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

Torsdag/Thursday 14.12.2006

Kl. 09.00 – 13.00

Faglig kontakt under eksamen:

Gunnar René Øie, tlf. 976 04 652

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 2007. Resultater gjøres kjent på http://studweb.ntnu.no/ og sensurtelefon 81548014.

January 15th 2007. 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 (10%) – Multiple Choice

Velg det svaret du mener er mest korrekt. Rett svar gir 2 poeng – feil eller inget svar gir 0 poeng.
Før det inn i besvarelsen din slik som dette: 1a, 2b, 3c,…

1. Programvaresikkerhet handler om…
   a) Å lage sikker programvare.
   b) Å lage programvare som kan motstå angrep.
   c) Å lage feilfri kode.
2. Hvorfor opererer man ofte med fete klienter i webapplikasjoner?
   a) Fordi det er ressursmessig effektivt.
   b) Fordi utviklerne ikke er klar over risikoen.
   c) For å kunne sjekke input fra brukeren.
3. En taksonomi kan brukes til:
   a) Sortering.
   b) Klassifisering.
   c) Strukturering.
4. Når en webapplikasjon bruker standard SSL betyr det at:
   a) Kommunikasjon mellom klient og server er kryptert.
   b) Kommunikasjon mellom klient og server er kryptert og serveren er autentisert med digitalt sertifikat.
   c) Kommunikasjon mellom klient og server er kryptert og server og klient er autentisert med digitale sertifikater.
5. Penetrasjonstester utføres:
   a) Av eksterne testere på testversjon av system.
   b) Av utviklere på testversjon av system.
   c) Av eksterne testere på system i produksjonsmiljø.
   d) Av utviklere på system i produksjonsmiljø.

Oppgave 2 (20%)

a) Beskriv i grove trekk trusselbildet for en webapplikasjon.

b) Hva er et ”software security touchpoint”? Beskriv de ulike ”touchpoints” fra faget og hvordan de passer inn utviklingsprosessen.

c) Hva er det første - og siste - en sysadm vil gjøre når et system feiler?

d) Code review er effektivt men ressurskrevende og derfor kostbart. Hvis du skulle gjøre code review av et system, men har et begrenset budsjett og gjennomgang av all kode er derfor uaktuelt - hvordan ville du prioritere? Begrunn valgene dine.

Oppgave 3 (20%) – Code Quiz – Spot the Bug

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.

```
public class BuggyClass{

      public static void main(String[] args){

      DbConnection con = DriverManager.getConnection(“myDb”);
      Statement stm = con.createStatement();

      ResultSet rs = stm.executeQuery(“INSERT INTO plaintexts VALUES (“ +
                     args[1] + “)”);

      SubProcedure();

      }
}
```

```
void SubProcedure() {
try {
      Byte[] text = GetPlaintextDataFromDB();
      Byte[] password = GetPassword();
      Byte[] salt = GetSalt();

      EncryptData(text,password);
      SendEncryptedData(text, salt);

      ScrubSecret(password);
      ScrubSecret(salt);
      ScrubSecret(text);

} catch (Exception e) {
   WriteToUI(“Error: “ + e);
}

}
```

Oppgave 4 (30%) – Case

Du jobber i et utviklingsteam som har fått i oppdrag å lage en applikasjon for firmaet NetworkServices. NetworServices selger sammensatte løsninger for overvåkning av bedriftsnettverk. En rekke sensorer plasseres ut i en bedrifts nettverk og data fra disse sammenstilles i et brukergrensesnitt for å gi bedre oversikt over trafikk og aktivitet i nettverket.
Tidligere har dette grensesnittet kun vært tilgjengelig som en selvstendig applikasjon. Kundene etterspør nå en web-basert løsning og mulighet for integrasjon med flere systemer via web-services. Sikkerhet er definert som en svært viktig kvalitet i løsningen.

Formuler en kravspesifikasjon og et overordnet design for systemet. Gjør bruk av de teknikker for utvikling av sikrere programvare som du har lært i faget og anser som relevante i disse utviklingsfasene. Gjør antagelser der du må, men marker og forklar de tydelig.

