Open Book Examination **UNIVERSITEIT TWENTE.**
Introduction to Information Security 201100072
April 16, 2014

Answer 6 out of 8 questions. Each question is worth 15%.
Illegible answers or excessively long answers will not be marked.

1 Encryption

The following crypto systems have a homomorphic property. Formulate and prove the property

(a) If the RSA public key is modulus *m* and exponent *e*, then the encryption of a message *x* is given by $\mathcal{E}(x) = x^e \bmod m$.

(b) In the Benaloh cryptosystem, if the public key is the modulus *m* and the base *g* with a blocksize of *c*, then the encryption of a message *x* is $\mathcal{E}(x) = g^x r^c \bmod m$, for some random $r \in \{0, \ldots, m-1\}$.

(c) In the Paillier cryptosystem, if the public key is the modulus *m* and the base *g*, then the encryption of a message *x* is $\mathcal{E}(x) = g^x r^m \bmod m^2$, for some random $r \in \{0, \ldots, m-1\}$.

2 Biometrics

a) We have a system with a high FAR and a system with a high FRR. One system is going to be used on the launch button for nuclear missiles and the other to log in on your laptop. Explain what system you would use where and why?
b) Which of the three measures FAR, FRR, or EER is best to compare the accuracy of a biometric system and why?

3 Access control

A University uses smart cards for access control to buildings. A unique number is stored on each card, which is looked up in a data base when an employee wishes to enter or leave the building.

a) Explain the main weakness of this system, give an attack that exploits this weakness, and indicate how likely it is that this weakness can be exploited.
b) To prevent the attack, the University decides to keep the cards and the authentication system in place but use a unique number that is regularly renewed, instead of the fixed number. Does this solve the problem? Is it now harder for the attackers or easier?
c) How would you prevent the attack?

4 General

Answer the following questions by stating yes or no and your reason in at most one line per item. A correct answer gives 1.5 marks, an incorrect answer will be penalized by subtracting 1.5 marks.

(a) The most frequently used electronic payment method on the Internet is transferring credit card information over a secured connection.
(b) Code obfuscation provides perfect protection of mobile agents against hostile hosts.
(c) DES encryption is distributive, i.e. for all x, y: $E(x) + E(y) = E(x+y)$.
(d) Using the same public/private key pair for signing and encryption is a bad idea.
(e) UNIX does not provide access control.
(f) True random numbers cannot be generated by software alone.
(g) Buffer overflow is the most common cause of security problems.
(h) Open source software is inherently more secure than closed source software.
(i) Carrying out intrusions requires huge technological skills on the part of the perpetrator.
(j) Cyber security is just a new term for what used to be called information security.

5 The Dark Side

The following question is related to the Tor Network and the Tor paper. Please refer to section 7 of the paper when explaining your answers.

Every sub-question describes a potential adversary of the Tor Network. Given the situation, resources and goal described, select the most viable and effective attack for the adversary from the following list,:

i. Run or compromise a substantial array of Nodes and mount a denial of service attack on non-observed Nodes
ii. Run a few end nodes and apply man-in-the-middle attacks on all connections going through the controlled nodes
iii. Destroy or block all directory servers
iv. Apply end-to-end timing and size correlation on the controlled part of the network
v. Apply the iterated compromise attack as described in the paper.

Select only one attack (attacks can be chosen multiple times) from the list above and explain and explain your choice!

a) After learning that a civilian rebellion uses Tor to communicate, a government wants to shut down all access to the Tor Network. It has power over all internet service providers in the country.
b) A security agency with virtually unlimited resources and barely any legal limitations wants to covertly scour the entire network for potential threats to public safety.
c) A malicious hacker wants to gather sensitive information for blackmailing purposes, with no specific target in mind.
d) A law enforcement agency wants to identify a malicious user on the tor network who they know operates within their jurisdiction.

6 Passwords

Academic research into the usability and effectiveness of passwords has a number of problems.

a) Mention at least 5 problems related to the getting access to passwords
b) Some aspects like the usability of passwords are difficult to quantify. Mention at least one other aspects that is difficult to quantify.
c) How did Mazurek et al solve the problem of getting access to passwords?
d) Give at least one argument in favour and one argument against the approach of Mazurek et al.
e) Which methods used Inglesant et al to get hold of passwords?
f) Which problems have Inglesant et al been unable to solve?
g) If you had to choose for your research between a collection of passwords created specifically for your research and a password collection that has leaked out of an existing system, which would you choose? Why?

7 Bitcoins

a) The transparency of the Bitcoin network causes privacy issues. Explain the most important privacy issue Bitcoin has in comparison with paper money.
b) Several services exist that are used to counter these privacy issues. What are these services called? Explain how they provide anonymity.
c) Which weakness of the Bitcoin system was partly responsible for the downfall of the Mt Gox Bitcoin exchange?

8 Key Escrow

a) What is the essence of a key-escrow system? (max. 1 sentence)
b) Name two disadvantageous side-effects of a key-escrowed encryption compared to a 'normal' encryption when looking at the level of security.
c) Either name a successful deployment of key-escrow, or explain why key-escrow systems are not widely used.