NTNU
Institutt for datateknikk
og informasjonsvitenskap

Eksamensoppgave i/Exam

TDT4237 – Programvaresikkerhet/Software Security

Tirsdag/Tuesday 14. desember/December 2010, 15:00 - 19:00

Oppgaven er utarbeidet av faglærer Lillian Røstad og kvalitetssikrer Torbjørn Skramstad.
Kontaktperson under eksamen er Lillian Røstad (mobil 994 00 628)

Språkform: Bokmål/Nynorsk/Engelsk
Tillatte hjelpemidler: D
Ingen trykte eller håndskrevne hjelpemidler tillatt. No printed or hand-written materials allowed.
Bestemt, enkel kalkulator tillatt. Approved calculator allowed.

Sensurfrist (results available): Fredag 14. januar 2010 (Friday January 14th 2010)

Les oppgaveteksten nøye. Finn ut hva det spørres etter i hver oppgave.

Dersom du mener at opplysninger mangler i en oppgaveformulering gjør kort rede for de antagelser og forutsetninger som du finner det nødvendig å gjøre.

Read each task carefully. Identify what the task asks for.

If you find that information is missing in a task you are free to make the assumptions you consider necessary, but remember to explain and clearly mark your assumptions.

-

BOKMÅL

Oppgave 1 (25% - hvert spørsmål teller 5%)

a) Hva brukes et angrepstre til? Illustrer med et eksempel.
b) Hva er forskjellen på *autentisering* og *identifisering*? Forklar med et eksempel.
c) Hvordan ville du ha beregnet risiko?
d) Hvilke hovedkategorier (Kingdoms) består McGraws taksonomi av?
e) For hvilken type angrep ville ha du brukt outputvalidering som et mottiltak? Forklar hvorfor.

Oppgave 2 (25%) – WikiLeaks

WikiLeaks ble opprettet i 2007 og er et nettsted som publiserer lekket informasjon fra anonyme kilder, som regel informasjon fra/om myndigheter og større organisasjoner. I november 2010 startet WikiLeaks publiseringen av mer enn 250 000 meldinger fra amerikanske ambassader. I en oppfølgerartikkel skriver Time (www.time.com/wikileaks) at:

- 11 000 av disse meldingene var klassifisert som ”secret” som per definisjon betyr at publisering av disse kan forårsake ”serious damage to national security”.
- at antall klassifiserte ”hemmeligheter” i USA har økt med 75% fra 1996 til 2009.

I 1995 ga Bill Clinton 20 personer myndighet til å klassifisere dokumenter som ”top secret”. Definisjonen av top secret sier at publisering av slik informasjon kan ”cause exceptionally grave damage to the national security”. Problemet var bare at disse 20 menneskene også fikk muligheten til å delegere denne myndigheten videre til 1336 andre. Samtidig har The Washington Post funnet at 854 000 mennesker er klarert for tilgang til informasjon klassifisert som ”top secret”.

Denne (foreløpig) siste store publikasjonen av klassifiserte dokumenter via WikiLeaks har ført til omfattende diskusjoner. Ut i fra informasjonen gitt ovenfor:

1. Hva mener du er det viktigste problemet som pekes på her?

I etterkant av hendelsen har deling av informasjon mellom offentlige myndigheter i USA nesten stoppet opp. Det er tydelig at de trenger et bedre system for sikker meldingsflyt seg imellom.

2. Hva mener du er de viktigste kravene de bør stille til et slikt system? Vis hvordan du kommer frem til disse kravene. Gjør gjerne antagelser der du må, men marker antagelsene dine tydelig.

Oppgave 3 (30%) – Identitetshåndtering

Identitetshåndtering (IAM – Identity and Access Management) er et stort og viktig tema innenfor sikkerhetsverdenen som har blitt enda viktigere og mer komplisert i de senere år fordi man i stadig større grad kobler systemer sammen og ønsker samhandling på tvers. For IAM i slike scenarier kan man velge mellom to ulike tilnærminger:

- Én sentral brukerbase som brukes av alle og som alle stoler på. Et eksempel er MinID som er en felles påloggingsløsning for offentlige tjenester.
- Sammenkobling gjennom etablering av tillitsrelasjoner mellom flere brukerbaser.

