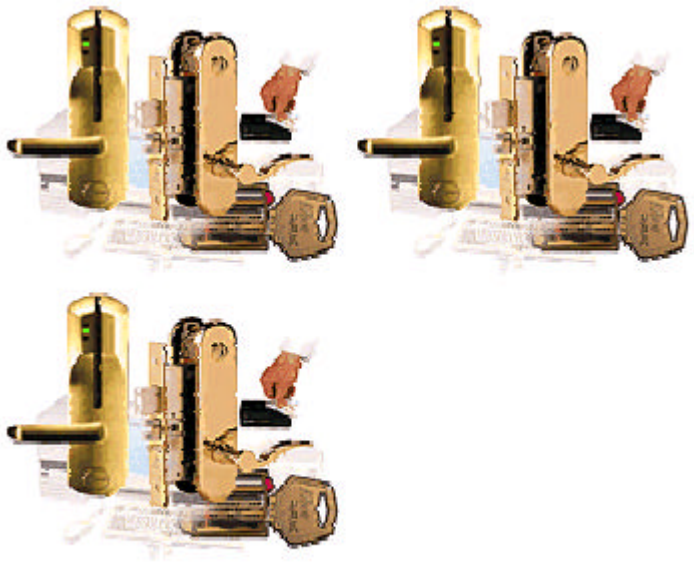
Betraktninger omkring sikkerhet for mobil IT-bruk i DNV



Jan Roger Sandbakken

September 1998

IMEDIA/09/98

Norsk Regnesentral
ANVENDT DATAFORSKNING

NR-notat/NR Note

Tittel/Title:
Betraktninger omkring sikkerhet for mobil IT-bruk i DNV

Dato/Date: September
År/Year: 1998
Notat nr: IMEDIA/09/98
Note no:

Forfatter/Author:
Jan Roger Sandbakken

Sammendrag/Abstract:

Emneord/Keywords: Sikkerhet, mobilt arbeid

Tilgjengelighet/Availability: Åpen/open

Prosjektnr./Project no.: 28007

Satsningsfelt/Research field: Mobil informatikk

Antall sider/No. of pages: 9

Norsk Regnesentral / Norwegian Computing Center
Gaustadalléen 23, Postboks 114 Blindern, 0314 Oslo, Norway
Telefon 22 85 25 00, telefax 22 69 76 60

Innhold

Innledning

Mobilt arbeid vil sette særlige krav til sikkerhet. De mest åpenbare sikkerhetsutfordringene ligger i at data ? som tidligere typisk har vært kommunisert, prosessert eller lagret internt i en organisasjon ? vil kunne bli utsatt for autorisert modifikasjon eller innsyn når de behandles eller overføres eksternt i en mobil arbeidssituasjon. Videre vil tilknytningsmulighetene mobile medarbeidere har til hjemmeorganisasjonen, også kunne åpne opp nye angrepskanaler inn i organisasjonens interne nett ? med mindre man tar nødvendige forholdsregler

Scenariene for mobilt arbeid, beskrevet i [IMEDIA/08/98], dekker ulike tilknytningsalternativer mellom mobil terminal og hjemmebase. I korthet vil en mobil medarbeider ute i felt kople seg til hjemmebasen etter behov fra sin mobile terminal. Flere kommunikasjonsprotokoller vil være aktuelle, og kanskje først og fremst de følgende:

- TCP/IP vha. PPP over en oppringt forbindelse
- TCP/IP direkte fra en kundes LAN
- WAP-familien av protokoller over GSM.

Det vil også være interessant benytte

- H.323 over IP.

Audio og særlig video krever riktignok en forbindelse med god kapasitet.

Medarbeideren vil både kunne være periodisk eller mer permanent tilknyttet. De ulike scenariene medfører også at prosesseringen og/eller lagringen av data kan skje i varierende grad lokalt i den mobile terminalen eller mer sentralt i hjemmebasen. Fleksibilitet vil være et viktig stikkord for systemløsningen.

