Applied Cryptography, COMPGA12, 2009-10

Answer ALL questions. 2 hours.

Marks for each part of each question are indicated in square brackets

Calculators are NOT permitted

1. Multiple Choice Questions. For each question, out of four answers (a), (b), (c), (d), indicate which one is **incorrect**. In each question exactly 3 answers are correct and exactly one is incorrect.

1. Challenge-response authentication systems are dynamic, and secure against simple replay attacks. However, they are not secure against relay attacks, in which the whole communication between the authentic card and the genuine reader is relayed by the attacker, who tricks the reader into believing that the smart card chip is in the proximity of the reader. One can remark that:

   (a) Relay attacks are also at least equally possible, with traditional smart cards with electrical contacts (wired connection).

   (b) Communications of an electronic passport cannot be relayed over large distances, because the internal battery in the passport chip does not have enough power.

   (c) A method to protect an electronic passport's chip against being used without owner's consent and knowledge through a relay of communications, is to shield it electromagnetically (for example keep it in a closed metallic box, or in special wallet with aluminium foil embedded in the cover).

   (d) Another defence against relay attacks is to respond to queries very quickly and measure the time very precisely, given the fact that electromagnetic waves cannot travel faster than the speed of light.

[5 marks]

2. A smart card authenticates to the server in the following way: the server sends a 4 digit random number (a challenge), and the smart card responds to this challenge with a certain cryptogram (response) that depends on the random challenge. This type of dynamic authentication is called "challenge-response". It is in principle secure against replay attacks, where the same cryptogram is replayed by the attacker at a later occasion. We can observe that:

   (a) The security breaks apart, if the server's random number generator can be reset to its previous state or repeat some of the random numbers.

   (b) This is also a "mutual authentication system", which authenticates both the card to the server, and the server to the card.

   (c) In this system, the challenge should not be very short (like 1 digit), otherwise the system is insecure.

   (d) To compute this cryptogram, we can use for example a MAC or a digital signature scheme.

[5 marks]

3. A SIM card found inside GSM mobile phones implements a challenge-response mechanism based on the key shared between the SIM card and the mobile phone operator. Best practice is to authenticate each individual phone call. The challenge should be different in each phone call and the smart card computes a suitable response cryptogram.

   (a) This cryptogram guarantees that the voice communication will be encrypted.

   (b) This is a dynamic authentication method, allows to prove that the right SIM card is present and alive.

   (c) The mobile phone and the base station (that can be in a different country) are just intermediaries in this process. They are not able to compromise the security of cryptographic keys stored in the SIM card.

   (d) If we insert our SIM card into our friend's phone and make a phone call, it is the owner of the SIM card that pays for the communication.

   [5 marks]

4. A Pseudo-Random Number Generator (PRNG) is such that:

   (a) it is a deterministic algorithm, redoing it gives the same result

   (b) it is a probabilistic algorithm, the outcome is truly random,

   (c) it expands a short string of bits (seed) into a very long sequence of bits

   (d) the sequence of output bits should be indistinguishable from a source of really random, uniformly distributed and independent bits.

   [5 marks]

5. When we “touch-in” or “touch-out” with the London Oyster card, some sort of authentication takes place before the reader is allowed to either read or write the data stored on the card.

   (a) The card first sends a password to authenticate the card to the reader, then the reader modifies an encrypted counter stored on the card. This password is a secret, different for each Oyster card.

   (b) When we use a London Oyster card, the terminal is cryptographically authenticated first, the card is authenticated second. Only in presence of a genuine reader, the card activates crypto functionalities that allow to prove it is genuine. The intention is to make it harder for hackers to attack a card that is in their possession, and makes the business of hacking the card harder and riskier for criminals. This is because they need to gain access to at least one legitimate reader, and it is usually available only at certain times, and at locations that can be closely monitored by CCTV and where all invalid authentication attempts will be recorded by the system.

   (c) The data within the card, such as our remaining credit, is encrypted during the transmissions between the card and the reader.

   (d) Every valid and functional Oyster card contains blocks of memory that cannot be modified, not even by the Transport for London chief system security officer.

[5 marks]

[Total 25 marks]

2. Precise Questions to Answer. Brief answers will be appreciated.

1. Give a definition of a side-channel attack, does it break the cryptography, or is it about something else? Make your definition as general as possible.

   [5 marks]

2. Explain what is an SPA attack and some simple method to protect against it.

   [5 marks]

3. Explain how a DPA attack works.

   [5 marks]

4. Describe at least one defence method against DPA.

   [5 marks]

5. Why we would never use RSA to encrypt long messages? Explain the concepts of hybrid encryption, and the principles of data and key encapsulation.

   [5 marks]

6. Explain (in simple words) the concept of an Advanced Electronic Signature that exists in EU directives and is translated in the law of many countries. What are the main two broad and general security requirements that a 'good' electronic signature should satisfy?

   [5 marks]

7. Explain what data the MRZ (Machine Readable Zone) in an electronic passport contains. Why or how does it through the BAC (Basic Access Control) prevent a person sitting next to you in the London underground, from extracting your biometric data from the passport (i.e. from reading your RFID chip)?

   [5 marks]

8. Explain the most basic technique that is used by electronic passport to authenticate the data inside the passport. What is the name of the similar technique used in bank cards?

   [5 marks]

9. Which data groups in electronic passports are considered as very sensitive, so that a normal border checkpoint is NOT authorized to read them, but only an authorized "inspection system" that must be explicitly authorized by the issuing country?

[5 marks]

10. Explain how a smart card can protect PGP electronic email on a PC running Windows against malware.

[5 marks]

[Total 50 marks]

3. Open Questions. In these questions the student has a substantial degree of freedom when answering. Students can use examples from their favorite industry; or focus on some particular technology; or expand on the question from a purely technical, theoretic or cryptographic perspective. Any mix of what could potentially be done, vs. current commercial technology is allowed.

1. Security Notion / Definition is a triple of 1.) Adversarial Goal, 2.) Resources of the Adversary, 3.) Access / Attack. Give two examples: one example from the IT industry or cryptography, and another one from the 'old economy' (airport, car industry, shoplifting, old-fashioned banking etc).

   [5 marks]

2. Give **two** examples of techniques, methods or other things that may prevent a criminal from making a credit card, a bank note, an ID card, a building pass, or an electronic passport that looks like a real one (to another human).

   [5 marks]

3. Give **four** examples of techniques, methods or other things that may prevent a criminal from extracting the PIN from a SIM card, or a bank card (we assume that the PIN is stored inside).

   [5 marks]

4. Give **four** examples of techniques, methods or other things that may prevent a criminal from learning the PIN or the password, when using a 2-factor authentication, in access control, payment or in a PC logon system.

   [5 marks]

5. Give **four** examples of techniques, methods or other things that allow to or help to authenticate **individual** payment transactions. This means doing more than entity authentication (entity can be a user, his card/token, his PC etc), and more than static data authentication. You should specifically focus on the problem whether transaction can be modified, or replayed by a dishonest store or employee that wants simply to charge you more money than the agreed price, or repeat the transaction. You may consider all sorts of attacks: man-in-the-middle, social engineering, chip cloning, etc. The response can but does not have to refer to the current Chip and PIN technology. Alternatively, the question can be answered in a broader context of payment technology and/or electronic commerce with any combination of hardware devices, cryptographic protocols, data and entity authentication.

[5 marks]

[Total 25 marks]

END OF PAPER