(Open Book) Exam Information Security

April 21, 2008, 9:00-12:00, room 5412.0025

Good Luck!

Frank.

==========

1. What are two fundamental encryption methods used in one form or another by most encryption ciphers? Mention two ciphers illustrating these methods (make sure each cipher illustrates one method). Which method -if used by itself- is generally considered the stronger method? What is an essential principle underlying all (secure) ciphers? Who originally formulated that principle? (Note: the principle bears the name of its formulator).

2. Describe the workings of a feistel cipher. Draw a diagram illustrating the cipher and explain how a feistel cipher can be used for both encryption and decryption.

3. Explain the way the Diffie-Hellman key exchange algorithm operates. Provide a numerical example (use relatively small (e.g., < 15) numbers)

4. Consider a CRC that uses the divisor 10011. Find two `collisions' with the data 10101011; that is: find two other data values that produces the same CRC checksum as 10101011. How many 8-bit data values (not counting the provided data value) will produce the same CRC value for the provided divisor as the provided data value?

5. The following is an example of a series of packets captured from an ethernet device. What packet numbers (as indicated by their time stamps) constitude the three way TCP/IP handshake? What is the IP address of the computer initiating the connection and what computer answered the request? Assuming all communications were according to standard protocols, was the connection secure? Why? What tcpdump expressions (provide 3 expressions, one for each part of the three way handshake) can be used to select the elements of the three way handshake from a series of captured packets?

   Additional info: The packet flags are at byte offset 13, having the following bit-definitions (FIN: bit 0, CWR: bit 7)

   CWR | ECE | URG | ACK | PSH | RST | SYN | FIN

```
11:50:58.389741 vlan 810, p 6, IP 172.30.10.3.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
state=standby group=0 addr=172.30.10.1
11:50:58.469010 IP 129.125.3.253.1985 > 224.0.0.2.1985: HSRPv0-hello 20: state=standby
group=29 addr=172.29.10.1
11:50:58.912708 vlan 480, p 7, 01:00:0c:cc:cc:cd > 00:1b:54:fe:a2:16 SNAP Unnumbered,
ui, Flags [Command], length 50
11:50:58.917504 (NOV-ETHII) IPX 00108022.00:11:85:63:a2:f3.0453 >
00108022.ff:ff:ff:ff:ff:ff.0453: ipx-rip-resp 1056768/1.2
11:50:58.925581 vlan 810, p 7, 01:00:0c:cc:cc:cd > 00:1b:54:fe:a2:16 SNAP Unnumbered,
ui, Flags [Command], length 50
```

```
...:59.123774 IP 129.125.3.162.33651 > 129.125.3.10.53: 37228+ A?
...urity.rc.rug.nl. (36)
...:50:59.124944 IP 129.125.3.10.53 > 129.125.3.162.33651: 37228* 1/2/2 A 129.125.14.81
(120)
11:50:59.125688 IP 129.125.3.162.60321 > 129.125.14.81.443: S 742738323:742738323(0)
win 5840 <mss 1460,sackOK,timestamp 399960466 0,nop,wscale 5>
11:50:59.127161 IP 129.125.14.81.443 > 129.125.3.162.60321: S 2940497265:2940497265(0)
ack 742738324 win 5792 <mss 1460,sackOK,timestamp 3885041859 399960466,nop,wscale 6>
11:50:59.127192 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 1 win 183
<nop,nop,timestamp 399960467 3885041859>
11:50:59.127814 IP 129.125.3.162.60321 > 129.125.14.81.443: P 1:73(72) ack 1 win 183
<nop,nop,timestamp 399960467 3885041859>
11:50:59.128283 IP 129.125.14.81.443 > 129.125.3.162.60321: . ack 73 win 91
<nop,nop,timestamp 3885041860 399960467>
11:50:59.165748 IP 129.125.14.81.443 > 129.125.3.162.60321: . 1:1449(1448) ack 73 win
91 <nop,nop,timestamp 3885041868 399960467>
11:50:59.165789 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 1449 win 273
<nop,nop,timestamp 399960476 3885041868>
11:50:59.165911 IP 129.125.14.81.443 > 129.125.3.162.60321: . 1449:2897(1448) ack 73
win 91 <nop,nop,timestamp 3885041868 399960467>
11:50:59.165924 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 2897 win 364
<nop,nop,timestamp 399960477 3885041868>
11:50:59.168988 IP 129.125.14.81.443 > 129.125.3.162.60321: P 2897:3423(526) ack 73
win 91 <nop,nop,timestamp 3885041869 399960476>
11:50:59.169001 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 3423 win 454
<nop,nop,timestamp 399960477 3885041869>
11:50:59.352258 vlan 810, p 6, IP 172.30.10.2.1985 > 224.0.0.2.1985: HSRPv0-hello 20:
state=active group=0 addr=172.30.10.1
11:50:59.640770 IP 129.125.3.162.60321 > 129.125.14.81.443: P 73:287(214) ack 3423 win
454 <nop,nop,timestamp 399960595 3885041869>
11:50:59.664462 IP 129.125.14.81.443 > 129.125.3.162.60321: P 3423:3498(75) ack 287
win 108 <nop,nop,timestamp 3885041994 399960595>
11:50:59.664511 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 3498 win 454
<nop,nop,timestamp 399960601 3885041994>
11:50:59.665127 IP 129.125.3.162.60321 > 129.125.14.81.443: P 287:996(709) ack 3498
win 454 <nop,nop,timestamp 399960601 3885041994>
11:50:59.704818 IP 129.125.14.81.443 > 129.125.3.162.60321: . ack 996 win 130
<nop,nop,timestamp 3885042004 399960601>
11:50:59.745389 IP 129.125.14.81.443 > 129.125.3.162.60321: . 3498:4946(1448) ack 996
win 130 <nop,nop,timestamp 3885042014 399960601>
11:50:59.747688 IP 129.125.14.81.443 > 129.125.3.162.60321: . 4946:6394(1448) ack 996
win 130 <nop,nop,timestamp 3885042014 399960601>
11:50:59.747727 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 6394 win 635
<nop,nop,timestamp 399960622 3885042014>
11:50:59.747830 IP 129.125.14.81.443 > 129.125.3.162.60321: P 6394:7819(1425) ack 996
win 130 <nop,nop,timestamp 3885042014 399960601>
11:50:59.785900 IP 129.125.3.162.60321 > 129.125.14.81.443: . ack 7819 win 726
<nop,nop,timestamp 399960632 3885042014>
11:50:59.916687 00:1b:54:fe:a2:16 > 01:00:0c:cc:cc:cd SNAP Unnumbered, ui, Flags
[Command], length 50
11:51:00.159248 IP 129.125.3.252.1985 > 224.0.0.2.1985: HSRPv0-hello 20: state=active
group=29 addr=172.29.10.1
```

