New directions in commercial encryption and secrecy protocols.

Helen Ashman
Computer Science and IT, University of Nottingham, Nottingham NG8 1BB, U.K.
hla@cs.nott.ac.uk

Secure transmission of bulk data is of interest to many content providers. A commercially-viable distribution of content requires technology to prevent unauthorised access. Encryption tools are powerful, but have a performance cost. Without encryption, intercepted data may be illicitly duplicated and re-sold, or its commercial value diminished because its secrecy is lost.

Two technical solutions make it possible to perform bulk transmissions while retaining security without too high a performance overhead. These are:

1. a) hierarchical encryption - the stronger the encryption, the harder it is to break but also the more computationally expensive it is. A hierarchical approach to key exchange means that simple and relatively weak encryption and keys are used to encrypt small chunks of data, for example 10 seconds of video. Each chunk has its own key. New keys for this bottom-level encryption are exchanged using a slightly stronger encryption, for example a whole-video key could govern the exchange of the 10-second chunk keys. At a higher level again, there could be daily or weekly keys, securing the exchange of whole-video keys, and at a yet higher level, a subscriber key could govern the exchange of weekly keys. At higher levels, the encryption becomes stronger but is used less frequently, so that the overall computational cost is minimal. The main observation is that the value of each encrypted item determines the strength of the key used to secure it.

2. b) non-symbolic fragmentation with signal diversity - communications are usually assumed to be sent over a single communications medium, and the data to have been encrypted and/or partitioned in whole-symbol packets. Network and path diversity break up a file or data stream into fragments which are then sent over many different channels, either in the same network or different networks. For example, a message could be transmitted partly over the phone network and partly via satellite. While TCP/IP does a similar thing in sending different packets over different paths, this is done for load-balancing purposes and is invisible to the end application. Network and path diversity deliberately introduce the same principle as a secure communications mechanism - an eavesdropper would need to intercept not just one transmission path but all paths used. Non-symbolic fragmentation of data is also introduced to further confuse any intercepted stream of data. This involves breaking up data into bit strings which are subsequently disordered prior to transmission. Even if all transmissions were intercepted, the cryptanalyst still needs to determine fragment boundaries and correctly order them.

   These two solutions depart from the usual idea of data encryption.

Hierarchical encryption is an extension of the combined encryption of systems such as PGP but with the distinction that the strength of encryption at each level is determined by the "value" of the data being transmitted. Non-symbolic fragmentation suppresses or destroys bit patterns in the transmitted data in what is essentially a bit-level transposition cipher but with unpredictable irregularly-sized fragments.

Both technologies have applications outside the commercial and can be used in conjunction with other forms of encryption, being functionally orthogonal.

Last update (HTML version) 16th October 2001, Helen Ashman.