

Intels CDSA: Sikkerhet i ordnede former?

Sikkerhet forblir en tematisk gjenganger her i Mellvik-Rapporten, men aldri før har Intel vært nevnt i en slik sammenheng – verken som teknologi- eller produktleverandør. Hva er årsaken til at chip-giganten nå stikker nese – og pengesekk – inn på nok et område?

Det er riktignok lenge siden Intel utelukkende konsentrerte seg om mikroprosessorer og andre halvleder-komponenter. Spennvidden er blitt tilstrekkelig stor til at amerikanske myndigheter nå kikker selskapet i kortene for å bekrefte eller avkrefte mistanker om brudd på den berømte *antitrust*-lovgivningen: Fra prosessorer og minnebrikker til nettverksutstyr og ferdige hovedkort for PCer, fra industrielle systemer til Internett-tjenester og programvareutvikling.

Å tekkes markedet

I dette perspektivet er interessen for sikkerhet mindre overraskende. Selskapets viktigste inntektskilde er fortsatt prosessorer og komponenter til PCer, enkeltvis eller ferdig sammensatte. For å opprettholde og videreutvikle dette markedet, er det nødvendig å gripe fatt i de utfordringene som finnes – og som blir satt fokus på fra markedets side.

Sikkerhet og sikring befinner seg midt i oppmerksomhetens sentrum. Markedet forlanger sikrere og mer stabile produkter – og er åpenbart villig til å betale for forbedringene. Dersom Intel kan bidra til å gjøre PC-plattformen bedre skikket til å dekke markedets krav og behov, er det åpenbart en investering i egen fremtid.

Som sagt så gjort: CDSA (*Common Data Security Architecture*) er blitt til nettopp ut fra en slik tankegang. Sikkerhet er en akseptert nødvendighet på system- og nettverksnivå, og Intel er tjent med at selskapets komponenter generelt og PC-plattformen spesielt, forblir sentrale elementer i både klienter og tjenere. Dermed er årsaken til at selskapet konsentrerer seg om sikkerhet på applikasjonsnivå, gitt: All sikkerhet krever ressurser, og for Intel er det ønskelig at ressursene konsumeres på deres plattformer (tjenere og klienter) i stedet for på nettverksnivå, der selskapets markedsandel er beskjedent.

Det er ingen grunn til å kritisere dette – tvert imot er det positivt at Intel tar et slikt initiativ, som i beste fall kan føre til nyttige og viktige resultater, og i verste fall gi verdifulle erfaringer. Samtidig er det alltid enklere å evaluere både argumenter og veivalg når vi vet hvor motivasjonen kommer fra.

Målsetting

Intels utviklere oppsummerer målsettingene for CDSA slik:

- ✓ Definere en åpen, plattformuavhengig infrastruktur for sikkerhet på applikasjonsnivå.

- ✓ Etablere støtte for kontroll, styring og bruk av grunnleggende sikkerhetslementer: Digitale sertifikater, kryptering, autentisering, autorisering, integritet.
- ✓ Sørge for fleksibilitet og skalerbarhet som ikke bare dekker eksisterende teknologier, men også gir *plug-and-play* funksjonalitet og lett kan utvides med nye tjenester.

Dette høres fint – og teknisk – ut, og er nettopp det. I avsnittet nedenfor skal vi oversette det hele til forståelig prosa, men la oss først se litt mer på målsettinger og bakgrunn:

Det er ingen tilfeldighet at Intel fikk følge av de store på programvarefronten umiddelbart etter at ideen og planene ble lansert i slutten av 1997: IBM, Compaq, Bull, Lotus, Security Dynamics, AT&T og HP. Tiden var åpenbart moden for en standard-arkitektur for sikring på applikasjonsnivå. Samtidig ser vi av de opprinnelige dokumentene fra Intel, at intensjonen var å knytte CDSA tett til selskapets komponenter, blant annet ved å integrere enkelte funksjoner i prosessorer og støttekretser.

Ett av elementene var innføringen av serienummer i prosessorene, som selskapet introduserte i 1999 (Pentium III). Målsettingen var blant annet å kunne spore systemer og å sørge for sikker identifikasjon (autentisering). Overraskende for Intel skapte imidlertid ideen et ramaskrik i markedet: Slike muligheter er like lette å misbruke som å utnytte, og de negative sidene var etter markedets oppfatning større enn de positive. Reaksjonene fikk Intel til å gå langt mer stille i dørene, og serienummeret ble en opsjon som kan slås av og på av brukeren i alle nyere prosessorer.

