Flernivåsäkerhet och multilateral säkerhet

Daniel Bosk[1]

Avdelningen för informations- och kommunikationssytem (IKS),
Mittuniversitetet, Sundsvall.

lvlltrl.tex 1093 2013-05-28 08:29:16Z danbos

Mittuniversitetet
MID SWEDEN UNIVERSITY

Översikt

1. Flernivåsäkerhet
   - Bell–LaPadula säkerhetspolicymodell
   - Bibamodellen
   - Alternativa modeller
   - Hemliga kanaler
2. Multilateral säkerhet
   - Gittermodellen (lattice model)
   - Kinesiska muren-modellen
   - BMA-modellen
   - Inferenskontroll

Litteratur

Denna föreläsning behandlar kapitel 8 ”Multilevel security” och kapitel 9 ”Multilateral security” i [And08].

Översikt

Översikt

Mittuniversitetet
MID SWEDEN UNIVERSITY

Bell–LaPadula säkerhetspolicymodell

Säkerhetspolicymodell Uttrycker koncist skyddegenskaperna ett system måste ha. Ligger till grund för formell analys.

Säkerhetsmål Mer detaljerad beskrivning av given implementation av mekanismer, hur dessa relaterar till mål (härledda från policymodellen). Grund för testning och utvärdering.

Skyddsprofil En implementationsoberoende version av säkerhetsmålet, används för att jämföra olika system.

Säkerhetspolicy Ett dokument som tydligt uttrycker målen våra säkerhetsmekanismer ska uppnå. Används ofta som synonym till både säkerhetspolicymodell och säkerhetsmål.

Bell–LaPadula säkerhetspolicymodell

- Ett säkert system bör göra en eller två saker väl – det måste vara enkelt.
- Dessa saker ska säkras av lika enkla mekanismer – som då går att analysera.
- Dessa mekanismer utgör vad som kallas *trusted computing base (TCB)*.
- Bell–LaPadula är exempel på en sådan säkerhetspolicymodell.
- Utvecklades av Bell och LaPadula under 1970-talet.
- Syftet är att skydda fleranvändarsystem.

Bell–LaPadula säkerhetspolicymodell

- Andra världskriget och Kalla kriget ledde NATO-länderna att utveckla en gemensam klassificeringsmodell för känsliga dokument.
- Klassificeringarna utgör etiketter som är ordnade i nivåer; från *ej sekretessbelagd (Unclassified)* till *förtrolig (Confidential)*, *hemlig (Secret)* och *kvalificerat hemlig (Top Secret)*.
- EU har även *begränsad (Restricted)*.
- En individ har *behörighet (clearance)* för en säkerhetsnivå.

Bell–LaPadula säkerhetspolicymodell

- En individ kan läsa information som är klassificerat till alla nivåer upp till den nivå denne är behörig.
- Det krävs speciella personer för att avklassificera dokument.
- Till de olika nivåerna hör olika skyddsnivåer.

Bell–LaPadula säkerhetspolicymodell

- Vi kan även lägga till speciella kodord till klassificeringarna.
- En klassificering med ett eller flera kodord utgör en *säkerhetskategori (security category eller compartment)*.
- Detta ger multilateral säkerhet.

Bell–LaPadula säkerhetspolicymodell

Bell–LaPadulamodellen (BLP)

NRU (Simple security property, No read up) Ingen process får läsa data från en högre nivå.

NWD (*-property, No write down) Ingen process får skriva data till en lägre nivå.

- Bell och LaPadulas säkerhetsmodell publicerades 1973.
- System som implementerar den kallas oftast *flernivåsäkra system (multilevel secure, MLS)*.
- Information kan inte flöda nedåt, bara uppåt.
- System som implementerar denna typ av policy oberoende av användaren sägs ha *obligatorisk åtkomstkontroll (mandatory access control)*.

Bell–LaPadula säkerhetspolicymodell

Utökning av BLP

Inför *tranquility property*, finns två varianter:

Stark Säkerhetsklassificeringar förändras aldrig under systemets gång.

Svag Säkerhetsklassificeringar förändras aldrig så att säkerhetspolicyn bryts.

- Anledningen till den svaga är *principle of least privilege*.
- Börja på lägsta säkerhetsnivån och öka allteftersom data med högre nivå används – *high watermark principle*.
- Vad händer då här en ny fil skapas senare?
- Det kommer att behövas en *trusted subject* för av avklassificera.

Översikt

Bibamodellen

- Vanligen kallad ”Bell–LaPadula upp-och-ned”.
- Används för integritet medan BLP används för konfidentialitet.
- Kan läsa data från högre nivåer men inte skriva till dem.
- Följaktligen används *low watermark principle*.
- Lägre nivåer innehåller osäkra data och data baserat på dessa kan därför inte vara mindre osäkra.
- LOMAC i Linux där en process nedgraderades från hög till låg då den mottog data från nätverket.
- Windows införde därefter liknande system för att säkra bland annat Internet Explorer.