Oppgave 5 (20%) – Security testing

Med utgangspunkt i forrige oppgave: lag en sikkerhets-testplan for systemet basert på angrepene dere er gjort kjent med i faget. Definer hvilke angrep som er mest relevante å bruke og hvorfor. Hvis du anser noen som irrelevante så forklar hvilke og hvorfor. Du står fritt til også å definere egne angrep du ville ha utført for å avdekke feil. Begrunn valgene dine.

Strukturer testplanen etter det du mener er en hensiktsmessig rekkefølge av angrepene. Angi også en prioritet for angrepene etter hvilke du mener vil gi mest nytte i forhold til innsats.

NYNORSK

Oppgåve 1 (10%) – Multiple Choice

Vel det svaret du meiner er mest korrekt. Rett svar gjer 2 poeng – feil eller inga svar gjer 0 poeng.
Før det inn i svara dine slik som dette: 1a, 2b, 3c,…

1. Programvaresikkerheit handlar om…
   a) Å lage sikker programvare.
   b) Å lage programvare som kan motstå angrep.
   c) Å lage feilfri kode.
2. Kvifor opererar man ofte med fete klientar i webapplikasjonar?
   a) Fordi det er ressursmessig effektivt.
   b) Fordi utviklarane ikkje er klar over risikoen.
   c) For å kunne sjekke input frå brukaren.
3. Ein taksonomi kan brukast til:
   a) Sortering.
   b) Klassifisering.
   c) Strukturering.
4. Når ein webapplikasjon bruker standard SSL betyr det at:
   a) Kommunikasjon mellom klient og server er kryptert.
   b) Kommunikasjon mellom klient og server er kryptert og serveren er autentisert med digitalt sertifikat.
   c) Kommunikasjon mellom klient og server er kryptert og server og klient er autentisert med digitale sertifikat.
5. Penetrasjonstestar utførast:
   a) Av eksterne testarar på testversjon av system.
   b) Av utviklare på testversjon av system.
   c) Av eksterne testarar på system i produksjonsmiljø.
   d) Av utviklare på system i produksjonsmiljø.

Oppgåve 2 (20%)

a) Beskriv i grove trekk trusselbildet for ein webapplikasjon.

b) Kva er eit ”software security touchpoint”? Beskriv dei ulike ”touchpoints” frå faget og korleis de passer inn utviklingsprosessen.

c) Kva er det første - og siste - ein sysadm vil gjere når eit system feilar?

d) Code review er effektivt men ressurskrevjande og difor kostbart. Viss du skulle gjøre code review av eit system, men har eit begrenset budsjett og gjennomgang av all kode er difor uaktuelt - korleis ville du prioritere? Grunnje vala dine.

Oppgåve 3 (20%) – Code Quiz – Spot the Bug

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

```
public class BuggyClass{

      public static void main(String[] args){

      DbConnection con = DriverManager.getConnection(“myDb”);
      Statement stm = con.createStatement();

      ResultSet rs = stm.executeQuery(“INSERT INTO plaintexts VALUES (“ +
                     args[1] + “)”);

      SubProcedure();

      }
}



void SubProcedure() {
try {
      Byte[] text = GetPlaintextDataFromDB();
      Byte[] password = GetPassword();
      Byte[] salt = GetSalt();

      EncryptData(text,password);
      SendEncryptedData(text, salt);

      ScrubSecret(password);
      ScrubSecret(salt);
      ScrubSecret(text);

} catch (Exception e) {
   WriteToUI(“Error: “ + e);
}

}
```

Oppgåve 4 (30%) – Case

Du jobbar i et utviklingsteam som har fått i oppdrag å lage ein applikasjon for firmaet NetworkServices. NetworkServices seljer samansette løysningar for overvaking av bedriftsnettverk. Ein rekke sensorar plasserast ut i ein bedrifts nettverk og data frå disse samenstillast i et brukergrensesnitt for å gi betre oversikt over trafikk og aktivitet i nettverket. Tidligare har dette grensesnittet kun vore tilgjengeleg som ein sjølvstendig applikasjon. Kundane etterspør nå ein web-basert løysning og muligheit for integrasjon med fleire system via web-services. Sikkerheit er definert som ein svært viktig kvalitet i løysningen.

Formuler ein kravspesifikasjon og eit overordna design for systemet. Gjør bruk av de teknikkar for utvikling av sikrare programvare som du har lært i faget og anser som relevante i disse utviklingsfasane. Gjør antakingar der du må, men marker og forklar dei tydeleg.