Det begynner etterhvert å komme flere generelle og mer spesielle sikkerhetsløsninger som kan anvendes for mobilt arbeid. Det bør i dag være mulig å håndtere de fleste aktuelle nivåer av sikkerhet tilfredsstillende, forutsatt at man i tillegg til de tekniske aspektene er motivert for å gjennomføre nødvendige organisatorisk sikringstiltak. Vi skal la organisatoriske forhold knyttet til sikkerhet ligge i første omgang ? disse er nødvendigvis heller ikke unike for mobilt arbeid ? og fokusere på de rent tekniske sidene i dette kapittelet.

Mobile terminaler har i dag klare ressursbegrensninger i forhold til vanlige stasjonære arbeidsstasjoner, både med hensyn til prosesseringskraft, lagringskapasitet og støtte for utvidelseskort og ulike periferenheter. Det er en gjennomgående forutsetning at dette relative styrkeforholdet vil vedvare i overskuelig framtid. Dette vil påvirke vurderinger rundt valg av sikkerhetsløsning.

Vi skal gi en relativt kortfattet beskrivelse av typiske trusler og risikoer ved mobilt arbeid, samt vurdere de mest aktuelle generelle sikkerhetsløsninger og
-standarder i dette kapittelet. I tillegg vil vi liste og vurdere en del tilgjengelig kommersielle sikkerhetsprodukter som kan ha interesse.

Trusler og risikoer

Vi skal ikke her foreta en full risikoanalyse av mobilt arbeid. Vi vil diskutere litt generelt rundt hovedtruslene og deretter fokusere på de viktigste tiltaksområdene.

Hva og hvem som skal sikres

Det er tre typer aktører som må sikres i vår mobile arbeidssituasjon:

- Mobil terminal
- Hjemmebase
- Kunde

Sistnevnte er aktuell i de tilfeller medarbeideren arbeider på eller via en kundes nett. I tillegg må

- data som transmiteres

mellom disse beskyttes tilsvarende. Målsettingen er kort å sikre at data og andre ressurser ikke utsettes for misbruk av noen art eller for uautorisert innsyn; altså å sikre konfidensialitet, integritet og tilgjengelighet iht. en egnet og konkret sikkerhetspolicy.

For den mobile terminalen betyr dette at kun eieren, eller autoriserte brukere, skal ha tilgang til terminalen. Viktige elementer vil være tiltrodde mekanismer for pålogging samt for disk- eller filkryptering. Sistnevnte for å sikre data tilstrekkelig også hvis terminalen skulle komme på avveie.

Hjemmebasen vil være opptatt av å beskytte sitt nett, sine data og andre ressurser slik at det kun legitime brukere har tilgang til ressursene ? og kun til tjenester og data de har tilstrekkelig autorisasjon til å aksessere. I dette ligger det å ha kontroll med hva som slipper inn utenfra og hva som slippes ut innenfra. Beskyttelsesmekanismene vil her være mer omfattende og vil også avhenge av organisasjonens sikkerhetspolicy. Det kanskje viktigste punktet vil være å ha tilstrekkelig identifisering og autentisering (I&A) av de mobile medarbeiderne i bunn, og basere rettigheter med tilgang til data, tjenester og andre ressurser i systemet på dette.

Mht. en eventuell kunde er det viktig at den mobile terminalen er i stand til å operere uten at kundens ressurser tilsvarende risikerer å bli utsatt for misbruk eller uautorisert innsyn.

Hovedtrusler

Sikkerhetsrisikoene for denne typen systemer, som baserer seg på kommunikasjon over åpne linjer, er mye diskutert og vel kjente. Det viktigste er at uvedkommende her har anledning til å avlytte eller modifisere kommunikasjonen, og at de har elektronisk tilgang til endesystemene slik at de kan forsøke å bryte seg inn eller gjennomføre uliketilgjengelighetsangrep mot systemet. Karakteristisk for åpne nett er også at man generelt ikke har garanti for at data leveres korrekt til mottaker eller at data virkelig kommer fra en oppgitt kilde. Dette åpner for en rekke maskerade- og spoofing-angrep.