6. What is the `web of trust' as used by PGP/GPG? Why do SSL certificates not need a `web of trust'? Assume you receive a GPG signed message from a

rson who claims it's Alice and and SMIME signed message from a person who claims it's Bob. How do you authenticate these two e-mails?

7. Describe at least 5 different ways to reduce the chances that your computer will be compromised. What security flaw is targeted by each of these ways?

8. Describe how Stealth can be used to check the integrity of files in various (more than one) computers. What are essential characteristics (with respect to using Stealth) of the computer on which Stealth is installed?

9. You use the following mounts to access various parts of your file system:

```
/dev/hda3 on / type ext3 (rw,errors=remount-ro)
/dev/hda2 on /boot type ext3 (rw)
/dev/hda5 on /usr type ext3 (rw)
/dev/hda6 on /home type ext3 (rw)
/dev/hda7 on /var type ext3 (rw)
/dev/hda8 on /tmp type ext3 (rw,noexec,nosuid)
```

   Since this is the standard operating situation, you never use your computer without these mounts.

   One bad day a hacker gained access to your computer. She unmounted /dev/hda2 and stored a program called `workbench' that she used for her hacking actions under the /boot directory and then remounted /boot again.

   Describe how you can find `workbench' when your computer has booted normally (so you're not booting your computer from a rescue disk or comparable and all filesystems are mounted as described above).

10. What is, according to Mark Stamp, the security value of open source vs. closed source software. Who (an author still alive) is Mark quoting when he discusses the relative security merits of open vs. closed source software? What is your opinion in this matter (do not simply state `I agree' or `I disagree'. Rather, clarify why you have your opinion).