Översikt

Alternativa modeller

- *Noninterference* kom 1982.
- Saker som händer på hög säkerhetsnivå har ingen effekt på vad låg säkerhetsnivå kan se.
- *Nondeducability* kom 1986.
- Förenkling av tidigare: bevisa att låg nivå inte kan härleda med 100 % säkerhet vad som händer på hög.
- Även om det går att se är det oförståeligt.
- Ett exempel på tillämpningsområde är ett nätverk med datorer med både hög och låg säkerhetsklassning.

Alternativa modeller

- *Type enforcement (TE)* tilldelar *domäner* för subjekt och *typer* för objekt.
- Därefter skapas en matris som specificerar tillåtna domän–domän- respektive domän–typ-kombinationer.
- Utökades till *Domain and Type Enforcement (DTE)*.
- Ger ett komplext språk att specificera policyer.

Alternativa modeller

- Rollbaserad åtkomstkontroll (*role-based access control, RBAC*) har sitt ursprung i bankvärlden.
- Baseras på användarens funktion som den utför snarare än en given användare.
- Det är skillnad på ”Daniel läraren” och ”Daniel studenten”.
- Men inte skillnad på ”Daniel läraren” och ”Lennart läraren”.
- Mina rättigheter kan således begränsas beroende på vad jag gör: inte installera program när jag läser e-post – och alltså skydda mot sabotageprogram.
- Kan då hantera både konfidentialitet och integritet.
- Detta implementeras i Linux genom TE och DTE.

Alternativa modeller

- Virtualisering är ett sätt att implementera olika nivåer och separera dem.
- NSA implementerade NetTop: en modifierad version av VMware.
- Linux som bassystem med Windows som virtuella maskiner.
- Anställda fick datorer som såg ut som Windows.
- Säkerhetsfolket fick hög säkerhet med separerade säkerhetsnivåer.
- Finns dock problem: Hur vet du vilken virtuell maskin som mikrofonen är ansluten till, hemlig nivå eller ej sekretessbelagd?

Översikt

Hemliga kanaler

Vad händer om jag skriver till en fil som redan finns på högre konfidentialitetsnivå?

Hemliga kanaler
NRL-pump

- Används för att begränsa bandbredden för hemliga kanaler.

Hemliga kanaler
Logistiksystem

- Ett militärlager med hemlig utrustning.
- En logistiker som inte har behörighet för hemlig, vad ska denne se?