En annen motivasjon var at både Microsoft og sikkerhetsselskapet RSA Data Security hadde lansert sine egne løsninger på samme problem, og Intel var bekymret for at disse skulle bli fordelaktige for alternative arkitekturer. For å gardere seg, sørget de for at både RSAs Security Framework og Microsofts CAPI (Crypto API) ble tatt rimelig hensyn til på alle nivåer i CDSA.

CDSA – Common Data Security Architecture

Utfordringen Intel griper fatt i, er altså sikkerhet på applikasjonsnivå. I tallrike diskusjoner omkring sikkerhet i tidligere artikler (se for eksempel Mellvik-Rapporten nr. 79 side 7), har vi konstatert at mens sikkerhet på dette nivå er ønskelig, er det vanskelig å få til – fordi:

- ✓ Applikasjoner må omskrives med tanke på sikkerhet
- ✓ Oppgaven er komplisert og omfattende
- ✓ Standarder, mekanismer og verktøy for utvikling, styring og kontroll mangler
- ✓ Utviklingsmiljøene har få incentiver for å gripe fatt i utfordringen, blant annet fordi markedet ikke spør etter – eller forlanger – applikasjonssikkerhet

- ✓ Sikkerhet har i mange miljøer vært oppfattet som en uttidig forstyrrelse, i stedet for en nødvendighet

Derfor har innsatsen med hensyn til sikringsmekanismer vært konsentrert om system- og nettverksnivå, hvilket gir raskere resultater, er enklere å få til, og kan gjøres relativt usynlig for brukerne.

Utfordringene knyttet til applikasjonssikkerhet har ikke forandret seg vesentlig de siste årene, men innstillingen til dem er en annen i dag:

- ✓ Sikkerhet blir tatt på alvor på en helt annen måte enn tidligere.
- ✓ At gamle applikasjoner vanskelig kan sikres på applikasjonsnivå, er i realiteten en dårlig unnskyldning for ikke å gjøre noe som helst. Den eneste måten å bedre forholdet på, er å sørge for at standardene og hjelpemidlene finnes. Først da kan progresjonen begynne.
- ✓ *Embedded systems* (industrielle systemer), *appliances* (nettapparater), tynne klienter, PDAer: En lang rekke 'nye' utstyrskategorier gjør at gamle oppfatninger ikke lenger gjelder. For nettapparater med én spesifikk funksjon, kan det være vel så effektivt å gi applikasjonen sikring som å legge den i et mager OS.¹⁴
- ✓ Sikkerhet kan aldri skapes av én applikasjon eller én løsning alene. Det er først når alle involverte elementer – klienter, operativsystemer, autentiseringsmekanismer, tjenere og applikasjoner kan spille sammen, at sikkerheten tar et skikkelig sprang i riktig retning.

Det er i dette scenario CDSA har ambisjoner om å spille en rolle. Tankene Intel måtte ha hatt om å knytte teknologien til egne produkter, er forlengst borte. CDSA har gått gjennom tre revisjoner (og befinner seg på versjonsnummer 3.0), den har fått prøve seg i praksis i en del sammenhenger, og sist, men ikke minst: Det finnes en pålitelig, lisensfri – *open source* – referanse-implementasjon tilgjengelig fra Intel. Videre er både referanse-implementasjon og konkrete produkter tilpasset og testet på en rekke ulike plattformer. Dette gjør at CDSA omsider fremstår som et attraktivt og praktisk anvendbart verktøy for etablering av god sikkerhet på applikasjonsnivå uten leverandørbinding.

Samspill i fokus

Det aller viktigste elementet i ligningen er samspill. For å kunne ta vare på sikkerheten, må løsningene ha tilgang til tjenester som implementerer de ulike mekanismene – autentisering, autorisering, kryptering, kontroll av signaturer og sertifikater og så videre. Slike tjenester kan ikke bygges inn i hver enkelt applikasjon – da det ville bli for komplisert og tidkrevende, og dessuten tungvint på grensen til det uanvendelige.

¹⁴ Den optimale løsningen er et effektivt samspill mellom applikasjon, OS og underliggende hardware, hvilket er karakteristisk for trenden i dag, med eller uten CDSA.

Først når tjenestene eksisterer i omgivelsene og blir gjort tilgjengelige via standard grensesnitt, er det mulig å realisere slik grad av sikring. Vi kan som eksempel tenke oss noe så alminnelig som autentisering: Tradisjonelle passord er ikke lenger tilstrekkelige, og blir erstattet av biometriske mekanismer: Retina- (øye-)skannere, fingerskannere og stemmegjenkjenning. I én og samme organisasjon kan det være behov for alle tre, kanskje enda flere, for ulike formål. Å integrere dem i organisasjonens systemer er imidlertid praktisk talt umulig uten standarder for grensesnitt og dataformater. Historisk har den eneste måten å utnytte slike identifikasjonsmekanismer på, vært å bygge dem inn i løsningene enkeltvis: Databasesystemet bruker en fingerskanner, laboratoriesystemet en øyeskanner, personalsystemet et SMART-kort og så videre. CDSA gjør det mulig å sende dette kaoset til de evige jaktmarker.