Begge disse to omtales gjerne under fellesbegrepet "identitetsføderering", men de er radikalt ulike. Det handler om man skal velge å etablere én part (TTP - tiltrodd tredjepart) som alle parter som inngår i samhandlingen stoler på og la denne håndtere registrering og autentisering av brukere, eller om man skal etablere felles kvalitetsstandarder for registrering og autentisering og deretter stole på hverandre.

I det første scenariet vil en bruker ved innlogging til en tjeneste videresendes til TTP for autentisering. Ved vellykket autentisering sender TTP et token som bevis for autentisering tilbake til tjenesten og brukeren sendes også tilbake til tjenesten.

I det andre scenariet vil brukeren autentiseres av tjenesten han først tar i bruk. Dersom brukeren så går videre til en annen tjeneste - som har et etablert tillitsforhold til den første tjenesten – vil dette foregå sømløst for brukeren. Han vil oppleve å være innlogget umiddelbart uten å måtte foreta noen aktiv handling. I bakgrunnen formidles et token som bevis for godkjent autentisering fra den første tjenesten, der brukeren autentiserte seg, til den nye tjenesten som brukeren nå ønsker å benytte.

I forrige oppgave utarbeidet du et sett med krav for en ny tjeneste for sikker meldingshåndtering mellom ulike offentlige myndigheter i USA. I denne oppgaven skal du:

1. Foreta et valg for hvordan IAM skal realiseres i tjenesten for sikker meldingshåndtering. Du må begrunne valget ditt. Vis hvordan du kom frem til dette valget.

Når du har gjort et valg vil IAM-løsningen realiseres av andre, men du er ansvarlig for å verifisere at løsningen er "sikker". IAM-løsningen blir en kjernekomponent i systemet for sikker meldingshåndtering. Sentralt her er derfor en testplan for å verifisere at sikkerhetskrav er ivaretatt. Du skal i denne oppgaven:

2. Utarbeide en risikobasert testplan for IAM løsningen.

Oppgave 4 (20%) – SQL injections

I siste versjon av OWASP top 10 er injection-angrep på førsteplass – opp en plass fra 2007-versjonen av listen. Det finnes et stort antall injection-angrep, men blant de aller vanligste er SQL-injections. I denne oppgaven skal du:

1. Forklare hvordan du best kan vite – eller finne ut – om en applikasjon er sårbar for SQL-injections.
2. Forklare hvordan du kan motvirke eller beskytte deg mot SQL-injections.
3. Gi et eksempel på kode som er sårbar for SQL-injection angrep.
4. Vise hvordan denne koden kan utnyttes og forklare hva resultatet ville blitt – dvs. hva en angriper kan oppnå.
5. Forklare hvordan du ville klassifisert sårbarheten i eksempelet ditt (fra punkt 3.) i McGraws taksonomi.

NYNORSK

Oppgåve 1 (25% - kvart spørsmål teller 5%)

a) Kva brukes eit angrepstre til? Vis med eit eksempel.
b) Kva er forskjellen på *autentisering* og *identifisering*? Forklår med eit eksempel.
c) Korleis ville du ha rekna ut risiko?
d) Kva for hovedkategorier (Kingdoms) består McGraws taksonomi av?
e) For kva type angrep ville ha du brukt output validering som eit mottiltak? Forklår kvifor.

Oppgåve 2 (25%) – WikiLeaks

WikiLeaks vart oppretta i 2007 og er ein nettstad som publiserar lekka informasjon frå anonyme kjelder, oftast informasjon frå/om myndigheiter og større organisasjonar. I november 2010 starta WikiLeaks publiseringa av meir enn 250 000 meldingar frå amerikanske ambassader. I ein oppfylgerartikkel skriv Time (www.time.com/wikileaks) at:

- 11 000 av desse meldingane var klassifisert som ”secret” som tuder at publisering av desse kan føre til ”serious damage to national security”.
- antall klassifiserte ”løyndomar” i USA har auka med 75% frå 1996 til 2009.

