All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Write lock the past, access control the present, anticipate the future

It seems that a lot of the large-scale challenges faced in information protection today stem from corruption rather than leakage. While leakage has long been more of a concern to many than other protection objectives, integrity has always been necessary in order to prevent leakage and denial of services.

Write lock the past

One of the easiest ways to maintain the integrity of content is to make it non-writeable. This is not new – it is in fact very old. In today's environment, where virus writers rename files and directories (a longstanding attack method), delete files (another longstanding one), and put Trojan horses in place of other files they have deleted (another old one), it seems obvious that files and directories that don't need to be changed should not be changeable. Simply write lock them and throw away the key – so to speak – and they are golden. Version control existed at least in the 1970s where DEC computers commonly provided this. The version you see is the latest one, but the past ones are retained under the same name with numerical counters as extensions. We have the past secured, and we can difference the future to see what changed – and un-change it. Version controlled repositories like CVS provide much the same capability, allowing you to go back to any point in time and see what things looked like then. Disk is cheap – just do it!

Access control the present

You can't really write lock the present – or you can't do your job. So access control it. There are plenty of access control schemes around, with varying granularity and administrative overhead. But regardless of the details, it's just ridiculous to allow anyone to write – or read something that they aren't responsible for. When they get attacked and their access is granted to an unauthorized party, you are granting access to everything they can access. Stop it! Only grant them what they need and you will also only grant the attacker access to the things the people they have successfully attacked have access to. This is not new. In the 1980s I ran a company with about 250 employees. They had a user ID and password, and they used it to get paid, so they kept it close. When they logged in, they got a menu. It presented all of the things they were allowed to do. Whatever they picked, they were authorized for, and they could only see what they were allowed to do. It was simple to manage, and I personally managed it for all 250 employees. It took about a minute per employee hire, job change, or termination. 250 minutes is only 4 hours for the whole company. If employee churn was once per quarter, that would have been 16 hours per quarter. Even a CEO could do it.

Anticipate the future

This is the easiest of all. To anticipate the future, read about the past. Every few years, something new might come up, but if you take care of everything that has already happened, you will almost certainly be safe almost all the time. And if you write lock the past and access control the present, you will be able to recover in the future, with minimal loss.

