Användningen av datorer har ökat mycket i försvaret. De är betydelsefulla och nödvändiga på de olika arbetsplatserna.

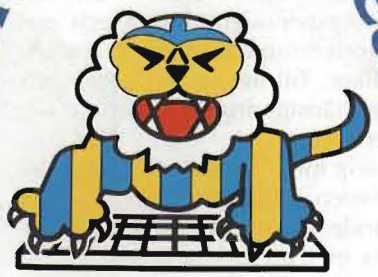
Dagens datasystem utvecklades med tanke på att de skulle vara lätta att använda och administrera. Man skapade mycket tillgängliga ADB-system. Nackdelen är att en obehörig ges stora möjligheter att läsa, manipulera och förstöra information.

Kraven på inbyggd säkerhet i datorerna har under årens lopp skärpts. Man uppmärksammar systemens sårbarhet och utvecklingen går mot mer skyddade system. Det finns ett extra stort behov av säkerhet i de "blandade miljöer" som finns inom försvaret, d v s i miljöer där hemligt och öppet material förekommer i samma datorsystem. Försvaret utarbetar en helhetslösning (säkerhetskoncept) som ökar säkerheten i försvarets vanligaste operativsystem – UNIX.

Denna artikel belyser försvarets säkerhetskoncept för UNIX-datorer, vilka skall fungera i såväl fred, kris som krig.

Av
Danuta Engstedt
Försvarsmedia

Högre säkerhet i försvarets UNIX-datorer



Projekt SÄKKO -90. – Inom försvaret bedrivs projektet ***Säkerhetskoncept 90 (SÄKKO -90)*** på uppdrag av ÖB. Projektet består av en projektgrupp med projektledare överstelöjtnant Carl-Adam Lewenhaupt (Ast/LI). I projektet samverkar flera myndigheter: Försvarets Materielvrk (FMV), försvarsstaben (Fst/Op 3), FörsvarsData, Försvarsmedia, Underröttelse- & säkerhetskontoret (USK) samt ÖB. Projektgruppen samordnar arbetet med att införa ökad säkerhet i försvarets UNIX-datorer.

Ett led i detta arbete är att installera SV/MLS *(System V/Multi Level Security)* på UNIX-datorerna. SV/MLS är en produkt[1] som innehåller ett antal skyddsfunktioner, vilket ökar säkerheten framför allt i försvarets "blandade miljöer".

Efter en utvärdering (FMV) har man funnit, att SV/MLS uppfyller de krav försvaret ställer på ett **säkert datorsystem**. Man har utnyttjat bedömningskriterierna för säkerhet i datorer som definierats av det amerikanska försvaret för amerikanska myndigheter. De är samlade i "The Orange Book"[2] som hittills har varit vägledande för datasäkerhet även i Europa. Det pågår dock arbete med att utveckla europeiska säkerhetsmodeller.

I "The Orange Book" definieras sju säkerhetsnivåer fördelade på fyra grupper[3] mot vilka ett system kan utvärderas. Varje nivå innehåller sina egna och underliggande nivåers mekanismer. SV/MLS uppfyller *nivå B1*.

1) AT&T har utvecklat operativsystem UNIX System V/MLS.
2) Department of Defence Trusted Computer System Evaluation Criteria. Bokens omslag är orange, därav "The Orange Book".
3) Nivå A1 – verifierat skydd, B1-B3 – reglerat skydd. C1–C2 – individuellt kontrollerat skydd, D – utvärderade system som inte uppfyller krav A1-C2.

Målet med införande av SV/MLS

SV/MLS möjliggör att man med tillfredsställande säkerhet kan hantera öppet och hemligt material i samma UNIX-datorsystem. SV/MLS ger dessutom en generell förbättring av informationsskyddet i datorerna utan att förlora den flexibilitet som kännetecknar ett öppet system.

Målet är att skapa ett användarvänligt system i vilket information kan lagras och bearbetas utan risk för obehörigt intrång eller insyn. SV/MLS mekanismer skyddar på så sätt att endast behörig får tillgång till den information som behövs i tjänsten.

Viktiga fakta om MLS

Skillnaden mellan ett traditionellt UNIX-system och UNIX med MLS skall för användaren inte upplevas som särskilt stor. De stora förändringarna ligger i systemets kärna. – Nedan följer en schematisk beskrivning av MLS och dess grundläggande funktioner.