Oppgåve 5 (20%) – Security testing

Med utgangspunkt i førre oppgåve: lag ein testplan for systemet basert på angrepa de er gjort kjent med i faget. Definer kva for angrep som er mest relevante å bruke og kvifor. Viss du anser noen som irrelevante så forklar kven og kvifor. Du står fritt til også å definere eigne angrep du ville ha utført for å avdekke feil. Grunngje vala dine.

Strukturer testplanen etter det du meiner er ein hensiktsmessig rekkefølgje av angrepa. Angi også ein prioritet for angrepa etter kven du meiner vil gi mest nytte i forhold til innsats.

ENGLISH

Task 1 (10%) – Multiple Choice

Select the answer you believe are the most correct. 2 points are rewarded for correct answer. 0 points are rewarded for wrong or no answer.
Enter your answers on a sheet like this: 1a, 2b, 3c, …

1. Software security is about…
   a) Creating secure software.
   b) Creating software is able to withstand malicious attacks.
   c) Creating code with zero bugs.
2. Why are fat clients commonly used in web applications?
   a) To limit network traffic and save resources.
   b) Because the developers are unaware of the risks.
   c) To perform validation of user input.
3. A taxonomy is used for:
   a) Sorting.
   b) Classification.
   c) Structuring.
4. When a web application is using standard SSL, it means that:
   a) Communication between client and server is encrypted.
   b) Communication between client and server is encrypted and the server is authenticated using a digital certificate.
   c) Communication between client and server is encrypted and both the server and the client are authenticated using digital certificates.
5. Penetration testing is performed:
   a) By external testers on a test-version of the system.
   b) By the developers on a test-version of the system.
   c) By external testers on the system in production environment.
   d) By developers on the system in production environment.

Task 2 (20%)

a) Provide an overview of the main threats towards web applications.

b) What is a ”software security touchpoint”? Give a short description of the different ”touchpoints” and how they fit into the software development process.

c) What is the first – and last – thing a system administrator is going to do if the system fails?

d) Code review is an effective technique but also resource demanding and therefore expensive. If you were to do code review of a system but your resources were limited, so it was not feasible to do a complete review of all code – how would you prioritize? Justify your choices.

Task 3 (20%) – Code Quiz – Spot the Bug

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.

```
public class BuggyClass{

      public static void main(String[] args){

      DbConnection con = DriverManager.getConnection(“myDb”);
      Statement stm = con.createStatement();

      ResultSet rs = stm.executeQuery(“INSERT INTO plaintexts VALUES (“ +
                     args[1] + “)”);

      SubProcedure();

      }
}
```

```
void SubProcedure() {
try {
      Byte[] text = GetPlaintextDataFromDB();
      Byte[] password = GetPassword();
      Byte[] salt = GetSalt();

      EncryptData(text,password);
      SendEncryptedData(text, salt);

      ScrubSecret(password);
      ScrubSecret(salt);
      ScrubSecret(text);

} catch (Exception e) {
   WriteToUI(“Error: “ + e);
}

}
```

Task 4 (30%) – Case

You are working for a development team that has been assigned the task of developing a software system for the firm NetworkServices. NetworkServices provides network monitoring services for their clients. Sensors are deployed in the internal network of the customer and sensor data are collected and displayed in a common interface – providing better overview over traffic flow and network activity.
This interface is currently a standalone application. The customers of NetworkServices are now demanding a new web-based interface that should provide potential for integration with other systems through web services. Security is a key property for this system.

Create a requirements specification and top-level design for this system. You should use the techniques presented in this course that you consider relevant in these development phases. You may make assumptions where needed, but make sure to clearly indicate what assumptions are made and explain why.

Task 5 (20%) – Security testing

Using the case from Task 4: create a security test plan for the system based on attacks you have been familiarized with in this course. Specify which attacks are most relevant and why. If you consider some attacks irrelevant then explain which ones and why. You may also create your own attacks if you consider it necessary. Justify your choices.

You should structure your test plan according to what you believe is a suitable order for carrying out the attacks.
Additionally, you should prioritize your attacks according to which attacks you believe will provide the best pay-off compared to required effort.