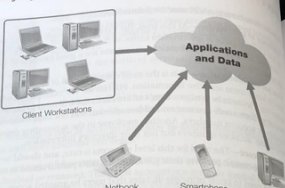
FIGURE 6-1
Portability of SaaS.



Private Sector Case Study

Cloud Collaboration is a large new media company that has recently launched a **Software as a Service (SaaS)** office suite. This suite includes a word processor, as well as presentation, e-mail, calendar, and spreadsheet applications. Also included are collaboration and Web authoring tools.

SaaS is a model of software distribution that hosts software in a cloud-based environment on a subscription basis. Instead of simply selling an application, a SaaS vendor offers access to the applications for a small subscription fee. The application and data are stored on the vendor's servers and the customer accesses them remotely. This benefits the customer by lowering operating costs, and adding security and portability. SaaS sometimes costs less, both in upfront and ongoing costs, than buying software in a traditional manner. This is especially true for a small-business environment that may not have the capital necessary for the hardware associated with large centralized applications.

NOTE
Cloud Collaboration's office suite provides services for many organizations from a single server, just as many families might live in a single apartment building. Each organization's data is segregated from the others, but it all resides on the same server.

SaaS also adds a new layer of document security; even if a workstation is physically stolen, the information is safe because all of the documents are stored on the vendor's servers instead of the customer's workstation. Storing the information remotely also gives the customer an amazing amount of portability. Any system with appropriate access software can access the data. In Cloud Collaboration's case, the office suite is Web-based, so any system with a Web browser can be used to access the applications, including smartphones. The portability of SaaS can be seen in Figure 6-1.

SaaS has its challenges as well. Privacy is a major concern because multiple organizations will have access to Cloud Collaboration's systems. Cloud Collaboration's customers do not want other groups or even Cloud Collaboration employees to have the ability to access their data. These are concerns above the normal data security issues internal to an organization. There is also the issue of ease of use. End users at the organizations using Cloud Collaboration's SaaS do not expect to have to log into their word processor, for example. For Cloud Collaboration's SaaS offering to be widely adopted, its security features must be seamless to end users. While these problems are daunting, they can be addressed with a well-designed access control system.

The first obstacle that Cloud Collaboration needs to address is cording off users and organizations to make sure information is not unintentionally shared between unrelated groups. This is handled with a RBAC system. Each organization is a "role" in Cloud Collaboration's design; data is restricted then by role. Only the organization that created the information has access to it initially, but access can be explicitly granted to other roles by sharing the data. Cloud Collaboration's own employees are included in this layer of control, guaranteeing that even internal Cloud Collaboration users can see only the data that they have rights to see.

Cloud Collaboration customers also have the ability to set up a mandatory access control schema. They can set up an administrator or group of administrators for their SaaS applications. These administrators control organization-wide rights to accessing the data. Administrators can explicitly add or deny access to users and groups of users in a similar manner to data that is stored locally. This allows organizations to have strict access controls based on their own access control policies.

There is also the ability to have DAC on user-created data. If an organization does not have the infrastructure for a centralized administrator, each document owner can set the access controls for his or her documents by explicitly allowing or denying access to other users in the organization, and even to other organizations.

Cloud Collaboration also wanted to allow customers the ability to verify document integrity, as required by various regulations. To achieve this, it implemented a granular, robust document logging and auditing system. Managers and end users can see what changes were made to a document, who made them, and when they were made. Users can also revert to a previous version of a document. This robust logging allows users to verify the integrity of the information stored in the system.

Cloud Collaboration also wanted to make all of this security seamless and invisible to the end user. Users are not used to logging in to a word processor or calendar application, and it would be difficult to convince new customers to adopt Cloud Collaboration's SaaS offering if it added a layer of unfamiliarity or complexity to applications that are constantly used and needed in an organization. To avoid this, Cloud Collaboration created an authentication API utilizing Security Assertion Markup Language 2.0 (SAML 2.0). SAML is an XML-like markup language that allows Web applications to pass a security token for user identification. This allows for organizations using Cloud Collaboration's SaaS to utilize a single sign-on (SSO) system. The end user logs onto his or her workstation, and that username and password acts as the login for Cloud Collaboration's

SaaS business suite as well. This also allows organizations to take advantage of existing password complexity and expiration rules.

