KTH Datavetenskap
och kommunikation

DD2395 Datasäkerhet
Tentamen 2007-10-24 kl 09.00–13.00

Inga hjälpmedel är tillåtna. För att få godkänt på tentan måste man få godkänt på del I (U på högst en fråga). Tentabetyget ges av poängen på del II. Betygsgränserna är preliminärt D – 15p, C – 20p, B – 25p. För betyg A krävs B på denna tenta och godkänt på en muntlig tenta.

Enligt nya bestämmelser så erbjuds studenter som varit mycket nära gränsen för godkänt att komplettera till betyg E på tentan. Detta sker i så fall genom muntlig eller skriftlig komplettering motsvarande ett område som man inte vid tentatillfället behärskat. Vid komplettering kan tentamensbetyget inte bli högre än E.

Del I

1 Vid till exempel inloggning kan man använda *N-faktorautentisering*.

1a Vad innebär *N-faktorautentisering* jämfört med vanlig löseonordsinloggning?

1b Ge exempel på hur 2-faktorautentisering skulle kunna gå till.

2 I både Biba och Bell–LaPadula använder man sig av säkerhetsnivåer och fack (eng. compartments).

2a Hur används nivåerna och facken i respektive modell?

2b Antag att man använder båda modellerna och att ett visst objekt har samma säkerhetsnivåer och fack i båda. Vad krävs för att en aktör (eng. subjects) ska kunna skriva till objektet respektive läsa från det?

3 Jämför symmetrisk och asymmetrisk kryptering. Vilka är de mest centrala skillnaderna. Om man har 100 personer som alla ska ha möjlighet att kommunicera parvis, hemligt, hur många nycklar behövs då i respektive fall?

4 Vad är en accesskontrollmatris? Vad är capabilities?

5 TCSEC eller ”Orange book” är en del av ”Rainbow Series” men varifrån kommer den och vad handlar den om?

6 I samband med kryptografi används begreppet ”certifikat”. Vad är ett certifikat? Berätta vad PKI står för och hur det fungerar / är tänkt att fungera.

Del II

7 En utvecklingschef på ett större företag använder en laptop i arbetet. Datorn har ett inloggningsförfarande som innebär att man antingen anger ett lösenord eller låter datorn scanna fingeravtryck. Med hjälp av datorn lägger hon upp projektbudgetar och tidplaner, och hon har även ibland kopior på data om produkten (den militära terrängbilen ”Lille Skutt”), som utvecklas. Datorn följer även med på resor när hon förhandlar med andra stater om eventuella vapenköp, för att hon ska kunna skriva avtal på plats (om det är riktigt bråttom).

7a Gör en hotanalys som även tar hänsyn till vilka skador som kan uppstå. [2p]

7b Föreslå rimliga sätt att skydda sig mot de hot du identifierat. [2p]

8 Kerberos är en utveckling av Needham–Schröder och används bland annat för inloggning. Här följer en kraftigt förenklad (och lite förvanskad) beskrivning av hur Dave loggar in på datorn HAL.

1. Användaren Dave skickar meddelandet $[Dave||HAL||TS_1]$ (där TS_1 är aktuell tid på Daves klient med noggrannhet i sekunder på Daves klient) till Kerberos-servern.
2. Kerberos-servern kontrollerar att TS_1 är tillräckligt nära (inom 5 minuter) dess egen tid och svarar med meddelande

   $E(K_{Dave}, [K_s||Dave||HAL||TS_2||T||L])$

   där $T = E(K_{HAL}, [K_s||Dave||HAL||TS_2||L])$

   Nyckeln K_{Dave} är härledd från Daves lösenord (man använder en kryptografiskt säker känd hashfunction på nyckeln), och nyckeln K_{HAL} är hemlig och delas mellan Kerberos-servern och HAL. K_s är en sessionsnyckel och L är nycklens livslängd.
3. Dave dekrypterar meddelandet, erhåller K_s och skickar $[T||E(K_s, TS_3)]$ till HAL.
4. HAL dekrypterar T, får K_s, dekrypterar andra halvan av meddelandet, får TS_3, jämför med sin klocka och skickar sedan tillbaka $[E(K_s, TS_3 + 1)]$

Antag att du avlyssnat en inloggning (dvs har tillgång till samtliga meddelanden som beskrivits ovan). Du misstänker att användaren har ett svagt lösenord. Du har en lista med 10,000 vanliga lösenord och vill veta om avändaren använder något av dem och i så fall vilket, men du vill inte testa att logga in flera gånger eftersom misslyckade inloggningar loggas. Hur kan du ta reda på lösenordet utan att göra testinloggningar?

