**Open Book Examination** **UNIVERSITEIT TWENTE.**

**Introduction to Computer Security 201100072**

**January 24 2013**

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

(1) El Gamal

| | |
|---|---|
| Multiplicative group | $Z_n^*=\{1...n-1\}$ |
| Prime: | n |
| Generator: | g |
| Private key: | $x \in Z_n^*$ |
| Public key: | $h = g^x$ |
| Salt: | $y \in_R Z_n^*$ |
| Enc(m,h): | $(c,d) = (mh^y, g^y)$ |
| Dec((c,d),x): | $c/d^x$ |

a) Prove that El Gamal is correct.
b) In the El Gamal algorithm the x and y are chosen from $Z_n^*$. What goes wrong if x and y are chosen from $Z_n$?

(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) What is better: a system with a low FAR, a low FRR, or a low EER? 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, and 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

Consider the three standard security objectives: confidentiality, integrity, and availability. For each of these objectives it is possible to have hardware and software solutions. For the following scenarios find the correct objective and if it is a hardware or software solution and explain why.

a) Your mother copies all the family photos to a rewritable DVD and gives it to you to keep them at your place, in case your parents' house burns down.
b) In a big child pornography case the police admitted that even though they had decrypted a lot of evidence they could not guarantee that they had decrypted all the evidence because the suspect had used TrueCrypt.
c) After copying files to a hard drive you turn off your computer, remove the hard drive and mail it to a friend for safe keeping
d) Your brother likes to Photoshop crazy things into your vacation photos. You want to keep the original images in case your brother edits them, so you burn all the photos to a writable DVD before he can get his hands on them.
e) There is a nice trick which makes it possible to use a jpeg as a zip file making it possible to store files in the jpeg without damaging the jpeg.

(5) Advanced Persistent Threat

a) Describe what an APT is and how it differs from "regular" hacking scenarios.
b) What are the different phases in targeted attacks? Describe each in your own words what is the purpose of each phase.
c) Describe in your own words what pivoting is and why you would use it.

(6) Offensive Security

a) What is a canary and how you could circumvent it's effect?

Consider the C program fragment below:

```
void foo () {
   // One
   char a [] = "first";
   char b [] = "challenge";
   char c [] = "my";
   char d [] = "formatting";
   char e [] = "string";

   printf(XXX-ONE, a, b, c, d, e);

   // Two
   int my_value;

   printf(XXX-TWO, &my_value);
```

```
    printf("my_value = %d\n", my_value);
}
```

b) How would you define the format string XXX-ONE so that the first line of output would be: "my first string formatting challenge"?
c) How would you define the format string XXX-TWO, such that after execution, the value of the variable my_value = 1337?
d) Explain the principle of return-oriented programming and give the main advantage for a hacker to use this technique.

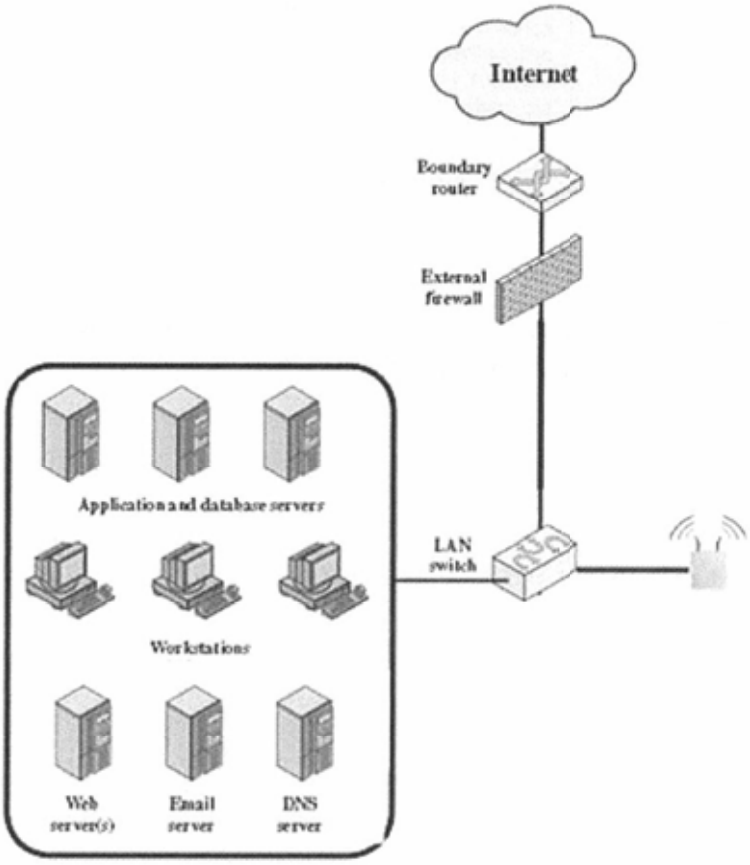


Figure 1. Network Architecture

(7) Network Security

a) Given the network architecture of figure 1, name at least three architectural network improvements concerning the network security. Argue why you made the changes. Draw the new architecture.
b) Which cryptographic algorithm does TKIP use to ensure data confidentiality? Which message digest algorithm does it use to ensure integrity?
c) The TKIP digest algorithm that provides message integrity makes use of a 64 bit key why is the key used in the algorithm?
d) See the two network messages in figure 2 and 3. IDS, IPSs, firewalls and even the targeted host itself will almost without exception fail to identify and report a pattern