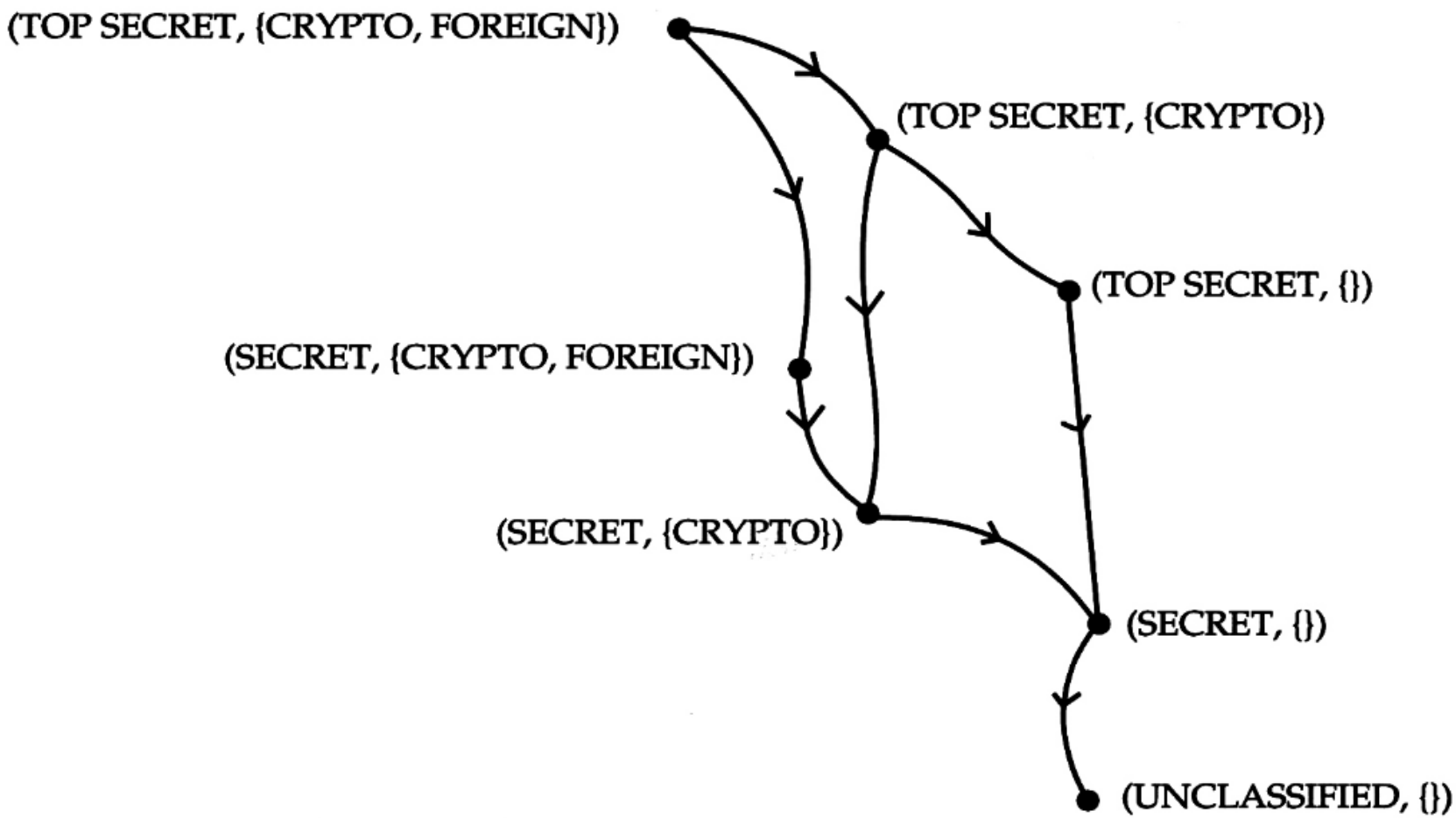
Översikt

Privacy is a transient notion. It started when people stopped believing that God could see everything and stopped when governments realised there was a vacancy to be filled.

Roger Needham

Översikt

Gittermodellen (lattice model)



Figur : Exempel på gittermodellen, idén är att BLP bara behöver en partiell ordning.

Översikt

Kinesiska muren-modellen

- Utvecklades av Brewer och Nash.
- Har sitt ursprung hos bankerna.
- *Separation of duty*: en användare får utföra A eller B, men inte båda.
- En systemadministratör får göra allt i ett system, men loggarna finns hos någon annan systemadministratör.

Kinesiska muren-modellen

Kinesiska muren

Låt c beteckna en resurs, $y(c)$ är c:s ägare och $x(c)$ är dess intressekonfliktklass. Då kan Kinesiska muren uttryckas enligt BLP som följande:

Simple security property Ett subjekt s har tillgång till c om och endast om för alla c' som s kan *läsa från* gäller $y(c) \notin x(c')$ eller $y(c) = y(c')$.

***-property** Ett subjekt s kan skriva till c om och endast om s inte kan läsa något c' sådant att $x(c') \neq \emptyset$ och $y(c) \neq y(c')$.

Översikt

BMA-modellen I

- Varje patientjournal har en åtkomstkontrollista (*access control list*, ACL) med alla som får läsa och skriva till journalen.
- För att komma åt journal:
  - En läkare får öppna journalen med sig själv och patienten på ACL:en.
  - Vid remiss, en läkare får öppna journalen med sig själv, patienten och remitterande läkare på ACL:en.
- Ägare: en läkare är ansvarig och kontrollerar ACL.
- Notifiering: alla förändringar av ACL notifieras till och godkänns av patienten.
- Beständighet: ingen kan ta bort data inom en förutbestämd tidsperiod.
- Loggning: all åtkomst till journalen noteras i den med subjektets identitet, tid och datum.

BMA-modellen II

- Informationsflöde: information från journal A får föras över till journal B om och endast om B:s ACL är en del av A:s.
- Sammanställningskontroll: patienter ska få en särskild notifiering om någon person med tillgång till en stor mängd patientjournaler föreslås läggas till ACL:en.
- Trusted computing base: datorsystem som hanterar patientjournaler ska påtvinga dessa principer.

Översikt

Inferenskontroll

- Att avanonymisera statistik: Vad är medelbetyget för alla kvinnliga studenter på Nätverksdriftsprogrammet i åk 1?
- Om det inte går: Vad är medelbetyget för alla studenter på Nätverksdriftsprogrammet, och vad är medelbetyget för alla manliga studenter på Nätverksdriftsprogrammet?
  - Nu kan jag beräkna medelbetyget för våra kvinnliga deltagare.

Referenser I

[And08] Ross J. Anderson. *Security engineering : a guide to building dependable distributed systems*. Wiley, Indianapolis, IN, 2 utgåvan, 2008.