

# File Cabinets and Pig Latin: Guards for Information Assets

Lawrence R. Rogers  
Software Engineering Institute

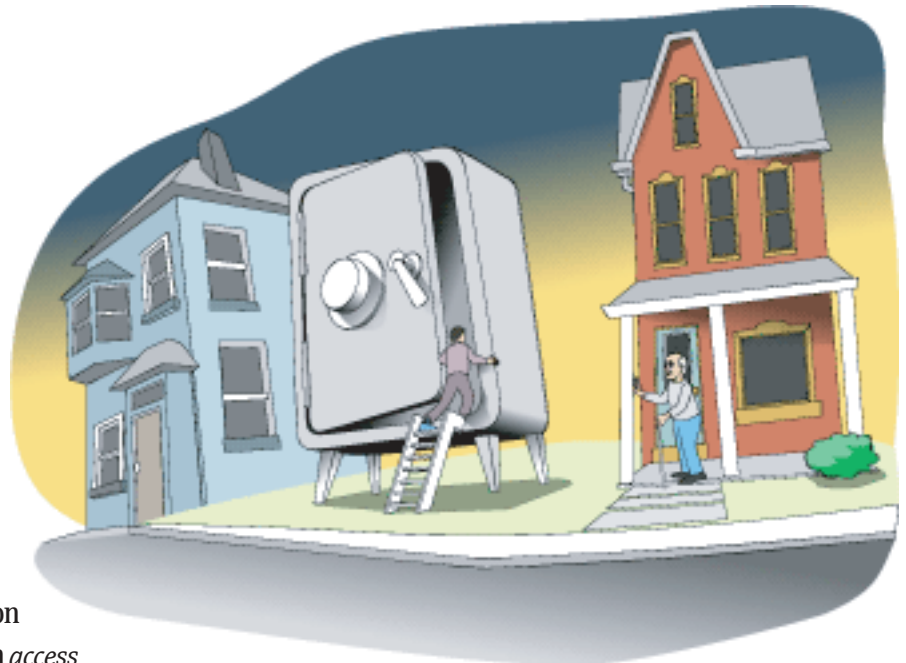
Carnegie Mellon University  
Pittsburgh, PA

Think about your checkbook, your insurance policies, perhaps your birth certificate or passport, and other important documents and papers you have around your house. Where are they? Probably, they are stored in a filing cabinet or a safe that can be or is routinely locked. Why did you divide your information into the important and the unimportant, and then store the important items in a locked container?

Without realizing it, you were satisfying one of the three components of information security—*confidentiality*. Confidentiality attempts to keep secrets secret. Only those who are supposed to see the information in question should have access to it. You were keeping information sensitive to you and others away from those who should not be able to get to it. By the way, the other two components are *integrity* (Has my information changed?) and *availability* (Can I get at my information whenever I need it?).

You went beyond simply recognizing information confidentiality when you enforced it by using an *access control device*, namely the locked filing cabinet or safe. This device stands between the information and those seeking access, and it grants access to all who have the combination, the key, or whatever tool unlocks the container. As a defense in depth measure—where several layers of access control devices are used—you may also find that those containers are themselves in locked rooms. Would-be intruders must pass through several levels of controls before finally gaining access to the information they seek.

Now, think of a computer system such as the one at home or in your office. The job here is to control access to files and databases, generally called *information assets*. The access control device is the *access control list* or ACL. ACLs define who can perform actions on an information asset and the



actions that are allowed: reading and writing, for example. ACLs are the locked filing cabinet and safe equivalent for more traditional paper assets.

Different computer systems provide different types of ACLs. Some have fine-grained controls while others have virtually none. The key is to use all the controls that are available on your system. In some cases, you may have the choice of selecting which computer system you use to house your information assets. Select the system with the ACLs most appropriate to keeping your assets safe.

Frequently computer system vendors define ACLs that are overly permissive. This satisfies their need to ensure that access limitations don't get in the way of you using their systems. Your

challenge is to tighten those ACLs so that they properly restrict access to only those who need access. This means that you need to do something to the ACLs guarding information assets on your computers when you buy them.

Returning to the home environment, do you remember when adults in your house wanted to say something to one another that the children shouldn't understand? They spelled their message or used something like Pig Latin (ig-pay Atin-lay) to conceal the meaning of their conversation. This worked for a while, until the children learned to spell or could otherwise understand what was being said. What's really happening here?

Very simply, the adults could not control who could hear their conversation. It was inconvenient or perhaps impossible for them to go to another room where they couldn't be heard by anyone else. So they had to talk in a way that only those who knew the concealing scheme could understand what was being said.

On a computer system, when access to information cannot be limited, such as an e-commerce transaction carried out over the Internet, that information is concealed through a mathematical process called *encryption*. Encryption transforms information from one form (clear text) to another (cipher text). Its intent is to hide information content from those who have neither the transformation method nor the particulars (the decryption keys) needed to transform the cipher text back to its original clear text form. The cipher text is gibberish and remains so when you don't have the scheme or the keys.

Eventually, the children learned how to spell and also learned the ways of Pig Latin. They could understand the conversations the adults were having. While they

could also understand the conversations held weeks, months, or even years ago, the information in those conversations was no longer important. The encryption scheme was strong enough to guard the information during its useful lifetime.

Computer-based encryption schemes must also withstand the test of time. For example, if a credit card encryption scheme needs six months to break, the resulting credit card number is likely to be still valid and, therefore, useful to an intruder after that six-month period. In this case, the encryption scheme isn't strong enough to guard the information for its entire useful lifetime.

In summary, to guard information assets, be they paper or computer files, you need to limit who has access to them by using the access control devices of filing cabinets, safes, and, on a computer system, access control lists. For assets where access cannot be sufficiently limited, you need to encrypt them strongly enough so that the time it takes to decrypt them is longer than the useful life of the asset.

Appy-hay omputing-cay!