of malicious activity. Explain when this behavior of the hacker occurs and which correlation rule in SIEM can help to detect it

e) What would be a limitation of the rule created? Thus how could the hacker cover his tracks?

*Internal Network: 10.1.1.xxx [block D]*

| | |
|---|---|
| ns5xt: NetScreen device_id=ns5xt system-notification-00257(traffic): start_time="2005-09-15 09:41:44" duration=5 policy_id=0 service=tcp/port: proto=6 src zone=Trust dst zone=Untrust action=Permit sent=1034 rcvd=19829 src=206.3.3.2 dst=10.1.1.167 src_port=1059 dst_port=23 translated ip=10.1.1.162 port=23 | ns5xt: NetScreen device_id=ns5xt system-notification-00257(traffic): start_time="2005-09-15 09:41:44" duration=5 policy_id=0 service=tcp/port:1214 proto=6 src zone=Trust dst zone=Untrust action=Permit sent=1034 rcvd=19829 src=10.1.1.167 dst=206.3.3.2 src_port=1059 dst_port=22 translated ip=10.1.1.162 port=22 |
| *Figure 2. Message 1 (port 23 is telnet)* | *Figure 3. Message 2 (port 22 is SSH)* |

(8) Indicate for each of the three phishing emails below at which line each of the 6 key principles of influence by Robert Cialdini is used and explain briefly why.

a) Phishing mail 1: Targeted PDF

```
1  Dear Eve,
2
3  As the head chairman of the University of Eden, I can tell you
4  that your husband Professor Adam was nominated for the best
5  teacher of the year 2012 award.
6  You and you husband are hereby invited to a dinner party where
7  the price will be handed out, which all the nominees will
8  attend. We have contacted you instead of your husband because
9  we would like to keep this a surprise and we would appreciate
10 it if you would keep it that way.
11 In the attached pdf file you will find all the details you need
12 to attend the event.
13
14 Kind regards
```

b) Phishing mail 2: Citibank

```
1  Dear Citibank Customer,
2
3  Security Alerts:
4
5  All Citibank accounts access for online use are required to
6  confirm their personal information due to high volume of fraud
7  and unauthorize access from outside US Territories.
8  For your protection your account is temporarly limited. An
9  account that is temporarly limited is required to confirm the
10 Account Information.
11 To successfully confirm your information we require your
12 Citibank® Banking Card and Personal Identification Number (PIN)
13 so you can access your accounts at ATMs and online. Here's how
14 to confirm your account information online:
```

Go to Citibank Online page and complete the Card Verification form.

Agree to site Terms & Conditions and confirm your personal information.

You'll be successfully confirmed and your Citibank® Account is Verified.

You may also want to view the Disclosures and Agreement that you agreed to when you applied, which you can do for the next 90 days at Citibank Online.

Again, thank you for choosing Citibank.

c) Phishing mail 3: 419 fraud

PROJECT MANAGER
NIGERIA NATIONAL PETROLEUM CORPORATION
FOLOMO -COMPLEX LAGOS NIGERIA
ATTN SIR/MADAM

I am the project manager with the Nigeria National petroleum Corporation (NNPC). I know you will be surprised to receive this kind of letter seeking for your assistance. To be candid, I got your e-mail address through a close relation of mine who is now with the Nigeria Chamber of Commerce (NCC), though I did not disclose to him what I will use it for.

Now the business in question is the transfer of US$ 25.5m. This sum came as a purposely over invoiced sum, which I as the project manager masterminded. The foreign contractors dully received their total contract amount leaving this over invoiced sum of USD$ 25.5m floating in the union bank Nigerian PLC, to be transferred to a foreign bank account. The Civil rule of conduct does not warrant us to operate an offshore account. That is the reason why we are strongly seeking for your assistance in proving your bank information where we can transfer the funds. Please, you are very important in this transaction as every document covering the transfer of this fund will be in your name.

So all we need now is your banking information and ability to keep it secret based on the nature of it all. We have mapped out 30% of US$25.5m to be for you the account owner, 60% for us while 10% is mapped out for any process of expenses to be incurred on the process of this transfer. On receipt of your bank information within 14 working days, this fund will be in your nominated account.

I will be very grateful to receive this information from you, and also pleased that you should not betray the trust I imposed in you.