Manual Authentication Technology

Authentication in computer security provides human users assurance that the agent they are communicating with is the one it claims to be. Just about all computer security applications, including secure communication, depend on authentication. My current research develops a new authentication technology that uses human trust and interactions to eliminate the need for passwords, shared secret keys, and trusted third parties, which are highly vulnerable to human misuses as in Bluetooth and the Internet. For example, an attacker can easily guess a weak password used to authenticate human users. But if good password disciplines are imposed then the acts of inventing and remembering them add up to a significant burden on humans.

This new technology can authenticate data as follows. For electronic devices to agree on the same data that are exchanged over an insecure medium, their human owners need to manually compare a *short digest* of both the data and some key. Since human comparison of a digest via conversation, phone or text message is time-consuming, a digest function must have a very short output of 16─20 bits. A keyed digest function is a new concept that has close links with probability theory through its use and security specification. Although given a key a digest function is weaker than a cryptographic hash function, the strategy behind all applications is to use each key once as well as keep it unknown until everyone is committed to their view of the authenticated data.

Using a digest function and the strategy mentioned above, I have designed a range of one-way, pair-wise and group authentication protocols using human interactions. The crucial advantages of these schemes are: (1) they do not rely on passwords, PINs, privates keys or PKI, and (2) they appear to maximise the level of security obtained relative to a given amount of human work while minimise the computation processing. Some of these have been standardised by ISO (L.H. Nguyen, Editor, ISO/IEC 9798-6: 2010) and are the subjects of three international patent applications. The latter include applications of these protocols in CHIP and PIN technology, online banking and bootstrapping of ad hoc networks.

Since a digest function underpins this technology, I am currently devising new digest algorithms which are both secure and more efficient than (long-output) cryptographic hash functions, e.g. SHA-1. One way to exploit the short output of digest functions is to use word-level integer multiplication instructions available in all microprocessors. This approach has resulted in a new construction that enjoys very fast implementation as well as strong and provable security as recently demonstrated by me. Moreover, this algorithm can be securely generalised to a long-output digest scheme without increasing the word length so that it can be used for a wider range of applications, including message authentication codes, than those protocols considered here.