

IY5601 Coursework B (2005–2006) Payment and e-commerce applications

Please complete and return this coursework at latest by Friday February 10th 2006. Please submit the coursework by email (as a pdf attachment) to `c.mitchell@rhul.ac.uk`.

1. The giro payment system is an example of a ‘push’ system.
 - (a) Describe the main security threats arising to a giro payment system, putting your answers in the context of the payment model presented in the course notes.
 - (b) What countermeasures commonly exist to address some of these security threats?
2. Popular PC web browsers such as Internet Explorer or Mozilla Firefox contain an implementation of SSL/TLS.
 - (a) On what basis does such an SSL/TLS implementation verify public key certificates provided by a web server?
 - (b) Describe how a ‘ciphersuite rollback attack’ works.
 - (c) Describe a known weakness in SSL version 2.0, and indicate how a malicious entity might take advantage of this to attack a user PC, even if the web browser on the target PC supports SSL version 3.0 and TLS.
3. Describe in detail how a ‘wedge attack’ (as mentioned in the course notes) might be used to allow the holder of a stolen DDA-capable EMV card to defeat the PIN verification process.
4. The 3-D Secure scheme employs SSL protection for key communications links, and also uses a digital signature to protect the PAREs message.
 - (a) List which entities in the 3-D Secure system need to hold public key certificates, and indicate what they are used for.
 - (b) Which of these certificates must be produced by a ‘public’ CA, i.e. not a payment system specific CA (assuming that the browser on the cardholder PC is not equipped with any ‘special’ root public keys)?