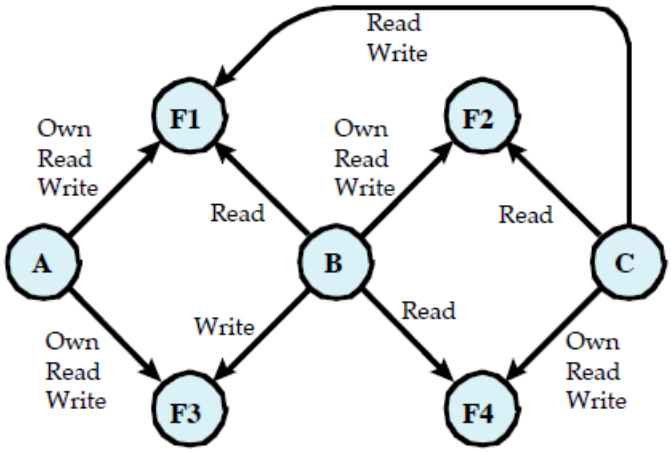
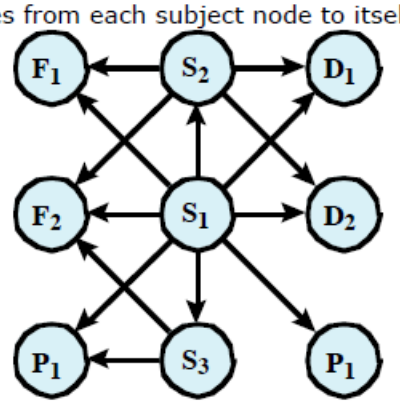
第一次作业：习题 4.1、4.3、4.10

4.1 a.



b. For simplicity and clarity, the labels are omitted. Also, there should be arrowed lines from each subject node to itself.



c. A given access matrix generates only one directed graph, and a given directed graph yields only one access matrix, so the correspondence is one-to-one.

4.3 a. The advantage of four modes is that there is more flexibility to control access to memory, allowing finer tuning of memory protection. The disadvantage is complexity and processing overhead. For example, procedures running at each of the access modes require separate stacks with appropriate accessibility.

b. In principle, the more modes, the more flexibility, but it seems difficult to justify going beyond four.

4.10 a. $r_1 \succcurlyeq r_2 \Rightarrow authorized\_permissions(r_2) \subseteq authorized\_permissions(r_1) \wedge authorized\_users(r_2) \subseteq authorized\_users(r_1)$

b. $r \succcurlyeq r_1 \wedge r \succcurlyeq r_2 \Rightarrow r1 = r2$

第二次作业：复习题 7.10，习题 7.1、7.4、8.4、8.6、8.8

7.10 An amplification attack involves sending packets to intermediaries with a spoofed source address for the target system. They differ in generating multiple response packets for each original packet sent, typically by directing the original request to the broadcast address for some network. Alternatively they use a service, often DNS, that can generate a much larger response packet than the original request.

7.1 In a DoS attack using ICMP Echo Request (ping) packets 500 bytes in size, to flood a target organization using a 0.5 Megabit per second (Mbps) link the attacker needs 500000 / (500 × 8) = 125 packets per second. On a 2-Mbps link its 2000000 / (500 × 8) = 500 packets per second. On a 10-Mbps link its 10000000 / (500 × 8) = 2500 packets per second.

7.4 The answers for the DNS amplification attack are the same as in Problem 7.1. On a 0.5-Mbps link, 125 packets, each of 500 bytes, are needed per second. 500 pps are needed to flood a 2-Mbps link, and 2500 pps to flood a 10-Mbps link. Assuming a 60-byte DNS request packet then 125 × 60 × 8 = 60 kbps is needed to trigger the flood on a 0.5-Mbps link, 240 kbps to flood the 2-Mbps link, and 1.2 Mbps to flood the 10-Mbps link. In all cases the amplification is 500 / 60 = 8.3 times.

8.4

a: This rule wants to catch attempts to create a new database instance. Line 1, the rule header, states that interesting packets are flowing from external IP addresses for database servers responding on Oracle ports. Line 2 is the text alert to be reported. Line 3 defines two additional matching conditions: first, packets must be directed to a server and must be part of an already established TCP connection, and second, the case-independent string "create database" must be contained in the packet payload.

b: Typically, a system administrator would configure a system to forbid database creation from across the Internet. Such attempts would be blocked by the firewall. The external NIDS would simply be a way of segregating out such attacks and alerting on them. If the NIDs is inside the firewall, it would be able to catch a serious deficiency in firewall behavior.

8.6

A file integrity checking tool such as tripwire can be very useful in identifying changed files or directories on a system, particularly when those change should not have occurred. However most computer systems are not static, and significant numbers of files do change constantly. Hence it is necessary to configure tripwire with a list of files and directories to monitor, since otherwise reports to the administrator would be filled with lists of files that are changing as a matter of normal operation of the system. It is not too difficult to monitor a small list of critical system programs, daemons and configuration files. Doing this means attempts to alter these files will likely be detected. However the large areas of the system not being monitored means an attacker changing or adding files in these areas will not be detected. The more of the system that is to be monitored, the more care is needed to identify only files not expected to change. Even then, it is likely that user's home areas, and other shared document areas, cannot be monitored, since they are likely to be creating and changing files in there

regularly. As well, there needs to be a process to manage the update of monitored files (as a result of installing patches, upgrades, new services, configuration changes etc). This process has to verify that the changed files are correct, and then update the cryptographic checksums of these files. Lastly the database of cryptographic checksums must be protected from any attempt by an attacker to corrupt it, ideally by locating on read-only media (except when controlled updates are occurring).

8.8 Let WB equal the event {witness reports Blue cab}. Then:

$$\Pr[\text{Blue}/\text{WB}] = \frac{\Pr[\text{WB}/\text{Blue}]\Pr[\text{Blue}]}{\Pr[\text{WB}/\text{Blue}]\Pr[\text{Blue}] + \Pr[\text{WB}/\text{Green}]\Pr[\text{Green}]}$$

$$= \frac{(0.8)(0.15)}{(0.8)(0.15) + (0.2)(0.85)} = 0.41$$

This example, or something similar, is referred to as "the juror's fallacy."