

IY5601 Coursework B (2005–2006)

Payment and e-commerce applications

Worked solutions

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?*

Answer

- (a) As described in the course notes, the main information flows in a push system are: transfer of payment instrument from seller to buyer, submission of the instrument by the buyer to the buyer bank, and clearing and settlement of the instrument between the buyer and seller banks.

Attacks will typically occur either on an entity holding stored data, or on the transfer of data (as part of a data flow). Hence attacks on a single push system transaction can occur at the following places:

- *Integrity of the instrument whilst being created and stored at the seller.* This could include modification of a legitimate instrument, or the introduction of a false instrument, e.g. by corrupt staff, or through an external attack on a seller database.
- *Integrity of the instrument whilst in transit between seller and buyer.* An active attacker on the communications link might manipulate, delete or duplicate genuine instruments, or may insert entirely spurious instruments.
- *Integrity of the instrument whilst stored at the buyer.* Identical threats to those arising at the seller apply.
- *Integrity of the instrument whilst in transit from the buyer to the buyer bank.* Identical threats to those arising to the communications link between buyer and seller apply.
- *Integrity of the instrument whilst being stored at the buyer bank.* Identical threats to those arising at the seller apply.

- *Integrity of the instrument whilst being cleared.* Identical threats to those arising to the communications link between buyer and seller apply.

Note that the above list has focussed on integrity and authenticity issues. However, there are also corresponding confidentiality threats, although these are generally regarded as being less serious (although nevertheless not unimportant).

- (b) The main countermeasures are as follows.
- The measures usually employed to protect data stored at an end entity include: access control, use of secure operating systems, use of secure subsystems (e.g. HSMs), physical protection, use of network protection devices (e.g. firewalls), user authentication, etc.
 - The measures usually employed to protect data in transit between two endpoints include: data encryption and data integrity measures (MACs or signatures).

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.*

Answer

- (a) Every web browser is equipped with a set of ‘root’ public keys. These are normally shipped as part of the browser source files. These root public keys are used to verify certificates sent by web servers — this enables the web browser to obtain a trusted copy of the web server’s public key. Of course, if the root public key store is corrupted (e.g. by a virus or other malicious code) then a third party may be able to successfully masquerade as a legitimate server.
- (b) This attack is described in section 4.2 of the paper: D. Wagner and B. Schneier, ‘Analysis of the SSL 3.0 protocol’.

In: *Proceedings of the 2nd USENIX Workshop on Electronic Commerce, November 1996*. Available at:
<http://www.cs.berkeley.edu/~daw/papers/>.

- (c) As described in the Wagner-Schneier paper referenced above, SSL v2.0 contains a weakness which allows the ciphersuite rollback attack to work. SSL v2.0 also uses an insecure MAC.

A server-client pair both supporting SSL version 3.0, but which both permit use of version 2.0, can be forced to use version 2.0 by a ‘version rollback’ attack. This is described in section 4.6 of the Wagner-Schneier paper.

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.*

Answer Suppose a criminal has a stolen DDA-capable EMV card. The criminal obtains a device which has two interfaces, namely a card reader and a smart card interface. This could be implemented as a ‘sleeve’ which is placed over the legitimate card, where the card reader interface is inside the sleeve (talking to the stolen card), and the card interface is on the outside of the sleeve, and is used for communication with a merchant card reader. This sleeve device is assumed to be capable of acting as a communications channel between its two interfaces, and which is also capable of selectively modifying messages.

The criminal now uses the card and the ‘sleeve’ when wishing to make a purchase from a merchant using the stolen card. The criminal, instead of inserting the stolen card directly into the merchant card reader, instead inserts the sleeve into the card reader (where the sleeve itself has the stolen card inside it). We assume that this attack takes place in an environment where the merchant cannot (or chooses not to) see the card insertion process.

When the terminal requests the cardholder to enter a PIN, the criminal inserts a random 4-digit combination. This is encrypted and sent to the card. However, the message is prevented from reaching the card by the sleeve device. The sleeve device instead simply sends a response to the merchant terminal (falsely) indicating that the PIN has verified correctly. The terminal now proceeds with the transaction, believing the cardholder to have been authenticated correctly.

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)?

Answer

- (a) The following entities need to hold public key certificates:
 - The merchant web server must have a certificate to be used to set up an SSL connection with the cardholder PC web browser.
 - The issuer ACS must have a certificate to be used to set up an SSL connection with the cardholder PC web browser. The AC must also have a certificate to be used to set up an SSL connection with the brand directory server.
 - The MPI must have a certificate to be used to set up an SSL connection with the brand directory server.
 - The brand directory server must have a certificate to be used to set up an SSL connection with the MPI. The directory server must also have a certificate to be used to set up an SSL connection with the issuer ACS.
- (b) The certificates used by the merchant web server and by the issuer ACS (when communicating with the cardholder web browser) must be signed by a ‘public’ CA.