Security

Assignment 1, Monday, September 12, 2011

Handing in your answers: There are two options:

1. Put your solutions in Pim's post box (in the white cabinet, lower door, near the printer at the station-side-end of the corridor on the second floor of the Huygens building). Before handing in, make sure:
   - your name and student number are written on the document.
2. Send your solutions by e-mail to `pim@cs.ru.nl` with subject '*assignment 1*'. This e-mail should only contain a single PDF document as attachment. Before handing in, make sure:
   - your name and student number are included in the documen (since they will be printed),
   - your name is part of the filename (for example PimVullers_assignment-1.pdf), and
   - the file is a PDF document.

Deadline: Monday, September 19, 12:00 (noon) sharp!

Note: These tasks require that you study Ross Anderson's chapter on Usability and Psychology[1] as well as the material on substitution[2], Vigenère[3], and one-time pad[4] ciphers.

1. **(2 points)** After reading Ross Anderson's chapter on Usability and Psychology, answer the following questions.
   (a) Describe in a few lines, *in your own words*, what identity fraud is. [Note: we also read Wikipedia.]
   (b) Consider the following case of identity fraud.

   > Alice opens an on-line bank account using her colleague's name 'Bob'. To do this the bank requires a copy of his identity document and a bank transfer from a bank account he owns. She gets the copy by pretending to help him when he has trouble making a copy of his passport. What Bob did not know is that she actually made two copies, one for Bob, and one for herself. Furthermore she contacts Bob for some help with her on-line banking, and asks him to transfer a small amount of money to her account to test if all is OK, and pays him back the amount in cash.
   > Using this account she now performs fraudulent transactions (selling goods without delivering them, acquiring credit cards) which lead to a bad seller reputation for Bob on the internet as well as collection agencies demanding money from Bob.

   For this case, identify:
   - the assets
   - the threat
   - the protection that was broken
   - what could be done/improved to counter the threat.
2. **(3 points)** Answer these multiple choice questions about security goals and briefly indicate why your choice is valid (or why other choices are less valid). The length of your explanation should be shorter than the length of the question.

[1] `http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c02.pdf`
[2] `http://en.wikipedia.org/wiki/Substitution_cipher`
[3] `http://en.wikipedia.org/wiki/Vigenere_cipher`
[4] `http://en.wikipedia.org/wiki/One-time_pad`

(a) A student has to give up his room because he makes too much noise during the night. Upset the student goes to the house owner and shouts that this is illegal and against the law. On which the house owner silently shows him the contract that clearly states that whenever a renter causes trouble during the night he can be kicked out of his apartment. The student sadly admits that he signed this contract half a year ago. Which security goal is crucial?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

(b) A police officer orders a donut in a highway restaurant. In the meantime, he is not aware that there is an emergency call on the radio in his car. Which security goal is compromised?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

(c) The A5/1 encryption cipher[5], which is used in GSM, is constantly under attack. Recently the tables (which contain the pre-computations) and tools to break cipher texts have been released. Which security goal of the GSM system is compromised when A5/1 is broken?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

(d) An on-line shop runs a website where customers can place orders. When the payment is received the shop guarantees delivery within three working days. At some point the sales manager notices that some orders in the database are registered as being paid but he can not find any linked payment information. After some investigation the system administrator finds out that the access rights of customers are too high and some smart customers managed to change their order status. Which security goal is compromised?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

(e) In 2008 the police started a pilot on the highways A28 and A50 near Zwolle where every passing vehicle was identified by its license plate using ANPR (Automatic Number Plate Recognition). This information is stored in a database for three days. In 2009,

[5]See `http://en.wikipedia.org/wiki/A5/1`

the police started ANPR projects on five locations in the Netherlands[6]. At some places the data is even kept up to four months. The main motivation for ANPR is to make crime investigation easier. What is the goal of this system?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

(f) In 2007 researchers of the University of Cambridge published a relay attack on EMV banking cards[7]. They showed that it is possible to relay genuine payment information, from a rogue terminal in one shop, to a card that is used for a malicious payment, at another shop. In effect an innocent customer will pay for the products the attacker buys at the other shop. Which security goal of the EMV system is compromised?

i. authenticity
ii. availability
iii. confidentiality
iv. identification
v. integrity
vi. non-repudiation

3. **(1,5 points)** Break the mono-alphabetic substitution cipher (which is just a permutation of letters) used to generate the following cipher text. The plain text is written in English.

> 'C pxcad sulinpjq ycqnojo oxunbf sunap go bckj. C pxcad cp ogto ouljpxcah gzunp xnlga agpnqj pxgp pxj uabt kuql uk bckj wj xgyj sqjgpjf ou kgq co inqjbt fjopqnspcyj. Wj'yj sqjgpjf bckj ca unq uwa clghj. Opjixja Xgwdcah'

Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

4. **(1,5 points)** Decrypt the following Vigenère cipher text using the key 'vigenere'.

> 'kixeasze da uye tisamywvse'

Explain briefly how you did it. [Note: 'I used a computer' is not accepted as an explanation.]

5. **(2 points)** Consider the flawed implementation of a 'one-time' pad which repeats after a certain number of bits. This is obviously vulnerable to a known plain-text attack. Decrypt the following cipher text that was encrypted with this flawed 'one-time' pad. The characters are translated to 7-bit ASCII binary representation[8]. XOR is the bitwise eXclusive OR operation. [Note: the repetition can start at any point in the bit-stream.]

ASCII	D	o	n	o	t		u	s	e	...	...	...	...		...	...
plain	1000100	1101111	0100000	1101110	1101111	...	...	...	...	...	...	...	...	...	...	...
pad	0111001	0101011	...	...	...	...	...	...	...	...	...	...	...	...	...	...
XOR	1111101	1000100	1000000	0101101	1010110	1000011	0110101	...	...	...	...	...	...	0011011	...	...
ASCII	}	D	@	-	V	C	5	N	&	Y	(	C	a	ESC	4	_

[6]See http://tinyurl.com/lv5h3e
[7]See http://www.cl.cam.ac.uk/research/security/banking/relay/
[8]http://en.wikipedia.org/wiki/ASCII