I 1995 ga Bill Clinton 20 personer myndigheit til å klassifisera dokumenter som ”top secret”. Definisjonen av top secret seier at publisering av slik informasjon kan ”cause exceptionally grave damage to the national security”. Problemet var berre at desse 20 menneskja og fekk mogelegheit til å delegera denne myndigheita vidare til 1336 andre. Samstundes har The Washington Post funni ut at 854 000 menneskje er klarert for tilgang til informasjon klassifisert som ”top secret”.

Denne (førebels) siste store kunngjeringa av klassifiserte dokument frå WikiLeaks har ført til røslige ordskifte. Ut frå informasjonen gitt ovanfor:

1. Kva meiner du er det viktigaste problemet som ein pekar på her?

I etterhand av hendinga har deling av informasjon mellom offentlege myndigheiter i USA nesten stoppa. Det er tydelig at dei treng eit bettre system for sikker flyt av meldingar mellom seg.

2. Kva meiner du er dei viktigaste krava dei bør stille til eit slikt system? Vis korleis du kjem fram til desse krava. Gjer gjerne antakelser der du må, men merk dei tydeleg.

Oppgåve 3 (30%) – Identitetshandtering

Identitetshndtering (IAM – Identity and Access Management) er eit stort og viktig område innan sikkerheitsverdenen som har blitt endå viktegare og meir komplisert i dei seinere år av di ein meir og meir kopler systema saman og ynskjer samhandling på tvers. For IAM i slike scenarier kan ein velgje mellom to ulike tilnærmingar:

- Ein sentral brukerbase som vert brukt av alle og som alle litar på. Eit eksempel er MinID som er ei sams påloggingsløysing for offenteige tenester.
- Samankopling gjennom å etablera tillitsrelasjonar mellom fleire brukerbasar.

Begge desse vert ofte omtala med eit sams begrep ”identitetsføderering”, men dei er radikalt ulike. Det handlar om ein skal velgje å etablere ein part (TTP - tiltrodd tredjepart) som alle partar som er med i samhandlinga liter på og la denne handtere registrering og autentisering av brukere, eller om ein skal etablera sams kvalitetsstandarder for registrering og autentisering og så lita på kvarandre.

I det første scenariet vert ein brukar ved innlogging til ein tjeneste sendt vidare til TTP for autentisering. Ved vellukka autentisering sender TTP eit token som prov for autentisering tilbake til tjenesten og brukaren vert og sendt attende til tjenesten.

I den andre scenariet vil brukaren autentiseres av den tenesten han fyrst tek i bruk. Om brukaren så går vidare til ei anna teneste - som har eit etablert tillitsforhold til den fyrste tenesta – vil dette gå føre seg sømløst for brukaren. Han vil oppleva å vera logga inn med det same utan å måtte gjera ei aktiv handling. I bakgrunn vert eit token som prov for godkjent autentisering formidla frå den første tenesten, der brukaren autentiserte seg, til den nye tenesten som brukaren nå ynskjer å nytta.

I førre oppgåve utarbeidde du eit sett med krav for ein ny teneste for trygg meldingshandtering mellom ulike offentlege myndigheiter i USA. I denne oppgåva skal du:

1. Gjere eit val for korleis IAM skal realiserast i tenesta for trygg meldingshandtering. Du må grunngje valet ditt. Vis korleis du kom fram til dette valet.

Når du har gjort eit val vert IAM-løysinga realisert av andre, men du er ansvarleg for å verifisere at løysninga er ”sikker”. IAM-løysinga blir ein kjernekomponent i systemet for trygg meldingshandtering. Sentralt her er difor ein testplan for å verifisere at sikkerheitskrava er ivareteke. Du skal i denne oppgåva:

2. Utarbeide ein risikobasert testplan for IAM løysinga.

Oppgåve 4 (20%) – SQL injections

I den siste versjonen av OWASP top 10 er injection-angrep på fyrsteplass – opp ein plass frå 2007-versjonen av lista. Det finnst eit stort antall injection-angrep, men blant dei aller vanlegaste er SQL-injections. I denne oppgåva skal du:

1. Forklare korleis du best kan veta – eller finna ut – om ein applikasjon er sårbar for SQL-injections.
2. Forklare korleis du kan motverke eller verne deg mot SQL-injections.
3. Gje eit eksempel på kode som er sårbar for SQL-injection angrep.
4. Vise korleis denne koden kan utnyttast og forklåre kva resultatet ville bli – dvs. kva ein angripar kan vinna.
5. Forklåre korleis du ville klassifisert sårbarheita i eksempelet ditt (frå punkt 3.) i McGraws taksonomi.