Mellomvare – MIDDLEWARE

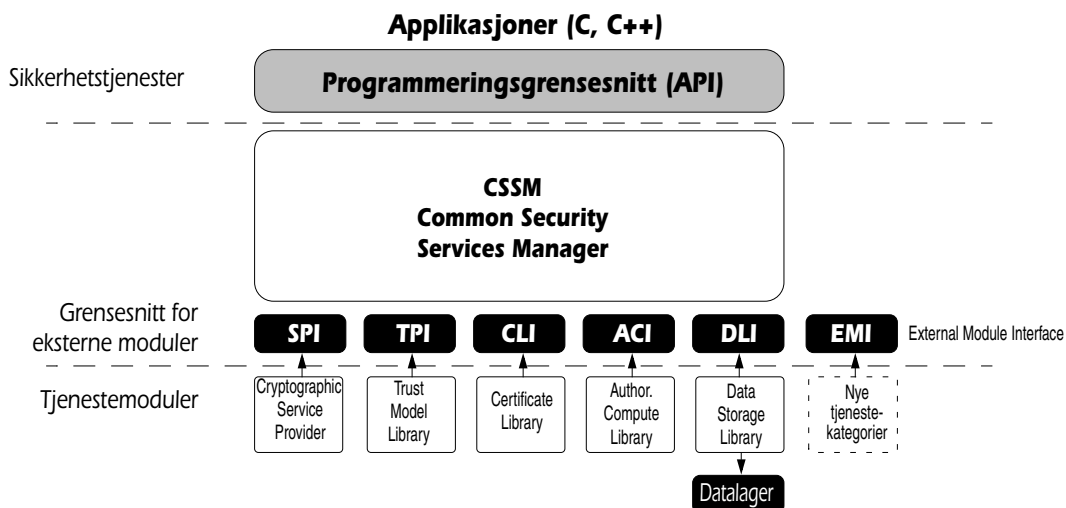
CDSA er kort og godt mellomvare, limet som sørger for å holde programmer, løsninger og utstyr fra ulike leverandører og på ulike nivåer, sammen. Arkitekturen definerer fem grunnleggende sikkerhetstjenester som gjøres tilgjengelige for 'klientene' – det være seg applikasjoner, systemer, biometrisk sikringsutstyr eller annet. Disse tjenestene kan kort beskrives slik:

- ✓ CSP, *Cryptographic Service Provider* – tar vare på alle slags operasjoner knyttet til kryptering, fra kryptering av datastrømmer (for eksempel filer eller transaksjoner) til kontroll eller generering av digitale signaturer. Her lagres personlige eller private nøkler som brukes ved kryptering og dekryptering.
- ✓ TP, *Trust Policy* – implementerer regelverk fra myndigheter eller organisasjonen selv, og definerer graderingen av ulike tjenester, dokumenter og systemer.
- ✓ AC, *Authorization Computation* – tjenesten som setter sammen en persons 'akkreditiver' og annen informasjon, som til sammen avgjør om en forespørsel eller operasjon på et gitt objekt er tillatt eller ikke.
- ✓ CL, *Certificate Library* – et lokalt register over digitale sertifikater – fremtidens identifikasjonspapirer. Tjenesten kommuniserer med tilsvarende eksterne tjenester, som etter hvert skal dekke alle nettbrukere over hele verden¹⁵. En viktig del av tjenesten er naturligvis å vite hvilke sertifikater som er inndratt og dermed ugyldiggjort.
- ✓ DL, *Data Library* – et pålitelig lager (bibliotek) for alle slags sikkerhets-relaterte objekter; sertifikater, nøkler, policy-objekter, person-objekter og mye mer. Hvordan denne

¹⁵ Slike sertifikater representerer fortsatt en gigantisk utfordring i større målestokk, fordi det enda ikke er etablert internasjonale regler og instanser for utstedelse og kontroll av dem. Inntil videre er derfor deres nytteverdi begrenset til å gjelde innenfor domener vi selv har kontroll over eller full tillit til. Det arbeides i flere internasjonale fora, blant annet EU og FN, med å rette på dette forholdet.

lagringen foregår er mindre viktig, det er funksjonen og påliteligheten som betyr noe.

