ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Family Name: .....

First Name: .....

Section: .....

Cryptography and Security Course

(Security Part)

Final Exam

March 2nd, 2006

This document consists of 14 pages.

Instructions

Electronic devices are *not* allowed.

Answers must be written on the exercises sheet.

This exam contains 4 *independent* exercises.

Answers can be either in French or English.

Questions of any kind will certainly *not* be answered. Potential errors in these sheets are part of the exam.

You have to put your full name on *each* page and you have to do it *now*.

IPSec with NAT

In some cases, IPSec cannot work correctly if NAT (Network Address Translation) is used.

1. Tick the IPSec configuration(s) below which is(are) **not** compatible with NAT:

   ☐ IPSEC/AH in Transport Mode
   ☐ IPSEC/ESP (Null encryption, with authentication) in Tunnel Mode
   ☐ IPSEC/AH in Tunnel Mode
   ☐ IPSEC/ESP (3DES encryption, no authentication) in Tunnel Mode

2. For each configuration above which is **not** compatible with NAT, draw a complete frame, highlight the problematic part and explain exactly why the configuration cannot work with NAT.

3. In configuration(s) which should work with NAT, it is sometimes necessary to encapsulate the complete frame in an UDP packet: explain why. Give details.

Organisational Security

You are hired as CSO (Chief Security Officer) in a Swiss bank. Your boss asks you:

1. Give me two arguments to justify why the security gap is increasing if no new measures are taken.

2. Give me two measures other than regular audits that could raise the real security level.

3. You notice that your Boss is the CTO (Chief Technical Officer, i.e. Supervisor) for all the IT (Information Technology i.e. computer) department of the company. Give two scenarios where this situation could be problematic.

Symmetric and Asymmetric Ciphers

1. You want to send a confidential message to a friend with GPG. You already have his public key: it is a 1024-bit RSA key. How exactly is the message encrypted with PGP/GPG? With what kind of algorithms? Give details:

2. You find on e-bay a quantum computer, able to factorize numbers of 2048 bits in six weeks, and a classical computer able to crack any symmetric cipher in less than one week. Assume that you want to attack a banking application running over HTTPS. For each computer describe an attack that it allows to carry out against the banking application. Which computer would be more useful? Explain why:

