16.5. Example Information Flow Controls

Like the program-based information flow mechanisms discussed above, both special-purpose and general-purpose computer systems have information flow controls at the system level. File access controls, integrity controls, and other types of access controls are mechanisms that attempt to inhibit the flow of information within a system, or between systems.

The first example is a special-purpose computer that checks I/O operations between a host and a secondary storage unit. It can be easily adapted to other purposes. A mail guard for electronic mail moving between a classified network and an unclassified one follows. The goal of both mechanisms is to prevent the illicit flow of information from one system unit to another.

16.5.1. Security Pipeline Interface

Hoffman and Davis [477] propose adding a processor, called a **security pipeline interface** (SPI), between a host and a destination. Data that the host writes to the destination first goes through the SPI, which can analyze the data, alter it, or delete it. But the SPI does not have access to the host's internal memory; it can only operate on the data being output. Furthermore, the host has no control over the SPI. Hoffman and Davis note that SPIs could be linked into a series of SPIs, or be run in parallel.

They suggest that the SPI could check for corrupted programs. A host requests a file from the main disk. An SPI lies on the path between the disk and the host (see Figure 16-4.) Associated with each file is a cryptographic checksum that is stored on a second disk connected to the first SPI. When the file reaches the first SPI, it computes the cryptographic checksum of the file and compares it with the checksum stored on the second disk. If the two match, it assumes that the file is uncorrupted. If not, the SPI requests a clean copy from the second disk, records the corruption in a log, and notifies the user, who can update the main disk.

Figure 16-4. Use of an SPI to check for corrupted files.

The information flow being restricted here is an integrity flow, rather than the confidentiality flow of the other examples. The inhibition is not to prevent the corrupt data from being seen, but to prevent the system from trusting it. This emphasizes that, although information flow is usually seen as a mechanism for maintaining confidentiality, its application in maintaining integrity is equally important.

16.5.2. Secure Network Server Mail Guard

Consider two networks, one of which has data classified SECRET[4] and the other of which is a public network. The authorities controlling the SECRET network need to allow electronic mail to go to the unclassified network. They do not want SECRET information to transit the unclassified network, of course. The Secure Network Server Mail Guard (SNSMG) [937] is a computer that sits between the two networks. It analyzes messages and, when needed, sanitizes or blocks them.

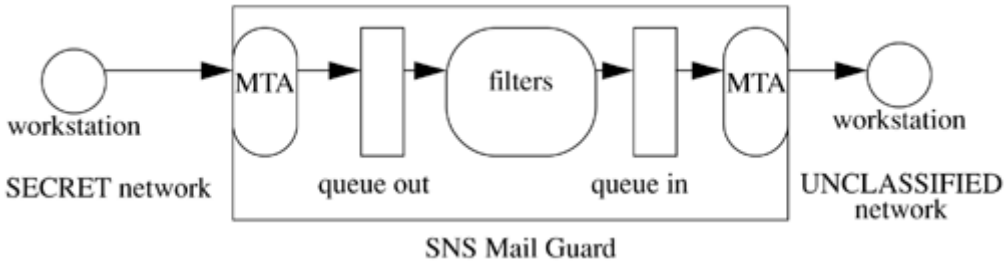
[4] For this example, assume that the network has only one category, which we omit.

The SNSMG accepts messages from either network to be forwarded to the other. It then applies several filters to the message; the specific filters may depend on the source address, destination address, sender, recipient, and/or contents of the message. Examples of the functions of such filters are as follows.

- Check that the sender of a message from the SECRET network is authorized to send messages to the unclassified network.
- Scan any attachments to messages coming from the unclassified network to locate, and eliminate, any computer viruses.
- Require all messages moving from the SECRET to the unclassified network to have a clearance label, and if the label is anything other than UNCLASS (unclassified), encipher the message before forwarding it to the unclassified network.

The SNSMG is a computer that runs two different message transfer agents (MTAs), one for the SECRET network and one for the unclassified network (see Figure 16-5). It uses an assured pipeline [785] to move messages from the MTA to the filter, and vice versa. In this pipeline, messages output from the SECRET network's MTA have type **a**, and messages output from the filters have a different type, type **b**. The unclassified network's MTA will accept as input only messages of type **b**. If a message somehow goes from the SECRET network's MTA to the unclassified network's MTA, the unclassified network's MTA will reject the message as being of the wrong type.

Figure 16-5. Secure Network Server Mail Guard. The SNSMG is processing a message from the SECRET network. The filters are part of a highly trusted system and perform checking and sanitizing of messages.



The SNSMG is an information flow enforcement mechanism. It ensures that information cannot flow from a higher security level to a lower one. It can perform other functions, such as restricting the flow of untrusted information from the unclassified network to the trusted, SECRET network. In this sense, the information flow is an integrity issue, not a confidentiality issue.