Tjenestene styres av en modul som kalles CSSM, *Common Security Services Manager*, og sammenhengen mellom tjenester og klienter (brukerprogrammer) kan illustreres som vist i figur 4.



Figur 4 CDSA består av et rammeverk og fem hovedmoduler. Like viktig er det at åpningen for nye elementer som nødvendigvis må komme i fremtiden, finnes.

Status

Sammen med blant andre IBM har Intel investert over 20 millioner USD i utvikling, testing og markedsføring av CDSA, hvilket blant annet har ført til at referanse-implementasjoner (klient og/eller tjener) ved inngangen til 2001 dekker følgende plattformer: Windows, Macintosh, Unix (flere varianter), og Linux. Videre har standarden, helt siden den ble introdusert i 1997, vært støttet av The Open Group, som eier, videreutvikler og foretar produktsertifiseringer på en rekke områder innen IT, og spesielt på Unix-siden.¹⁶

Hvor er resultatene?

Med et slikt utgangspunkt, en slik innsats og ikke minst gitt situasjonen i markedet, hva årsaken være til at vi knapt har hørt om CDSA i løpet av disse tre årene? Har innsatsen vært forgjeves? Finnes resultatene? Er de ganske enkelt usynlige?

Usynlige av natur er de i alle fall ikke: Dersom CDSA hadde hatt stor utbredelse, ville situasjonen i markedet sett ganske annerledes ut enn den gjør i dag. Det faktiske forhold er at modningen hos markedet generelt og hos programvare-leverandørene spesielt, har tatt vesentlig lengre tid enn noen – spesielt hos Intel og IBM – hadde forestilt seg. Spesielt førte aktiviteten og hysteriet rundt årtusenskiftet til en full-

¹⁶ The Open Group er blant annet eier av varemerket 'Unix'.

stendig defokusering av de sikkerhetsmessige problemstillingene. Og sist, men ikke minst var lisensieringen av CDSA problematisk inntil Intel på vårparten 2000 bestemte seg for at *Open Source* var riktig medisin for å få fart i sakene. Først da kom flere av aktørene på Linux-siden inn på banen. Dessuten ga 'åpningen' i seg selv betydelig publisitet.

Den beskjedne utbredelsen betyr imidlertid ikke at innsatsen har vært forgjeves eller at resultatene mangler helt. CDSA er tatt i bruk av HP (HP-UX), i en rekke IBM-produkter – spesielt på stormaskiner, Apple Computer, Motorola, Netscape, og relativt nylig Caldera (OpenLinux). Ekspertene hos IDC (International Data Corp.) mener at slakk markedsføring er en viktig årsak til dagens 'underutnyttelse', og forventer at Linux og frigivelsen av kildekoden til referanse-implementasjonen vil gi utviklingen videre et kraftig dytt bak.

Konklusjon

Ironien i det hele er at markedet er overmodent for den teknologien CDSA representerer. Praktisk talt alle slags løsninger – fra ERP-systemer til nettlesere, fra industrielle systemer til PDAer – har et akutt behov for bedre sikringsmekanismer på alle nivåer. Videre ser vi av produkttilfanget på markedet at blant annet biometrisk identifikasjonsutstyr er kommet tilstrekkelig langt ned i pris til å få bred interesse. Sammen med etablering av nasjonale og internasjonale myndigheter for utstedelse og administrasjon av digitale sertifikater (identifikasjonspapirer), vil slikt utstyr sørge for en sikkerhetsmessig revolusjon. I snart 40 år har tradisjonelle passord og 'pass-setninger' vært vårt viktigste verktøy for identifikasjon av enkeltindivider, og i over halvparten av perioden har de fleste av oss vært sørgelig klar over dets utilstrekkelighet.

Årsaken til at IDC tror Linux vil akselerere utviklingen og akseptansen av CDSA, er at hele miljøet er langt mer bevisst opptatt av sikkerhet og sikring enn tradisjonelle IT-miljøer. Når Linux-plattformen kan demonstrere sikrere virksomhetskritiske løsninger enn NT, W2000 og Unix, sier det seg selv at en del leverandører vil få fart i sakene.

For oss som befinner oss på kundesiden, er det først og fremst viktig å vite at teknologien ikke bare finnes, men sågar kan kalles moden. Med denne kunnskapen kan vi slå tilbake de altfor vanlige argumentene fra leverandørsiden om at "de også gjerne skulle hatt bedre sikkerhet, men teknologien/standardene finnes ikke". Konkurransепress er et godt incentiv til forbedringer, men ingen ting slår å få det rett fra kundene. ■