NTNU
Norges teknisk-naturvitenskapelige universitet

Fakultet for informasjonsteknologi, matematikk og elektroteknikk

Institutt for datateknikk og informasjonsvitenskap

BOKMÅL//NYNORSK/ENGLISH

AVSLUTTENDE EKSAMEN I/FINAL EXAM

TDT4237
Programvaresikkerhet/Software Security

Mandag/Monday 15.12.2008

Kl. 09.00 – 13.00

Faglig kontakt under eksamen:

Lillian Røstad, tlf. 994 00 628

Hjelpemidler (supporting materials):

D: Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.
D: No written or printed supporting materials allowed. Basic calculator allowed.

Sensurdato (date for examination results):

15. januar 2009. Resultater gjøres kjent på http://studweb.ntnu.no/ og sensurtelefon 81548014.

January 15th 2009. Results available at http://studweb.ntnu.no/ and phone 81548014.

Det er angitt i prosent hvor mye hver deloppgave teller ved sensur.

Each task is labeled with maximum obtainable score in percentage of the total score.

BOKMÅL

Oppgave 1 (30%)

a) Forklar begrepene white hat, grey hat og black hat hacker.
b) Hva er en metacharacter? Hvorfor er bruken av metacharacters relevant for programvaresikkerhet?
c) Forklar kort hvilke trinn som inngår i å utføre en risikonalayse for programvare.
d) Hva betyr *ikke-benekting* (eng.: non-repudiation) i en SOA-sammenheng?
e) Hva er *stack smashing*? Forklar kort hvordan det fungerer.
f) Hva er angrepstrær (attack trees) og hvordan og når brukes de? Illustrer med et eksempel.

Oppgave 2 – Sikkerhetskrav (25%)

Selskapet *Web Solutions* har ansatt deg som konsulent for å bidra med sikkerhetsekspertise i deres prosjekter. I det første prosjektet du skal jobbe på skal det utvikles en nettbutikk for å selge musikk. Din første oppgave er å delta i kravutviklingsfasen der du har ansvar for å ivareta sikkerhetsfokuset.

Forklar hvordan du vil gå frem for å løse denne oppgaven. Fokuser på hvilke metoder og teknikker du ville brukt og forklar hvorfor. Bruk eksempler for å illustrere fremgangsmåten din.

Oppgave 3 – Sikkerhetstesting (25%)

Du har fått i oppgave å utføre penetrasjonstesting på en webapplikasjon.

a) Forklar hva penetrasjonstesting er. Hvor passer det inn i livssyklusen for programvare? (5%)

b) Hvordan ville du utført denne oppgave? Beskriv fremgangsmåten din i detalj. Bruk eksempler for å illustrere fremgangsmåten din. (15%)

Oppgave 4 – Code Quiz – Spot the bug (20%)

I denne pseudo-Java-kodesnutten er det feil som kan forårsake sikkerhetsproblemer. Identifiser, klassifiser og beskriv feilene. Forklar også hvordan du ville ha gått frem for å endre på koden slik at samme funksjonalitet ble beholdt, men uten sårbarheter. Skriv gjerne pseudokode for å forklare.

```
byte[] buffer;

/*
* This method transmits a message made in a web form from the sender to the receiver using
* email. Befor the message is sent it is encrypted to protect the content.
*/
public void sendMessage (String from, String to, String note) {

Message msg = new Message(from,to,note);
buffer = encrypt(msg);
//Used to keep track of sent messages – important for auditing purposes
RandomAccessFile raf = new RandomAccessFile(“messagelogg.txt”, "rw");
raf.writeBytes(buffer);
sendMail(from,to,buffer);
}

public byte[] encrypt(Message msg){
RandomAccessFile raf = new RandomAccessFile(“keyfile.txt”, "rw");
byte[] key = raf.readLine();
byte[] encrypted = DESEncrypt(msg, key);
return encrypted;
}
```

NYNORSK

Oppgåve 1 (30%)

a) Gjer greie for uttrykka white hat, grey hat og black hat hacker.
b) Kva er ein metacharacter? Kvifor er bruken av metacharacters relevant for programvaresikkerheit?
c) Forklar kort kva trinn som inngår i å utføre ei risikonalayse for programvare.
d) Kva betyr *ikkje-benekting* (eng.: non-repudiation) i ein SOA-sammenheng?
e) Kva er *stack smashing*? Gjer greie for korleis det fungerer.
f) Kva er angrepstrær (attack trees) og korleis og når brukast de? Illustrer med eit eksempel.