ENGLISH

Task 1 (25% - each task counts 5%)

a) What would you use attack-trees for? Use an example to illustrate.
b) What is the difference between authentication and identification? Explain by providing an example.
c) How would you calculate risk?
d) What main categories (Kingdoms) does McGraw's taxonomy consist of?
e) For what type of attack would you use output validation as a countermeasure? Explain why.

Task 2 (25%) – WikiLeaks

WikiLeaks was established in 2007 as an organization aimed at enabling publication of otherwise unavailable documents, typically leaked from sources in government or large organizations. In November this year WikiLeaks began publishing more than 250 000 messages from US embassies. In a follow-up article Time magazine (www.time.com/wikileaks) notes that:

- 11 000 of the published messages were classified as "secret". According to the US government definition of "secret", publication of this information may cause "serious damage to national security".
- The number of classified "secrets" in has increased by 75% from 1996 to 2009

In 1995, Bill Clinton granted 20 people the authority to classify documents as "top secret". By definition, a classification as "top secret" means that publication of this information may "cause exceptionally grave damage to the national security". The problem was that these people were also granted the power to delegate their authorities to a total of 1336 other persons. In addition, The Washington Post reports that 854 000 people are currently authorized to view information classified as "top secret".

This (for now) latest publication of classified documents via WikiLeaks has initiated some major discussions. Based on the information given above:

1. What do you think is the most important problem these facts point at?

After this incident, information shared between government agencies has come to a halt. It is evident that they need a better system for secure messaging between agencies.

2. What do you think are the most important requirements for such a system? Show how you arrived at these requirements. Make assumptions where you need to, but remember to clearly mark and justify your assumptions.

Task 3 (30%) – Identity management

Identity management (IAM – Identity and Access Management) is an important topic within security that has become increasingly relevant lately as more and more systems are interconnected and the demand for interoperability and cooperation is increasing. In cooperative environments there are two main possibilities for IAM:

- A centralized solution in which there is one central user base that is used and trusted by everyone. MinID (MyID) which is a common eID-solution for public services in Norway is an example of one such approach.
- A decentralized solution connecting several user bases by establishing trust relationships between service providers.

Both these approaches, though very different, are often referred to as "identity federation". The main difference is whether one shall select a trusted third-party (TTP) that everyone trusts to handle user registration and authentication, or if one shall establish a set of common quality standards for registration and authentication and trust each other to execute these services.

In the first scenario (centralized) a user will be forwarded to the TTP on logging in to a service. If authentication is successful the TTP returns a token as proof of authentication and redirects the user back to the originating service.

In the second scenario (decentralized) the user is authenticated by the first service he uses. If the user then accesses another service – that has an established trust relationship with the originating service – this process will be seamless to the user, meaning that he will be logged in and recognized by the new service. This is enabled by a background call where a token is sent form the originating to the new service.

In the previous task you developed a set of requirements for a system for secure messaging between government agencies in the US. In this task you shall:

1. Select the appropriate IAM-method for the secure messaging service. You must explain your decision. Remember to demonstrate how you arrived at this decision.

Once you have made your decision, someone else will be implementing the IAM-solution, but you are still responsible for making sure the resulting solution is "secure" The IAM-solution is a core component of the secure messaging service. It is therefore important to create a test plan that enables you to verify that all security requirements are met. In this task you shall:

2. Create a risk-based test plan for the IAM-solution.

Task 4 (20%) – SQL injections

The latest version of the OWASP top 10 lists injection-attacks at number one – up one spot from the 2007 list. There are a number of injection attacks, but SQL injections are among the most common. In this task you shall:

1. Explain how you can tell – or figure out – if an application is vulnerable to SQL injections.
2. Explain how you may prevent or protect your application from SQL injections.
3. Provide/create a code example illustrating SQL injection vulnerability.
4. Demonstrate how this code may be exploited and explain what the result of an attack would be – i.e. what an attacker could achieve.
5. Explain how you would classify the vulnerability in your code (from 3.) according to McGraw's taxonomy.