I SV/MLS klassificeras information enligt:

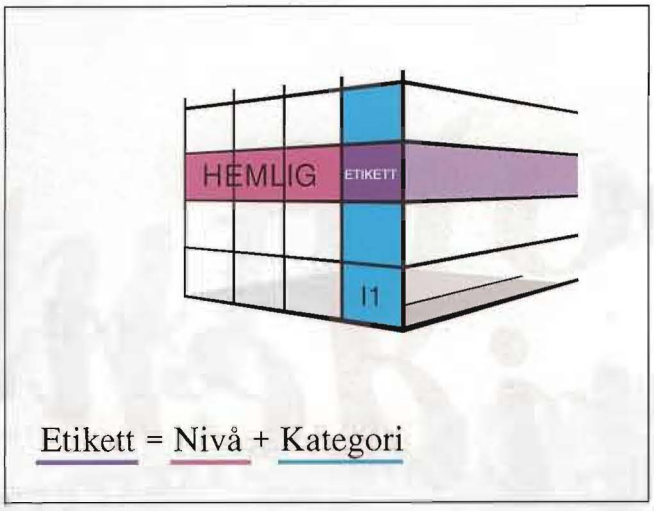
- ▶ Sekretessnivåer (sekretessgrad).
- ▶ Kategorier (verksamhet/tjänstegren).
- ▶ Grupp.

Sekretessnivå. – Om vi tänker oss MLS som en tredimensionell kub (**bild 1**), placerar användaren informationen på olika **sekretessnivåer**. 256 sådana nivåer är möjliga. Indelningen kan förfinas, men grunden är: Öppen, Hemlig, Kvalificerat hemlig och Kvalificerat hemligt material i sammanställd form.

Systemet förhindrar all otillåten kommunikation mellan olika nivåer. – **Exempel:** En användare som arbetar på en viss nivå, t ex Öppen, kan inte läsa ett dokument på högre nivå, t ex Hemlig. På motsvarande sätt kan den användare som arbetar på högre nivå, t ex Hemlig, inte skapa/förändra dokument på lägre nivå.

Dessa grundläggande regler förhindrar effektivt att sekretssbelagd information "smygvägen", t ex genom

Bild 1



inkopiering till lägre nivå, blir tillgänglig för en obehörig grupp användare. Systemprogram och betrodda applikationsprogram lagras på lägsta nivå, vilket gör att de inte kan manipuleras av användaren.

Kategori. – Informationen delas in i kategorier. 1024 sådana är möjliga. Försvaret utarbetar en försvarsgemensam kategoriindelning (KMÄ[4]) som klassificerar information enligt verksamhetsområden. Informationen behöver dock inte tillhöra någon kategori.

4) KMÄ står för Klassifikationssystem för militära ärenden och utarbetas av Fst/Op 3.

Grupp. – Användare kan delas in i **grupper**, t ex ADM för "administrativa enheten".

Etikett. – Kombinationen sekretessnivå och kategori kallas **etikett**. Man säger att etikett = sekretessnivå + kategori. **(Bild 1.)**

Privilegium. – Begreppet **privilegium** är mycket centralt i SV/MLS eftersom:

- Informationen tillhör ett privilegium.
- Användaren arbetar inom ett privilegium.
- Kringutrustning (terminal, bandutrustning, skrivare m m) kan tillhöra ett privilegium.

Användaren arbetar inom ett arbetsområde som benämns privilegium. Privilegium = etikett + grupp. I vår ovannämnda kub får privilegiet formen av en stapel. **(Bild 2.)**

Privilegiet styr användarens tillgång till information.

Behörighet. – Användaren får en **behörighet** och arbetar inom sitt privilegium. Han kan läsa i dokument inom *sitt* privilegium och även i de dokument som har lägre sekretessnivå inom den kategori där han arbetar.

Åtkomstkontroll. – Ett traditionellt UNIX-system har endast en *användarstyrd* åtkomstkontroll (dvs att den som har skapat ett dokument kan besluta om vem som skall ha tillgång till det). I SV/MLS är åtkomstkontrollen i huvudsak *regelstyrd*. Den användarstyrda åtkomstkontrollen finns dock kvar.