Vi vil også minne om at TCP/IP-sesjoner kan kapres av angripere. Dette betyr at en angriper kan overta en mobil medarbeiders forbindelse med hjemmebase, f eks. *etterkant* av en pålogging. Angrepet krever riktignok at angriperen sitter passende plassert i ruten mellom endepunktene, men er ellers fullt ut gjennomførbart med tilgjengelig programvare. Den eneste fullverdige beskyttelsen mot dette er kryptering eller signering av dataene.

Det er videre en betydelig risiko for at mobile terminaler kan bli stjålet, forlagt eller bli skadet. Dette krever egne sikringstiltak. Merk at angripere med fysisk tilgang til disken kan få fram både eksisterende data og data som er logisk eller fysisk slettet/overskrevet.

Man eksponerer seg ellers for et stort antall potensielle angripere i et åpent nett. I en kommersiell situasjon må man dessuten ikke glemme trusselen for mer målbevisste angrep fra konkurrenter, utro tjenere hos tjenestetilbydere eller andre. Disse kan ha mer ressurser tilgjengelig og kan utnytte spesiell kjennskap til bedriften i angrep.

Sikringstiltak

De sikringstiltak vi skal diskutere her er:

- Sikring av data under transmisjon mht. konfidensialitet og integritet
- I&A av mobile medarbeidere mot hjemmebase
- I&A og tilgangskontroll av medarbeider mot mobil terminal
- Disk- eller filkryptering i mobil terminal

Som der fremgår vil vi her *ikke* fokusere på tilgangskontrollen i hjemmebasen i full bredde, selv om dette er et sentralt punkt. Dette ville føre for langt og vil også avhenge sterkt av den tekniske løsningen. Hjemmebasen vil imidlertid ha en brannmurliknende løsning som et sentral element i sin tilgangskontroll, og vi skal komme litt inn på enkelte momenter av betydning for denne.

Vi skal videre si litt om:

- Autorisasjon av mobile medarbeidere i hjemmebasen
- Beskyttelse mot troyanske hester og andre former for ondsinnede programmer eller programoduler.

Det sistnevnte vil være viktig siden en mobil terminal i stor grad vil kunne ønske å laste ned og sette sammen program-moduler etter behov.

Vi skal ha i bakhodet at tiltak og løsninger også bør kunne samspille med kunder-systemer rent sikkerhetsmessig.

Vi skal generelt forutsette at hjemmebasen har sikret sitt interne nett, sine servere og databaser og andre ressurser tilstrekkelig.

Sikring av data under transmisjon

Konfidensialitet av data under transmisjon kan kun sikres vha. kryptering. Symmetrisk kryptering vil av effektivitetsgrunner være mest aktuell og flere algoritmer er aktuelle. Mht. fordeling av krypteringsnøkler har man i praksis to muligheter:

- Asymmetrisk nøkkelfordeling
  - *Man benytter hybride krypteringssystemer og baserer seg på par av offentlige/private brukernøkler og utveksler symmetrisk krypteringsnøkler etter behov ved anerkjente nøkkelutvekslingsalgoritmer*
- Symmetrisk nøkkelfordeling
  - *Man fordele ut par av symmetriske krypteringsnøkler til de som har behov for å kommunisere kryptert.*

Det førstnevnte krever at man utsteder offentlige nøkkelsertifikater til de mobile medarbeiderene. Det er sannsynligvis mest aktuelt at organisasjonen opererer en egen *Public Key Infrastructure* (PKI) og utgjør en egen sertifiseringsautoritet. En slik løsning skalerer brukbart. Det andre tilfellet krever at organisasjonen opererer et eget nøkkelfordelingssenter (KDC).