The *BreakRSA* Company

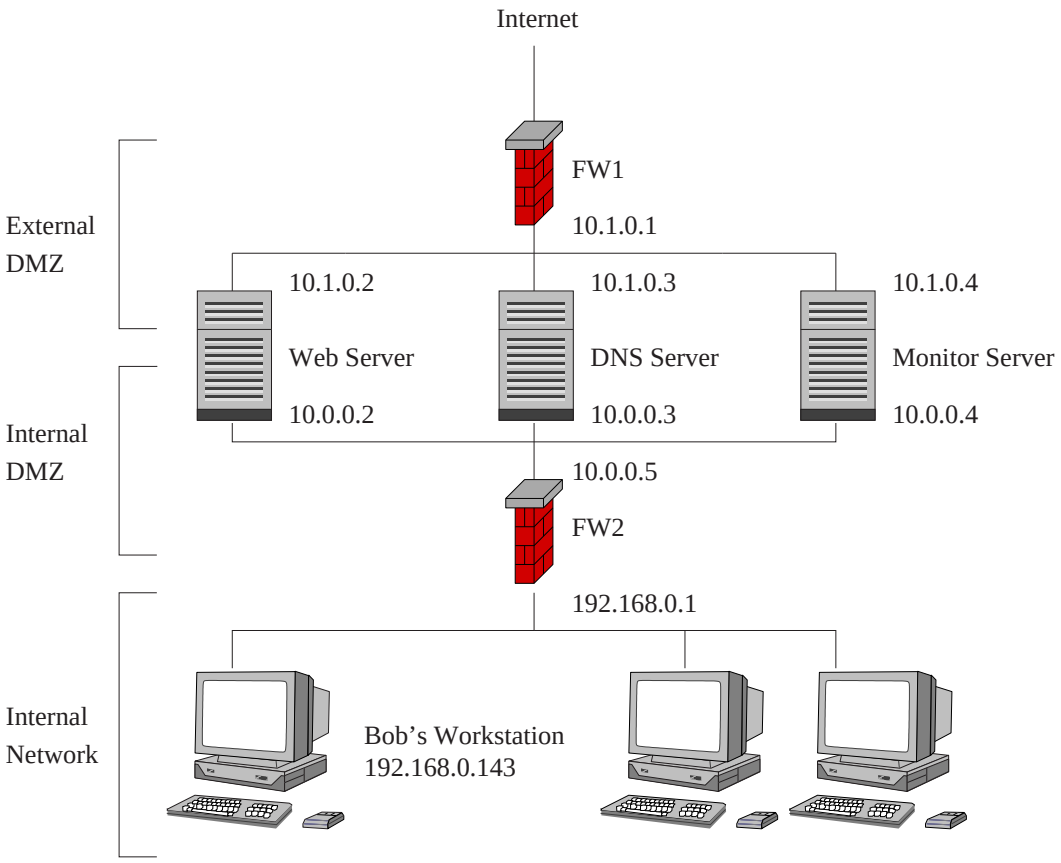

Figure 1: Map of the BreakRSA's Network

A new security challenge has been proposed on the Internet by the computer security company *BreakRSA*. In order to win the price (100'000 $) participants must find the private key from a 1024-bit RSA public key. Because the price is quite important, the company wants to be sure that nobody can penetrate their computer network and steal the private key. Because you are one of the best security expert in the world, they hired your services and challenged you to steal the private key.

First of all, participants must be identified on the web server of the company by creating an account with a CGI script. Then, they will receive the public key by e-mail . The private key is saved on Bob's workstation – Bob is in charge of this challenge. His computer is directly connected to the network of the company but it is protected by a firewall from the DMZ (see figure 1). Bob is always connected via SSH from his workstation to a server used to monitor all the DMZ: the Monitor Server. From this server, he checks the logs of the firewalls (FW1 and FW2), the DNS Server and the Web Server.

1. Give the name of the firewall configuration (see figure 1) and explain the role of the second firewall (FW2). Give an advantage and a disadvantage of using the same brand of firewall for FW1 and FW2:

Firstly, you decide to check the security of the CGI script. It is a C program called from a HTML page. The source code of the page and the program are given below:

```
<HTML>
<BODY bgcolor="#FFFFFF">
  <P align="center">
  <HR noshade>
  <TABLE align="center">
    <TR><TD align="center">
    please enter your e-mail in order to receive the public key:</TD></TR>
    </TD></TR>
    <TR><TD align="center">
        <FORM ACTION="/cgi-bin/public.cgi" METHOD=POST>
        <INPUT TYPE="text" NAME="mail"><BR>
        <INPUT TYPE=SUBMIT VALUE="Send">
        </FORM>
    </TD></TR>
  </TABLE>
  <HR noshade>
  </P>
</BODY>
</HTML>
```

```
/**** check the query string for the argument "mail" ****/
void parse_query_string(void) {
  int query_size;
  char buffer[256];
  char *data;
  char *mail;

  /* retrieve the length of the string */
  query_size=atoi(getenv("CONTENT_LENGTH"));

  /* retrieve the string which contains the parameters sent by the client */
  data = getenv("QUERY_STRING");

  /* copy the string in the local buffer */
  strcpy(buffer, data);

  /* copy the parameter given by mail */
  mail = give_mail(buffer);

  /* send an e-mail */
  execute_string("/usr/bin/mail %s < ./reply.txt", mail);

}

int main(void) {
  /* parse the query string */
  parse_query_string();

  /* exit normally */
  return 0;
}
```

2. Obviously there are at least two vulnerabilites in this C-program. Mention them below and explain how you can exploit them:

