Безпека операційних систем і комп'ютерних мереж

Лекція 21

Анотація

Описано протоколи захисту віртуальних з'єднань на канальному рівні. PPTP (Microsoft) - розширення протоколу PPP. L2F (Cisco Systems, Shiva, Nothern Telecom) - більш зручний для використання Інтернет-провайдерами, має аналогічну структуру пакетів і подібну схему використання. L2TP (IETF) - побудований на основі PPTP і L2F, поєднує переваги обох, але успадкував обмеження L2F: відсутність захисту з'єднання комп'ютера віддаленого користувача з сервером провайдера.

Протоколи захисту віртуальних каналів на мережевому рівні представлені протоколом IPSec (входить в специфікацію IPv6, сумісний з IPv4), який охоплює кілька областей: шифрування, аутентифікацію і керування ключами. Архітектурно IPSec складається з декількох рівнів: протоколи захисту віртуального каналу і узгодження параметрів захисту (верхній рівень), криптографічні алгоритми, що використовуються в протоколах AH і ESP, алгоритми управління та узгодження ключів, що використовуються протоколом ISAKMP (середній рівень) та "домен інтерпретації" - база даних з інформацією про протоколи, що використовуються, а також їх параметри (нижній рівень).

Розглянуто протоколи захисту каналів на сеансовому рівні. Найбільш поширений SSL / TLS (Netscape Communications), що є загально визнаним стандартом. Описано процедури встановлення SSL-сесій і аутентифікації. Представлений протокол SOCKS, що розроблений для організації взаємодії між клієнт-серверними застосуваннями.