IPsec er et eksempel på en sikkerhetsprotokoll som kan basere seg på begge typer nøkkelfordeling.

Det er normalt enklest for vanlige bedrifter å benytte asymmetrisk nøkkelfordeling. Symmetrisk nøkkelfordeling benyttes tradisjonelt mest innen forsvar og diplomati. En mobil arbeidssituasjon kan imidlertid være velegnet også for en symmetrisk nøkkelfordeling. Mobile medarbeidere vil besøke hjemmebasen jevnlig og kan dermed enkelt få utdelt nye nøkler. Asymmetrisk teknologi har imidlertid fordelen av at muligheter for autentisering, signering og *non-repudiation* er direkte innebygd. Slik funksjonalitet vil være viktig i mobilt arbeid, hvilket vi skal komme noe tilbake til. Det vil potensielt også være mulig for en kunde å verifisere gyldighet av organisasjonens sertifikater, om nødvendig.

Det finnes flere anerkjente, sikre krypteringsalgoritmer å basere seg på. Et problem ligger imidlertid fortsatt i de amerikanske eksportrestriksjonene, som medfører redusert krypteringsstyrke i mye toneangivende programvare. Nøkkellengdebegrensingene på 40 bit (ved symmetrisk kryptering) og 512 bit (ved de vanligste algoritmene for asymmetrisk kryptering), gir i dag ikke lenger opphav til særlig sterk kryptering.

Integriteten av overførte data kan også sikres vha. kryptering, men i situasjoner der konfidensialitet ikke er påkrevet, løses dette enklest vha. kryptografisk beregnede hash-verdier. SHA og MD5 er eksempler på mye benyttede hash-algoritmer. Man vil også kunne ønske at dataene autentiseres. I det asymmetriske tilfellet løses dette enklest ved at partene signerer data. I et symmetrisk tilfelle vil man typisk inkludere krypteringsnøkkelen, eller data avledet av denne, i hash-beregningen. HMAC er et eksempel på det sistnevnte.

Det vil føre for langt å diskutere forskjellige algoritmer her. Men teknisk sett bør det være greit å sikre konfidensialitet og integritet over åpne linjer. Det kan imidlertid være visse begrensninger i en overgangsperiode som følge av eksportrestriksjoner, og man må også sørge for sikker nøkkelhåndtering og -fordeling med tilhørende infrastruktur.

Kryptering kan også utnyttes i tilgangskontrollen mot hjemmebasen, også selv om konfidensialitet ikke nødvendigvis er det primære. En brannmur vil kunne slippe gjennom krypterte eller signerte data i forvisning om at de vil bli forkastet om alt ikke er i orden. Kriterier for å tillatte eller avvise trafikk basert på kryptografiske attributter vil klart kunne oppnå veldig høy tiltro.

I&A av mobile medarbeidere mot hjemmebase

Som nevnt er det essensielt at mobile medarbeidere i felt identifiserer og autentiserer seg overfor hjemmebasen. Visse tjenester kan være åpne, men for å få tilgang til interne ressurser eller få utført bestemte oppgaver, kreves autorisasjon. Identiteten til den mobile medarbeideren må verifiseres, hvilket oftest skjer vha. en initiell pålogging. Til nå har man mye basert seg bruk av passord for autentisering, selv om det er vel kjent at dette er forbundet med risiko. Passord kan være lette å gjette for uvedkommende, de kan gis bort til andre, de kan bli skrevet ned, de kan glemmes for å nevne noe. Dårlig passorddisiplin er fortsatt sikkerhetsproblem nummer én og årsak til langt de fleste datatekniske innbrudd. Merk at selv når overførte passord skjules vha. hashing (eller for såvidt krypteres med en offentlig nøkkel) beskytter dette ikke mot ordliste-angrep med mindre man tar nødvendige forholdsregeler. Det finnes eksempler på sentrale sikkerhetsprodukter som har uteglemt dette. Tiden er i det hele tatt moden til å unngå å basere seg på passord-autentisering alene.