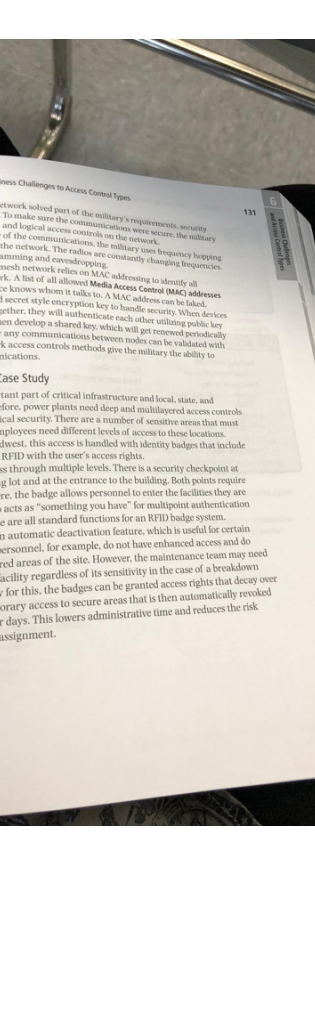
Utilizing a deep and robust access control system, Cloud Collaboration was able to provide information privacy and integrity for its SaaS customers.

Public Sector Case Study

The U.S. military needed a way to communicate information quickly and securely in the rapidly changing environment of a battlefield. Wired communications, while secure and robust, had significant drawbacks. Communication lines could easily be severed, and military personnel were limited to communicating only at fixed locations. Radio and wireless communications removed the threat of cut lines and expanded the range of communications, allowing military personnel to communicate with remote units, but only to a fixed range. Stationary installations were still needed as base stations and throughput degraded the farther the units were from the base station. That led the military to turn to a new type of wireless networking called wireless mesh networks.

Wireless mesh networks are based on a distributed network mesh topology. Each node in the network connects to multiple nodes. Each node also acts as a router for the data it connects to, allowing traffic to hop along multiple paths to a destination. This allows for a very robust and flexible network. The loss of one node will not hurt the network, and nodes can be added at will. Range of the total network is also massive because nodes don't need to be close to a central point. They need just one other node to function. An example of a mesh network can be seen in Figure 6-2.

FIGURE 6-2
Mesh network topology.



While a wi
remained a m
implemented
For the phy
on the radios
This allows th
For logical
of the devices
is generated a
so they also u
in the network
infrastructure
to handle enc
that key. These
secure its wire

Critical Infra

Power plants a
national econ
due to concern
be secured, an
At a plant in t
images of the
The RFID h
the entrance t
a badge to ent
authorized to
onto secure sy
The badges
personnel. Ma
not require ac
access to any
or special proj
time. This allo
over a numbe
of human erro

While a wireless mesh network solved part of the military's requirements, security remained a major concern. To make sure the communications were secure, the military implemented both physical and logical access controls on the network.

For the physical security of the communications, the military uses frequency hopping on the radios connected to the network. The radios are constantly changing frequencies. This allows them to avoid jamming and eavesdropping.

For logical security, the mesh network relies on MAC addressing to identify all of the devices in the network. A list of all allowed **Media Access Control (MAC) addresses** is generated and each device knows whom it talks to. A MAC address can be faked, so they also utilize a shared secret style encryption key to handle security. When devices is the network first link together, they will authenticate each other utilizing public key infrastructure (PKI) and then develop a shared key, which will get renewed periodically to handle encryption. Now any communications between nodes can be validated with that key. These two network access controls methods give the military the ability to secure its wireless communications.

Critical Infrastructure Case Study

Power plants are an important part of critical infrastructure and local, state, and national economies. Therefore, power plants need deep and multilayered access controls due to concerns over physical security. There are a number of sensitive areas that must be secured, and various employees need different levels of access to these locations. At a plant in the upper Midwest, this access is handled with identity badges that include images of the user and an RFID with the user's access rights.

The RFID handles access through multiple levels. There is a security checkpoint at the entrance to the parking lot and at the entrance to the building. Both points require a badge to enter. From there, the badge allows personnel to enter the facilities they are authorized to enter. It also acts as "something you have" for multipoint authentication onto secure systems. These are all standard functions for an RFID badge system.

The badges also have an automatic deactivation feature, which is useful for certain personnel. Maintenance personnel, for example, do not have enhanced access and do not require access to secured areas of the site. However, the maintenance team may need access to any area of the facility regardless of its sensitivity in the case of a breakdown or special project. To allow for this, the badges can be granted access rights that decay over time. This allows for temporary access to secure areas that is then automatically revoked over a number of hours or days. This lowers administrative time and reduces the risk of human error in rights assignment.