3. You chose to exploit the Stack-Based Buffer Overflow (Processor Intel/AMD 32 bits). According to the disassembled code below and the source code of the CGI script above, give the number of bytes needed in decimal, in order to completely overwrite the return address and justify why:

```
080483f4 <parse_query_string>:
push   %ebp
mov    %esp,%ebp
sub    $0x04,%esp
sub    $0x100,%esp
sub    $0x04,%esp
sub    $0x04,%esp
push   $0x8048594
call   80482e8 <getenv@plt>
add    $0x10,%esp
sub    $0xc,%esp
push   $0x80485a3
call   80482e8 <getenv@plt>
add    $0x10,%esp
mov    %eax,0xffffef4(%ebp)
sub    $0x8,%esp
pushl  0xffffef4(%ebp)
lea    0xffffef8(%ebp),%eax
push   %eax
call   8048318 <strcpy@plt>
add    $0x10,%esp ...
```

By using the Stack-Based Buffer Overflow, you can now have a complete access to the Web Server. From the Web Server, you start a *portscan* on the Internal DMZ in order to identify reachable services:

```
Starting Nmap 4.00 ( http://www.insecure.org/nmap/ ) at 2006-02-22 16:49 CET
Interesting ports on web (10.0.0.2):
(The 65536 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh
80/tcp  open  http

Interesting ports on dns (10.0.0.3):
(The 65536 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh
53/tcp  open  dns
53/udp  open  dns

Interesting ports on monitor (10.0.0.4):
(The 65536 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh

Interesting ports on fw2 (10.0.0.5):
(The 65536 ports scanned but not shown below are in state: closed)
PORT    STATE SERVICE
22/tcp  open  ssh
23/tcp  open  telnet
443/tcp open  https
```

4. Obviously some unecessary services are available. Mention which services should not have been available and justify your answer:

5. Give the name of the firewall's principle which is not respected here:

The interesting part is the telnet service proposed by the second firewall FW2. You know that Bob is monitoring this firewall from the Monitor Server (10.0.0.4). Thus he must be connected on it. You launch a *sniffer*. The network is switched, but arp spoofing tools allow you to sniff the traffic between the Monitor Server and the FW2 anyway. Luckily Bob is using telnet. You want to try to catch the login and the password sent in clear (Remember that telnet is unsafe!) but unfortunately he is already connected. You need to do something to force Bob to re-authenticate (and to send his login and his password in clear).

6. According to the situation, give a method to force Bob to re-authenticate on FW2 from the Monitor Server. Give details:

Great! Because Bob uses an unsafe service – telnet – you sniffed the login and the password. You have now access to the firewall FW2. Remember that the goal is to gain access to Bob's Workstation. Thus, you need to change the rules of the firewall.

7. According to the rules of the firewall below, cross out the line(s) you need to remove or/and add line(s) in order to have access to Bob's Workstation on every port from the Web Server only, without disturbing the current configuration:

firewall table						
zone	source	port	destination	port	protocol	action
	any	any	INTERNAL	any	any	deny
	INTERNAL	any	INTERNET	80	tcp	allow
	192.168.0.143	any	10.0.0.4	22	tcp	allow
	INTERNAL	any	10.0.0.3	53	any	allow
	INTERNAL	any	any	any	any	deny
any	any	any	any	any	any	deny, log

You can now reach Bob's Workstation but when you try to mount Bob's hard-disk, it asks for a Windows Password. The password you sniffed from the network does not work. Disappointed, you decide to try the same login/password on the Monitor Server which runs Linux... and this time it works! You obtain a full access on the server. You decide to retrieve the file `/etc/shadow` (it is a Linux/DES hash file) and launch a dictionary attack on it. In fact, there are only three accounts on this server. The table below lists the users and gives the passwords they use to log in:

```
login:  root   password:  r0xb4f
login:  bob    password:  password#&1337
login:  admin  password:  january!,1
```

8. Which account will be the easiest to crack? Explain why:

You decide to test Bob's password on Bob's Workstation and it works! Great! You can now have access to the hard-disk of Bob's Workstation! There, you see that the set of keys (public and private) has been generated with GPG. You copy the files `pubring.gpg` (the public key) and `secring.gpg` (the private key) and you send them to Bob to prove that you finished the test. But Bob just answers that you didn't win the challenge yet.

9. Is Bob correct? Why? Give details:

10. Suggest two attacks that could let you win the challenge. Give details:

Please, do not turn over this sheet

before the start signal.