Du kan först anta att alla klockor går lika och att det går fort (dvs $TS_1 = TS_2 = TS_3$ i konversationen). Berätta också hur det går om klockorna inte går lika, men tillräckligt rätt för att inloggningen ska lyckas (anta att det skiljer högst 5 minuter mellan de TS som skiljer sig mest och att alla tider anges i sekunder). [4p]

9 Myndighetsavvecklingsmyndigheten är en ny myndighet som tillkommit för att bekämpa onödig byråkrati inom statsförvaltningen. Dess slimmade organisation betår av myndighetschefen och tio tjänstemän. Alla deras IT-behov täcks av en server och de får inte köpa in ytterligare hårdvara. Således sköter de sin surfning, sin epost, sin bokföring, ja hela sin verksamhet, med den datorn. Personalen har tunna klienter för inloggning på datorn, och det finns även en terminal i receptionen för att besökare ska kunna surfa för att t.ex. ta reda på tågtider, eller telefonnumret till det lokala taxibolaget (alla besökare grips förr eller senare av en stark lust att åka någon annanstans).

9a På serverdatorn körs bland annat en webbserver med fina php-sidor. Hittills har den kört med administratörsrättigheter (för då fungerade den plötsligt). Varför är det en dålig idé? [2p]

9b Till sist fastnar man för att göra en speciell användare `webb` som man låter webbservern köra som. Man gör filerna som webbservern ska läsa läsbara gör `webb`, och på så vis kan den läsa nödvändiga filer utan att man för den skull gör dem tillgängliga för alla. De anställda kan nu göra egna fina php-sidor i sin `public_html`-katalog och behöver bara göra dem läsbara för `webb` och inte för hela världen. Vad får detta för konsekvenser om man anväder det i en större organisation (till exempel på KTH)? [2p]

10 Ett spoofing-filter är en enkel form av brandvägg. Vad kontrollerar det? Ge exempel på någon vanlig attack eller vanligt missbruk som spoofing-filter kan stoppa. [2p]

11 Hur fungerar ett bootsektorvirus? [2p]

12 En av skillnaderna på Windows XP Home edition och Windows XP Professional är hur man specificerar accesskontroll. I XP Professional finns en ganska rik struktur för att specificera till exempel accesskontrolllistor för enskilda objekt och ange rättigheter för enskilda användare eller grupper av användare. I XP Home är modellen enkel: en mapp kan vara privat (bara användaren som äger den kan se den), delad (alla kan se den) eller så kan användaren och administratören se den. En mapp kan även vara skrivskyddad. Vad är den troliga orsaken till att man valt att göra den skillnaden mellan versionerna? [3p]

13 Vi erbjuds att köpa ett NIDS (Network intrusion detection system) som enligt säljaren har följande egenskaper: hög chans för upptäckt (om vi attackeras är chansen att systemet larmar 87%) och låg risk för falsklarm (ett inkommande paket som inte är del av en attack leder till larm med sannolikhet 0.01%). Verkar det vara en bra affär? Varför / varför inte? [3p]

14 PHP är ett språk som låter dig skriva kod som exekveras på en webbserver och som (oftast) fungerar så att HTML genereras och skicks till den webbläsare som anropat sidan. Här följer ett fragment av sidan `check.php` som rättar en inskickad tipsrad på ett flervalsprov:

```
$corr = '1X22X2X11X122';
if (strlen($ans) != strlen($corr)) /* om olika långa så fel */
  $err=1;
else {
  for ($i=0; $i<strlen($ans); ++$i)
    if ($ans[$i] != $corr[$i]) ++$err;
}
if ($err>0) {
  /* kod om man svarat fel */
} else {
  /* kod om man svarat rätt */
}
```

Anropet till sidan kan se ut så här:
`http://www.example.com/check.php?ans=1XX211XX2121X`
Att det fungerar beror på att variabler inte behöver deklareras eller initieras i PHP. `$err` börjar alltså på 0. Dessutom finns ett direktiv `register_globals` som om det är satt till sant gör att variabler i url:en automatiskt importeras som globala variabler i skriptet.

Från början var `register_globals=true` som standard, men från och med PHP 4.2.0 så har det satts till `false` som standard. Varför tror du man valt att göra så (relatera till exemplet)? [4p]

15 Följande pseudokod beskriver hur en överföring mellan konton skulle kunna gå till.

```
transfer(fromacct, toacct, amount)
/* vi kan anta att parametrarna har filtrerats
 * så att de har giltigt format
 */
  if (amount<0 or amount>MAX_TRANSFER)
    return ILLEGAL_AMOUNT
  elif (not acct_exists(fromacct))
    return NON_EXISTENT_ACCT
  elif (not acct_exists(toacct))
    return NON_EXISTENT_ACCT
  elif (balance(fromacct) < amount)
    return INSUFFICIENT_FUNDS
  else
    deposit(amount,toacct)
    withdraw(amount,fromacct)
    return success
```

Vad finns det för potentiella problem? Hur hanterar man sådant i ”riktiga” system? [4p]