Norges teknisk-naturvitenskapelige universitet
Institutt for telematikk

EKSAMEN I
SIE5040 – INFORMASJONSSIKKERHET

Faglig kontakt under eksamen: Stig F. Mjølsnes. (tlf. 41305114).

Eksamensdato: 8. mai 2003.

Eksamenstid: kl. 09:00 – 13:00 (4 timer).

Sensurdato: 30. mai 2003.

Vekttall: 2,5.

Tillatte hjelpemidler: Kalkulator. Ingen trykte eller håndskrevne hjelpemidler tillatt (D).

Ingen vedlegg.

Oppgaver

Vektlegging på oppgavene er gitt i prosent, og som heltall på enkeltspørsmålene. Skriv helst konsist og oversiktlig.

Oppgave 1. (15%) Modeller

a) Hvilke tre eller fire hovedkrav til informasjonssikkerhet vil du liste opp? (1)

b) Forklar mulige nytteverdier av formelle sikkerhetsmodeller. (1)

c) Beskriv Bell-LaPadula (BLP) modellen på en konsis måte? (2)

d) Hvilke anvendelsesproblemer har BLP-modellen? (1)

e) Hvorfor kan ikke Kinesisk-mur modellen beskrives ved hjelp av BLP-formalismen?(1)

Oppgave 2. (25%) Aksesskontroll

a) Hva legger du i begrepet ”referansemonitor”? (1)

b) ”The user identity is a parameter in access control decisions” påstår læreboka. Forklar dette. (1)

c) ”The superuser is the main security flaw in the UNIX system”. Lag ett argument for og ett argument mot dette utsagnet. (2)

d) Hvordan oppstår problemet med ”styrt iverksetting” (controlled invocation)? Forklar gjerne med et eksempel på hvordan Unix løser problemet. (3)

e) Hva er Kerberos, og hvilken funksjon har dette systemet? Beskriv, tegn og forklar arkitektur og virkemåte (anbefalt 2 sider). (3)

Oppgave 3. (35%) Sertifikater

a) Hvorfor kan RSA-algoritmen fungere som en offentlig-nøkkel algoritme? (1)

b) Definer egenskapene til en enveis hashfunksjon med sterk kollisjonsfrihet, og gi to eksempler på anvendelse. (2)

c) Hva menes med et X.509 sertifikat, og hva er hovedinnholdet av dette? (2)

d) Nevn to kriterier for at et X.509 sertifikat skal være gyldig? (2)

e) Nevn punktvis noen av bruksområdene til slike sertifikater. (1)

f) Beskriv og lag skisser på hvordan SSL benytter slike sertifikater. (4)

g) Du skal sette opp en Tomcat webserver. Denne skal motta forespørsler via HTTPS. Du har laget et nøkkelpar, og fått utstedt et sertifikat fra sertifikatautoriteten (CAen) ServerCerts, denne er igjen signert av en autoritet som heter Root. Forklar hva nøkkelringene KeyStore(/KeyManager) og TrustStore(/TrustManager) må inneholde for at oppsettet skal virke slik du ønsker. Hint: KeyStore i Java tilsvarer blant annet SSLCertificateChainFile i Apache. TrustStore tilsvarer SSLCACertificateFile. (2)

Oppgave 4. (25%) Sikkerhetsanalyse

Som datasikkerhetsekspert i Lommerusk AS får du i oppgave å foreslå og konstruere en enkel og billig tilgangskontroll for bedriftens nye lommemaskin LM. Biometriske metoder blir av ukjente grunner ikke aktuelt, så du faller ned på den enkle løsningen at maskinen ved oppstart skal kreve at et passord besvares. Passord kan tastes inn på LM fra et norsk alfabet (små og store bokstaver) samt tall?

a) Hvilken minstelengde må kreves for å kunne velge blant mer enn 10^{10} mulige passord? (1)

b) LM har en tastatur-enhet som kan utvide alfabetet til å omfatte 28 forskjellige skille- og punktasjonstegn i tillegg. Hvilken minstelengde må nå kreves for å kunne velge blant mer enn 10^{10} mulige passord? (1)

c) Du gjør også en analyse på om LM skal kunne startes opp ved hjelp av ekstern kommunikasjon til en innebygget kortholds radioenhet (f.eks. Bluetooth). Dette medfører at uttømmende testing av passord kan foregå med en hastighet på 10 passord/sekund. Vi antar at brukeren vil oppdage et slikt angrep senest etter 72 timer. Hvor stort alfabet og passordlengde vil du anbefale for å trygge mot dette scenariet? Angi antagelser du gjør i dimensjoneringen her. (2)

d) Utfør en sikkerhetsanalyse av en funksjonalitet som gjøre det mulig med trådløs oppstart og kommunikasjon (”fjernbruk”) av en LM? Foreslå tekniske mottiltak på mulige angrep du finner. (3)

Oppgave 4. (fortsettelse)

Du vurderer å bruke samme teknikk som Unix for å beskytte passord som lagres i LM. Du har lest at Martin Hellman laget en generell metode som kan benyttes for å angripe slike beskyttede passord. Gitt at angriperen får tak i et beskyttet passord så kan metoden benyttes til å finne passordet i klartekst på mye kortere tid enn uttømmende søk. Søketiden etter passordet kan reduseres ved å forhåndsberegne og lagre en tabell av verdier. Du husker ikke detaljene for dette, bare følgende egenskaper til metoden: La n være antall mulige passord. Generering av tabellen med $n^{2/3}$ verdier krever n beregninger. Dersom angriperen deretter får tak i et beskyttet passord, så kan metoden benyttes til å finne passordet ved søke i tabellen samt å utføre inntil $n^{2/3}$ beregninger.

e) Hvor stor lagringsplass krever tabellen dersom passordene antas å ha lengden som du beregnet i a)? Kommenter tabellstørrelsen du finner med hensyn på praktisk gjennomførbarhet. (2)

f) Hvor raskt kan en angriper finne passordet ved hjelp av denne metoden dersom en beregning tar ett millisekund? Er dette angrepet relevant i forhold til sikkerhetsanalysen din i pkt. d)? (1)
