KTH Datavetenskap
och kommunikation

2D1395 Datasäkerhet
Lösningar till tentamen 2006-10-18

Del I

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

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

Lösning: Att man bevisar sin identitet på mer än ett sätt (på två sätt vid 2-fatorautentisering), på så vis att autentiseringen lyckas om samtliga sätt att bevisa identiteten lyckas.

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

Lösning: Man kan kombinera en ”smartcardläsare” med fingeravtrycksigenkänning.

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?

Lösning: Varje dokument och varje aktör har en säkerhetsnivå s och en mängd av fack M. Säkerhetsnivåerna anger hur ”känslig” information är (till exempel ”hemlig”), och facken talar om vad informationen handlar om (t.ex. skulle ett dokument om arméns oljedepåer kunna tillhöra facken ”militär” och ”drivmedel”). Man säger att (s, M) dominerar (s', M') om $s \geq s'$ och $M \supseteq M'$. Låt oss anta att aktören a har (s_a, M_a) och dokumentet d har (s_d, M_d). I Bell-Lapadula kan a läsa d om (s_a, M_a) dominerar (s_d, M_d), och skriva till d om (s_a, M_a) domineras av (s_d, M_d). I Biba är det tvärt om: a kan skriva till d om (s_a, M_a) dominerar (s_d, M_d) och läsa d om (s_a, M_a) domineras av (s_d, M_d).

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?

Lösning: Aktören måste då både dominera objektet och domineras av objektet, så hennes nivå och fack måste vara exakt desamma som objektets i båda fallen.

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?

Lösning: Viktigaste skillnaden är att vid symmetrisk kryptering mellan A och B måste de i förväg ha bestämt en hemlig nyckel K_{AB} som bara de känner till. Vid Asymmetrisk kryptering har de istället varsitt nyckelpar som de kan bestämma var och en för sig. As par innehåller en publik krypteringsnyckel K_A^E och en hemlig dekrypteringsnyckel K_A^D. B krypterar med K_A^E för att skicka meddelanden till A som A kan dekryptera med K_A^D. I det ena fallet får man $100 \cdot 99/2 = 4950$ symmteriska nycklar, i det andra 100 nyckelpar.

Kommentar: även svar där man räknat ett nyckelpar som EN nyckel eller där man räknat lite fel på antal par av personer har gett G, så länge det gått att avgöra att tentanden förutom räknefelet tänkt rätt.

4 Vad är en accesskontrollmatris? Vad är capabilities?

Lösning: En accesskontrollmatris beskriver vilka aktörer (”subjects” eller ”principals”) som ska ha vilken access till vilka objekt. För varje aktör finns en rad och för varje objekt en kolumn. I ruta $A_{a,o}$ anges as rättigheter till objektet o. Rättigheter kan vara t.ex. ”own”, ”read”, ”write” och ”execute”. Capabilities är ett sätt att lagra matrisen radvis. Dvs, en aktörs rättigheter ”lagras hos aktören” på ett sätt som inte låter aktören själv påverka vilka rättigheter hon har.

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

Lösning: Ett dokument framtaget av amerikanska staten som standardiserar hur anskaffning och utvärdering av datasystem ska göras inom statlig verksamhet. Dokumentet är numera ersatt av nyare standarder men har varit mycket inflytelserikt när det gäller begrepp och praxis på området.

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.

Lösning: Ett certifikat är ett elektroniskt signerat dokument som associerar en identitet med de publika nycklar som den personen / den aktören använder. Det används inom PKI, Public Key Infrastructure, för att sätta upp en virtuell katalog över användares nycklar. För att kunna verifiera ett certifikat behöver du de publika nycklar som hör till den som ställt ut certifikatet. På så vis räcker det att du kan nyklarna för ett fåtal parter som ställer ut certifikat, för att du ska kunna kontrollera certifikat som talar om vilka publika nycklar som andra personer använder.

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]

Lösning: Datorn kan skadas med dataförlust som följd. Någon skulle kunna stjäla datorn, och i det läget spelar inte autentisering så stor roll. Hårddisken kan monteras ur och läsas med hjälp av annan dator utan att man behöver autentisera sig. Om den lämnas obevakad finns risk för att någon lyckas lägga in någon form av rootkit, keylogger, trojan eller annan elak mjukvara. Eftersom fingeravtryck är ett alternativ (dvs inloggning görs med fingeravtryck eller lösenord) så finns förstås de vanliga problemen med ev dåligt lösenord. Eftersom datorn ev kopplas in på nätverk under resorna finns risk att trafiken avlyssnas.

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

Lösning: Viktig information bör inte finnas enbart på den bärbara datorn. Hemlig information bör vara krypterad för att skydda den även vid stöld. Kommunikation bör också krypteras. Datorn bör egentligen inte lämnas obevakad, och gör man det behöver den på något sätt låsas in så att obehöriga inte kan komma åt den. Något i still med tripwire kan användas för att upptäcka om systemfiler modifierats. Viktig information bör vara signerad (för at avslöja förändringar) förutom att vara krypterad.

