Activities Board (IAB) has developed a set of guidelines for secure electronic mail. The new security standard will provide end to end encryption and authentication of messages through the use of public and private keys. The group hopes to have the 'privacy enhanced mail' guidelines adopted as an Internet standard sometime this year.

The architecture is similar to OSI's 1988 standard for X.400. Few of the messaging systems on Internet are X.400-based, and those that are tend to use the 1984 version, which does not include the security enhancements. It is unlikely that the X.400 OSI standard will be widely used on Internet for another five years, and the group's guidelines are an intermediate measure.

Although X.400 and privacy enhanced mail share similar architectures, there are some key differences between the two. Principally, privacy enhanced mail has fewer user-configurable security levels, and focusses only on security issues visible to the end user. It adds a software module to the user agent (UA) which, unlike X.400, does not require revision of existing mail applications. The module uses RSA encryption for privacy and authentication.

Houston hackers attack US agencies

Computer hackers active in the Houston, Texas, are reported to have compromised the telecommunication facilities of various local US government agencies. The two incidents disclosed thus far involve the Johnson Space Center of the US National Aeronautics and Space Administration and the local office of the US Drug Enforcement Administration (DEA), a major component of the US Justice Department. For at least 18 to 24 months members of this group used the unauthorized access that they had gained to these two agencies' private branch exchange (PBX) facilities to gain further access to the US government's Federal Telecommunications System 2000 (FTS 2000) private interagency network.

FTS 2000 is operated under a long term contract by the US Sprint Telecommunications Co. Both Sprint and the US General Services Administration (GSA), which administers the contract, had apparently been unaware of the hacker intrusions into the network until after an account of it was published by the *Houston Chronicle*. One source familiar with the situation indicated that GSA has been uninterested in providing any sort of security for FTS 2000. It has relied upon each seperate Federal Government agency to ensure the security of its use of FTS 2000. (The Houston DEA fraud was actually discovered by Southwestern Bell, which provides local telecommunication service in the Houston area.)

These hackers may have cost the DEA upwards of $2 million in unauthorized long distance domestic and international voice and data call charges. It has been estimated that the cost of the Johnson Space Center break-in may be as much as $12 million. However, a NASA representative claimed that the loss was more like $10 000 for the two year period. (A source familiar with the situation suggested that NASA's actual loss was somewhere between these two figures.)

Belden Menkus

Revlon and Logisticon settle differences

The two companies have recently agreed to settle out of court their dispute over an inventory management system developed by Logisticon for Revlon (see January *CFS*). Revlon had refused to make a $180 000 progress payment on the $1.2 million order, claiming that the software was "inadequate" for their purposes. In retaliation, Logisticon gained access to the system overnight, and disabled the software. The action forced Revlon to close two distribution centres for three days.

Revlon subsequently filed a suit against Logisticon for extortion, breach of contract,

tresspass and interference, claiming that Logisticon's action was "commercial terrorism". Although prepared to confirm that an agreement had been reached, neither side would discuss the terms and agreements of the out of court settlement. Nor would they comment on what compensation, if any, was to be paid.

Modem maker distributes viruses

At least 200 units distributed by GVC Technologies, a Sparta, New Jersey-based modem maker, contained the so-called 'Stoned' or 'Marijuana' computer virus. They were part of a lot of 2000 sold by GVC to CompuAdd, an Austin, TX-based computer retailer, which then distributed the units nationally in the US. GVC have laid the blame for the introduction of the virus on a Chinese company which under contract had duplicated the software used with the modems.

This does not appear to be the first time that a computer virus has been introduced into purportedly factory clean software and allowed to propagate into customer computers because the manufacturer's and distributor's product quality assurance effort either was inadequate — or in some instances, essentially nonexistent.

Belden Menkus

Canadians convict first computer pirate

More than five years after the offence was added to the federal criminal code, the first criminal conviction for software piracy has been registered in a Quebec court, according to a recent report in the *Montreal Gazette*. Marc Alarie was fined C$5000 by Quebec Court judge André Chaloux. He could have received a maximum sentence of 10 years in prison, and an unlimited fine.

Alarie, along with Normand Pigeon, currently face lawsuits for C$180 000 filed on behalf of SBI Technologies Inc, a St. Laurent software producer. Both are former employees of SBI. During a preliminary hearing the Crown presented evidence gathered in three raids by the police. Alarie subsequently changed his plea on the piracy charge to guilty.

Alarie operated through a company called Services Cité Informatique Enr. SBI president Michel King estimated that the activities of this company cost SBI C$200 000 in lost revenue. King also claimed that the research and development effort on the software over eight years had cost SBI about C$1.4 million.

Power problems plague NYSE

Electric power supply problems continue to plague the computers of the New York Stock Exchange (NYSE). While its operations survived the August 1990 general electric power loss in Manhattan's financial district, the 23 November failure of an internal NYSE generator delayed trading for 90 minutes, and affected interconnected activities at several Chicago commodities trading exchanges. On 26 December there was an explosion and fire in the underground Consolidated Edison transformer that serves the building housing the Securities Industry Automation Association data processing facilities. This again delayed the start of NYSE trading for 90 minutes. Other US securities exchanges were not permitted, under the rules of the US Securities and Exchange Commission, to begin trading until the NYSE was able to begin operations for the day.

In a pertinent but unrelated incident, a power grid short circuit interrupted electric service on 11 December for an hour at the IBM Business Recovery Services facility in Tampa, Florida. An emergency generator kept the hardware operating, but dozens of people in the facility — including IBM customers carrying out backup and recovery tests — were evacuated from the site.

Belden Menkus