Oppgåve 2 – Sikkerheitskrav (25%)

Selskapet *Web Solutions* har ansatt deg som konsulent for å bidra med sikkerheitsekspertise i deira prosjekter. I det første prosjektet du skal jobbe på skal det utviklast ein nettbutikk for å sele musikk. Din første oppgåve er å delta i kravutviklingsfasen der du har ansvar for å ivareta sikkerheitsfokuset.

Forklar korleis du vil gå frem for å lause denne oppgåva. Fokuser på kva metodar og teknikkar du ville brukt og forklar kvifor. Gje eksemplar for å illustrere fremgangsmåten din.

Oppgåve 3 – Sikkerheitstesting (25%)

Du har fått i oppgåve å utføre penetrasjonstesting på ein webapplikasjon.

a) Forklar kva penetrasjonstesting er. Kor passer det inn i livssyklusen for programvare? (5%)

b) Korleis ville du utført denne oppgåven? Gjer greie for fremgangsmåten din i detalj. Gje eksempla for å illustrere fremgangsmåten din. (15%)

Oppgave 4 – Code Quiz – Spot the bug (20%)

I denne pseudo-Java-kodesnutten er det feil som kan forårsaka sikkerheitsproblema. Identifiser, klassifiser og beskriv feilane. Forklar også korleis du ville ha gått frem for å endre på koden slik at same funksjonalitet vert behald, men utan sårbarhetar. Skriv gjerne pseudokode for å forklåra.

```
/*
* This method transmits a message made in a web form from the sender to the receiver using
* email. Befor the message is sent it is encrypted to protect the content.
*/
public void sendMessage (String from, String to, String note) {

Message msg = new Message(from,to,note);
buffer = encrypt(msg);
//Used to keep track of sent messages – important for auditing purposes
RandomAccessFile raf = new RandomAccessFile(“messagelogg.txt”, "rw");
raf.writeBytes(buffer);
sendMail(from,to,buffer);
}

public byte[] encrypt(Message msg){
RandomAccessFile raf = new RandomAccessFile(“keyfile.txt”, "rw");
byte[] key = raf.readLine();
byte[] encrypted = DESEncrypt(msg, key);
return encrypted;
}
```

ENGLISH

Task 1 (30%)

a) Explain the terms white hat, grey hat and black hat hacker.
b) What is a metacharacter? Why is the use of metacharacters a concern for software security?
c) Explain the steps involved in performing a risk analysis for software.
d) What does *non-repudiation* mean in the context of SOA-security?
e) What is *stack smashing*? Explain briefly how it works.
f) What are attack trees and how and when are they used? Provide an example.

Task 2 – Security requirements (25%)

The Company *Web Solutions* has hired you as a consultant to contribute security expertise on their projects. The first project you are to work on is to develop an online webshop for selling music. Your first task is to participate in the requirements engineering phase to ensure a strong focus on security.

Explain how you would approach this task. Focus on the methods and techniques you would use and explain why. Also provide examples to illustrate your approach.

Task 3 – Security testing (25%)

You have been assigned the task of performing penetration testing on a web application.

a) Explain what penetration testing is. Where does it fit in the software lifecycle? (5%)

b) How would you perform this task? Describe your approach in detail. Provide examples to illustrate your approach. (20%)

Task 4 – Code Quiz – Spot the bug (20%)

In this pseudo-Java-code excerpt there are hidden security vulnerabilities. Identify, classify and describe the vulnerabilities. Additionally, explain how you would change the code so that the functionality remains the same but without the vulnerabilities. You may use pseudo code to elaborate your answers.

```
/*
* This method transmits a message made in a web form from the sender to the receiver using
* email. Befor the message is sent it is encrypted to protect the content.
*/
public void sendMessage (String from, String to, String note) {

Message msg = new Message(from,to,note);
buffer = encrypt(msg);
//Used to keep track of sent messages – important for auditing purposes
RandomAccessFile raf = new RandomAccessFile(“messagelogg.txt”, "rw");
raf.writeBytes(buffer);
sendMail(from,to,buffer);
}

public byte[] encrypt(Message msg){
RandomAccessFile raf = new RandomAccessFile(“keyfile.txt”, "rw");
byte[] key = raf.readLine();
byte[] encrypted = DESEncrypt(msg, key);
return encrypted;
}
```