priorities to be used in developing a plan for increased computer security:

- Prevent unauthorized access to business systems and confidential data;
- Protect accelerator control systems; and
- Protect physics data and programs.

Constraints

Of course, that isn't the whole story! We needed to be sure we implemented credible responses to major vulnerabilities: compromised passwords, and the combination of "scientist maintained" workstations and a mode of thinking that PC meant "personal" computer even in an environment with significant resources. We had to balance the need for a secure, reliable computing and network infrastructure with the need for an open, collaborative research environment. The bottom line is that the Physics must get done!

Threat Analysis

In terms of possible threats to the business systems, the major point of vulnerability was considered to be the Oracle database machine. The attacks we were primarily protecting against were external network-based attacks or attacks involving unauthorized but authenticated users (compromised password, etc.). An additional goal was that the architecture be adaptable enough to reasonably respond to new threats over the next two years. In particular, it should include elements making it resistant to keyboard monitoring programs like Back Oriface and Netbus.

Corporate-world Solution

As we started doing our research, it was clear the "standard corporate model" was to build a fortress. Corporate networks were behind firewalls which allowed almost no protocols to travel through them and often used proxy servers for people inside the firewall to have access to Internet services. There might be a sacrificial web or email server siting outside the firewall, but that was all.

This is not a viable solution in the academic or research environment. An important factor in a research environment is to provide for the unexpected. Would the web have been developed (at a HEP site, by the way) without that kind of open environment?

Mini-corporate Solution

Another possibility was to treat the business people as sort of a mini-corporation and place them behind the kinds of barriers described above. While that thought made the physicists happy for a few minutes, a only little reflection was necessary to realize these people **support** the rest of the Lab. To perform their mission, they have to communicate fairly heavily concerning budgets, personnel, and financial issues. Not only that, but realistically, the senior research leaders were often heavily involved in financial aspects of the experiments and needed access to budget information.

Layered Solution

A layered solution finally survived a number of discussions and presentations. The researchers would see basically no changes in their current environment in the way of additional restrictions. People directly using the business system (as opposed to just viewing information through a web interface) would be required to have a standardized hardware and software configuration with basically interchangeable but fully functional workstations -- all data being stored on a home directory server rather than locally. Mission critical users would have workstations locked down to running just the business application and not much else and would be on the same network as the servers -- and very restrictive filtering rules would apply to that subnet.

Plan A Features

Major features of the "Plan A" design are:

- Mission critical work can be done using what works now
- Token cards will provide two-factor authentication
- IDS will watch for what gets past filters
    - NIDS for network attacks
    - System IDS for critical servers
- Response to intrusion
    - Mission critical functions proceed
    - Business users reconnected on priority basis
    - Management understands “air gap” concept
    - Physics systems handled “appropriately”

Role of IDS

Intrusion Detection Systems play key roles in this environment. For the researchers, the IDS acts as the "cop on-call". This allows a much higher level of comfort (appropriate or not) without having to have overly restrictive barriers. For the business users, the IDS acts more like a security guard where we want a near real time warning and reaction to the threat of compromise. On the mission critical side, the IDS should function like the Maytag repairman -- always good insurance when the "impossible" occurs.

Future

In the future, we see applying a similar layered model to the networks handling the accelerator controls. Due to differing requirements, the expectation is there would be a decreased emphasis on the traffic filters and an increased emphasis (with higher trigger sensitivity) on intrusion detection systems.

We will use our experience in implementing the restrictions for Business Systems to gain a better understanding of the security issues and to explore ways which enable us to be secure without trading off too much functionality. The business area provides a good proving ground in that it is easier there to start out with strict controls and it is also easier to mandate a standard hardware and software configuration.

Suggestions and other feedback are greatly appreciated. Provide said feedback through email to the author and not via "exploration" of the SLAC network! Thanks.