Computers & Security, 15 (1996) 585-590

Abstracts of Recent Articles and Literature

Helen Meyer

The new US encryption policy, *Angela Hickman.* Cylink, Digital Equipment Corp, IBM, and RSA Data Security are backing the US Government's proposal to ease export restrictions and to implement a system known as the Key Recovery Initiative. However, some privacy advocates and computer industry representatives say that the system neither goes far enough to ensure competition abroad nor limits the potential for governmental abuse. Under the new plan, the Government increases the size of exportable cryptography keys from 40 bits to 56 bits for a period of two years, provided that companies give the Government a way to access the encrypted messages. All key-size restrictions end thereafter if a legitimate method of 'key recovery' is provided. IBM proposed a 'key system' whereby the company gives the keys to decipher encrypted message headers to two independent parties as well as to a law enforcement agency upon receipt of a search warrant. A law enforcement agency could then unscramble the header but would be responsible for mathematically decoding the rest of the encrypted information. The new policy allows industry not government to develop the actual key recovery system, an approach that should ensure greater privacy. *PC Magazine, November 19, 1996, p. 37.*

Computer viruses: myth vs reality, *Bill Machrone.* The incidence of virus infection is simply far lower than what is claimed in the general press. This is not claiming that viruses are a hoax or that we shouldn't be concerned about them. A virulent outbreak can be difficult to eradicate and expensive in terms of effort and lost productivity. For example, the Hare virus, like 1992's Michelangelo virus scare, was more hype than reality. But both sold a lot of anti-virus software. Most of our systems have anti-virus software as a result. The vast majority of virus infections have come from the disks that come from software manufacturers. But what about those mail viruses? If you have an E-mail account, you more than likely got a warning about the 'Good Times' virus. Supposedly, you would get a message with 'Good Times' in the header. If you so much as opened the file, it would erase your hard disk. In this case, the warning was the virus. Countless megabytes of storage space were lost to this inane message. Mail systems choked on the sheer volume of messages and nobody ever saw the virus: it was a hoax. *PC Magazine, November 19, 1996. p. 85.*

Computer hackers turn to pager systems, *Michael McCormack.* Computer hackers in Britain have turned their attentions to the nation's pager systems and revealed a number of disturbing security lapses. Messages about the movements and security arrangements for Labour leader Tony Blair in the UK were tapped over British Telecommunications' (BT) system, as was sensitive information including till takings from pubs and shops, credit card authorization numbers and passwords for alarm systems. The majority of Britain's pager systems work on 25-year-old analogue technology and transmit over only 10 frequencies. Cracking them was no difficult feat for a generation of scanner enthusiasts weaned on digital cellphones.

By scanning all 10 channels, a hacker can quickly build up a database of thousands of calls. They can then use a

0167-4048/96/$15.00