Kommentar: Förslaget att man under resor ska ta hjälp av sin värd för att få datorn bevakad eller inlåst är inte lämpligt. I det här sammanhanget finns det skäl att misstänka att värden skulle vara mycket intresserad av att komma åt innehållet i datorn.

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]

Lösning: Eftersom den kryptografiska hashfunktionen är känd kan vi använda den för att hasha de 10,000 vanliga lösenorden. För varje nyckel K vi får på det viset, testa att dekryptera meddelandet som sänds i steg 2 med K. Förutom K_s vet vi innehållet i det meddelandet, så vi vet när vi träffat rätt, och då vet vi också vilket av de 10,000 orden som är Daves lösenord.

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]

Lösning: Eventuella fel på servern kan göra stor skada eftersom den har alla rättigheter. Om det finns säkerhetshål som kan ge utomstående möjlighet att köra godtyklig kod på servern (p.g.a. buffer overrun eller dåligt konfiguerad php eller annat), så skulle en angripare antagligen kunna göra godtyckliga saker som administratör.

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]

Lösning: Problemen från uppgift 1 finns förstås kvar, men på en lägre nivå. Problemet här är att användare kan lägga aktiva sidor som exekveras av servern, t.ex. php-sidor, i sin `public_html`. Dessa sidor körs sedan med webbwerverns rättigheter, och kan därmed göra allt som webbservrn kan göra, vilket är tveksamt om det är bra. Om webbservern t.ex. används för att köra php-sidor som uppdaterar eller läser i en databas kommer dessa sidor att vanligtvis att innehålla databaslösenord. Eftersom dessa sidor är läsbara av webbservern kan en användare skriva php-sidor som genom att läsa andra php-sidors innehåll extraherar databaslösenordet. Detta problem är tyvärr inte helt enkelt att komma ifrån. Lämpligen bör man inte använda samma webbserver för användarnas allmäna sidor som för sidorna som hanterar databasen.

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]

Lösning: Filtret kontrollerar att paket som kommer från det lokala nätverket har avsändar-IP-adresser som tillhör det lokala nätverket och att paket som kommer ”utifrån” har inte har avsändar-IP-adresser som ligger i det lokala nätverket. Detta kan till exempel stoppa utsändning av spam (som ofta har förfalskad ”source-adress”) från en dator som infekterats.

11 Hur fungerar ett bootsektorvirus? [2p]

Lösning: Se kursboken.

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 access-kontrolllistor 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]

Lösning: Man kan se ett par olika skäl som dock bottnar i att hemanvändare i allmänhet har andra behov än företag och organisationer. Den enkla modellen är otillräcklig för företag men ofta tillräcklig i ett hushåll. Dessutom är den enklare modellen lätare att förstå – risken för att en oerfaren användare konfigurerar XP professional fel är antagligen större och den större komplexiteten skulle därmed ofta medföra ett sämre skydd. Desstuom kan man förstås ta ut olika proser för olika produkter, och en enklare version för hemanvändare minskar trycket på supportavdelningen.

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]

Lösning: Det skulle antagligen innebära att de flesta larm är falsklarm. Låt oss göra ett enkelt räkneexempel. Låt oss anta att datorn utsätts för en attack genomsnitt en gång om dagen. Vi får då i genomsnitt knappt ett larm om dagen orsakat av attacker. Å andra sidan tar vi antagligen emot en stor mängd trafik per dag:100,000 paket är inte orimligt. Dessa paket skulle i genomsnitt utlösa ett tiotal falsklarm, dvs tio ggr så många falsklarm som larm som faktiskt innebär en attack.

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]

Lösning: Precis som `$ans` kan få sitt värde från URL:en så kan `$err` och `$corr` få det. Om `$corr` sätts så gör det inte så mycket eftersom den tilldelas ett värde explicit i koden. Däremot antar koden att `$err` är noll utan att explicit tilldela den värdet 0. Vi skulle alltså kunna skicka in t.ex. `http://www.example.com/check.php?ans=1XX211XX2121X&err=-13` och på så vis vara säkra på att `$err<=0` när det testats om man svarat rätt. Att klienten på så vis kan styra värdena på globala variabler på servern för förstås farligt.

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]

Lösning: Det finns två relaterade risker. Om programmet kraschar mitt i en transaktion så finns risken att pengana satts in på mottagarens konto men att de aldrig hann tas ut från avsändarens konto. Ett likartat problem kan uppstå ifall två överföringar går parallellt från samma konto. Det kan hända att två uttag på 900 kr godkänns fast det bara finns 1500 på kontot. Det skulle kunna vara så att båda transaktionerna kollar ”balance” innan någon av dem hinner ta ut pengarna. I praktiken hanteras sådant typiskt av att man har databastranskationer som kan ”rullas tillbaka”, dvs databasen återställs i tillståndet före transaktionen, om något går dåligt under en transaktion. För att hindra problemen med samtidiga läsningar och skrivningar använder man låsmekanismer (typiskt på rader i databastabeller, men i andra sammanhang på t.ex. filnivå).