Mission Impossible: Stopping Data Leakage (1)

by M. E. Kabay, PhD, CISSP
Associate Professor, Computer Information Systems
Norwich University, Northfield VT

As regular readers know by now, information security assurance must include protection of data confidentiality, possession, integrity, authenticity, availability and utility. Perhaps the most insidious breach of confidentiality and possession of sensitive or proprietary data is unauthorized copying. This is hardly a new problem; physical security applied to written records is as old as writing. The Caesar cipher, designed to protect military information in transit from commanders to field officers, is more than 2,000 years old. In more recent times, people have been copying data from computer systems for decades. For example, in the early 1970s, three computer operators stole copies of 3 million customer names from the Encyclopedia Britannica; estimated commercial value of the names was $1 million at the time. Many other cases of outright data theft are well known; some examples are as follows:

- Employees have sold documentation about tax audit procedures to help unscrupulous buyers reduce the risks of being audited;
- Police officer have sold computerized criminal records to criminals;
- Records about sick people have been obtained from health services organizations and sold to to drug companies;
- Subscribers' credit card data have been stolen from many organizations and used for fraud.

This loss of control over confidential information is known as _data leakage_. It's a very difficult problem, and it is probably impossible to stop altogether, even in theory. Most operating systems (although not Windows 9x) can enforce restrictions based on access-control lists; one can easily define lists of authorized people for specific resources (data or devices) and prevent others from accessing those resources. Even more restrictively, some high-security operating systems typically used for government and military work enforce security policies using compartmentalized security levels; for example, they make it impossible to copy a file from a higher-security partition to a lower-security partition such as a removable disk.

The fundamental difficulty, though, is that no operating system in the world can distinguish between an honest authorized user and a dishonest authorized user. An authorized user is going to be able to bypass even the best automated restrictions because there are so many covert channels for transmitting information out of a secured area.

***

In the next article in this occasional series on computer crime techniques, I'll look at the easy availability of portable data storage media and their implications for data theft.

***

NEW! 18-month online Master of Science in Information Assurance offered by Norwich