SV/MLS regelstyrda åtkomstkontroll är baserad på etikett och privilegium. Användaren kontrolleras obligatoriskt genom att all inloggning sker i *eget namn* – dvs inloggning kan inte ske anonymt genom t ex "root". Dessutom registreras all rörelse i systemet och alla inloggningsförsök. Systemet genererar självt lösenord för att undvika alltför "olämpliga" val och byter obligatoriskt lösenord efter viss tid.

All behörighet till information begränsas. På motsvarande sätt styr SV/MLS all åtkomst till kringutrustning för att undvika en svag länk i systemet. Vid utskrift märks alla dokument med sin säkerhetsnivå.

Införandet av MLS

SV/MLS kommer att installeras med början under hösten 1991. För närvarande avslutas en försöksverksamhet vid tre myndigheter, som skall ge riktlinjer och erfarenheter för den vidare spridningen.

SV/MLS ger en väsentlig förstärkning av informationsskyddet i UNIX, men ger inte ensam full säkerhet. Säkerhetsskyddet för information i datorer måste kombineras med de traditionella säkerhetsskyddsfunktionerna (bl a tillträdesskydd, infiltrationsskydd, administrativa regler och utbildning). Det är också viktigt att föreskrifter för hantering av datamedia och skydd mot röjande signaler (RÖS) följs. Först då kan man få ett heltäckande skydd av myndighetens datorbearbetade information.

SV/MLS kommer att beröra all personal som arbetar med UNIX-datorer och alla chefer som har dessa i sin organisation. Införandet av SV/MLS kommer även att ställa ökade krav på systemadministratörerna. FörsvarsData ansvarar för att ta fram ett nytt stödsystem och en handbok för systemadministratörer samt för utbildning av all berörd personal.

För att underlätta installation och användning av SV/MLS bygger FörsvarsData upp stödfunktioner inom sina regionala kontor (kundcentra). ■

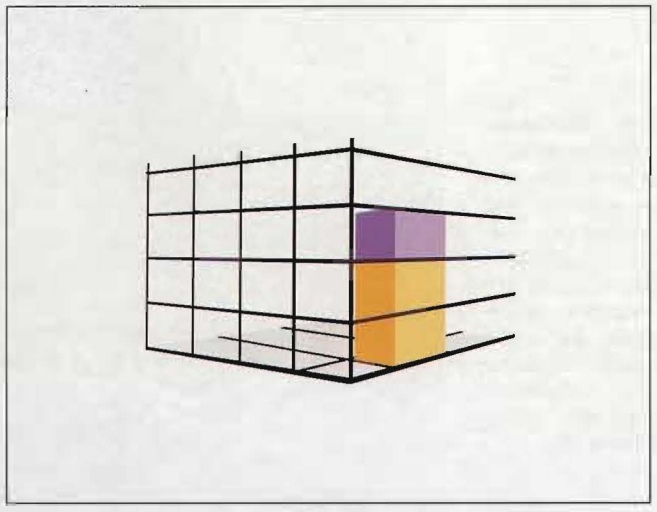


Bild 2

FV utökar skyddet än mer

– MLS (Multi Level Security) kommer att ge en väsentlig förstärkning av informationsskyddet i UNIX. Detta säkerhetssystem ger emellertid inte ensam full säkerhet, säger överstelöjtnant GÖRAN BRAUER (chef för flygstabens Projekt LI) då FV-Nytt ber honom kommentera ÖB:s datorsäkerhetssatning.

– Detta är viktigt att notera i samband med en eventuell driftsättning. CFV avvaktar nu resultatet av de prov som genomförs och den "prislapp", som införandet av MLS kommer att ge upphov till.

– Inom LI FV pågår arbete med att komplettera säkerhetsskyddet med moderna behörighetskontrollsystem (BKS), utbyggnad av lokala opofibernät (LAN), krypterad kommunikation m m.

– För LI FV måste arbetet fortsätta mot att nå högre säkerhet i systemen för att möjliggöra hanteringen av kvalhemlig (KH) information blandat med öppen och hemlig.

– Därför ser FV fram emot det fortsatta arbetet inom "SÄKKO 95". Ett projekt som CFV, på ÖB:s uppdrag, är beredd att driva inom ramen för projekt LI FV, avslutar Göran Brauer. ■