WARSAW UNIVERSITY OF TECHNOLOGY
DEVELOPMENT PROGRAMME

Centrum Studiów Zaawansowanych PW
Center for Advanced Studies WUT

“Covert Cryptography and Steganography”

One of the principal weaknesses of all encryption systems is that the form of the output data (the ciphertext), if intercepted, alerts the intruder to the fact that the information being transmitted may have some importance and that it is therefore worth attacking and attempting to decrypt it. This aspect of ciphertext transmission can be used to propagate disinformation, achieved by encrypting information that is specifically designed to be intercepted and decrypted. In this case, we assume that the intercept will be attacked, decrypted and the information retrieved. The ‘key’ to this approach is to make sure that the ciphertext is relatively strong (but not too strong!) and that the information extracted is of good quality in terms of providing the attacker with ‘intelligence’ that is perceived to be valuable and compatible with their expectations, i.e. information that reflects the concerns/interests of the individual(s) and/or organisation(s) that encrypted the data. This approach provides the interceptor with a ‘honey pot’ designed to maximize their confidence especially when they have had to put a significant amount of work in to ‘extracting it’. The trick is to make sure that this process is not too hard or too easy. ‘Too hard’ will defeat the object of the exercise as the attacker might give up; ‘too easy’, and the attacker will suspect a set-up!

In addition to providing an attacker with a honey-pot for the dissemination of disinformation, it is of significant value if a method can be found that allows the real information to be transmitted by embedding it in non-sensitive information after (or otherwise) it has been encrypted, e.g. camouflaging the ciphertext. This is known as Steganography which is concerned with developing methods of writing hidden messages in such a way that no one, apart from the intended recipient, knows of the existence of the message in contrast to cryptography in which the existence of the message itself is not disguised but the content is scrambled. Steganography provides a significant advantage over cryptography alone in that messages do not attract attention to themselves, to messengers, or to recipients. No matter how well plaintext is encrypted (i.e. how unbreakable it is), by default, a ciphertext will arouse suspicion and may in itself be incriminating, as in some countries encryption is illegal. This seminar discusses methods of ‘hiding’ encrypted information in digital signals and image. This provides a facility for the authentication and self-authentication of documents such as letters, certificates and audio files. For example, the self-authentication of e-documents sent as attachments over the internet provides a solution for exchanging legal and financial transactions that have traditionally relied on paper based documents to secure authenticity. The method also provides a unique way of ‘propagating’ disinformation in the form of an encrypted document which contains hidden information.

Lecture co-financed by the European Union in scope of the European Social Fund

HUMAN CAPITAL
HUMAN – BEST INVESTMENT!

EUROPEAN UNION
EUROPEAN
SOCIAL FUND