Bruk av engangspassord vha. passordkalkulatorer osv. er å foretrekke framfor tradisjonelle, memorerte passord. Under TCP/IP vil dette likevel ikke alltid være tilstrekkelig pga. den tidligere beskrevne truslen for sesjonsovertakelser.

Autentisering basert på kryptografiske atributter vil langt være å foretrekke. Som antydet synes bruk av sertifikater og offentlignøkkel-teknologi å være mest aktuelt. Dette kan utnyttes for

- autentisering av mobile medarbeidere
- signering av data, skripts, program-moduler eller annen kode
- utveksling av symmetriske trafikknøkler

Både sikkerhets- og funksjonalitetsmessig vil dette være å foretrekke. Flere av de sentrale og aktuelle sikkerhetsprotokollene baserer seg også på denne teknologien.

I&A og tilgangskontroll av medarbeider mot mobil terminal

Det er behov for en tilgangskontroll til den mobile terminalen. For å få tilgang til data og programmer i terminalen må medarbeieren identifisere og autentisere seg. Tilgangskontrollen må gripe tilstrekkelig dypt inn i hardware, slik at kontrollen ikke kan omgås f eks. ved å boote terminalen på spesiell måte. Videre må det være enlåse-funksjon i terminalen, slik at medarbeidere kan forlate terminalen midlertidig i beskyttet tilstand.

Tilgangen må basere seg på en verifisert identitet. Sidenautentiseringsdata i dette tilfellet ikke overføres eksternt, vil gode memorerte passord eller engangspassord kunne benyttes i dette tilfellet. Men som allerede argumentert for, peker bruk av sertifikater og offentlignøkkel-teknologi seg fordelaktig ut i autentiseringen mot hjemmebasen. Ved å basere tilgangen til terminalen på smartkort eller tilsvarende, kan man oppnå *både* støtte for denne teknologien og en tiltrodd lokal pålogging til

terminalen. Smartkortet lagrer private nøkler og kan også utføre nødvendige kryptografiske operasjoner. Og ved å basere terminalpåloggingen på smartkort, baserer man seg både noe medarbeideren *har* (smartkortet) og noe han *vet* (en tilhørende PIN-kode/ passordfrase), hvilket gir en sikkerhetsgevinst.

Et slikt smartkort hindrer også at nøkkelinfomasjon blir liggende ubeskyttet i terminalens memory eller disk, f eks. i cash eller virtuelt minne.

Merk at billige biometriske avlesningsenheter, vanligvis basert på fingeravtrykk, etterhvert er på vei inn i markedet. Disse kan installeres i vanlige mobile terminaler og kan være et gunstig supplement ved at man helt kan unngår bruk av PIN-koder og passordfraser.

Et hovedbudskap også her er at bruk av memorerte passord alene bør unngås.

Disk- og filkryptering i mobil terminal

Ved tap av terminalen vil ikke den diskuterte tilgangskontrollen være tilstrekkelig. Siden en angriper i et slikt tilfelle kan ta ut å inspisere disken direkte, vil den eneste beskyttelsen her være kryptering av diskdata.

Man kan kryptere diskdata på to nivåer:

- På fil-nivå
- På driver-nivå.

I det første tilfellet krypteres og dekrypteres filer separat. I det andre tilfellet opprettes en logisk disk der alle data krypteres og dekrypteres automatisk. Førstnevnte er enklere å implementere og kan være mer fleksibel ved at filer enkelt kan flyttes mellom ulike maskiner. En ulempe er at den er brukerstyrt og at man kan glemme å kryptere sensitiv informasjon. Informasjon kan dessuten lekke til disken via cash, virtuelt minne etc. Kryptering på driver-nivå er mer kompleks å implementere, men har fordelen av å virke mer skjult for brukeren. Alle data, også temporære data, vil bli beskyttet. En ulempe er imildetid avhengigheten løsningen har til bestemte drivere og system.

Disk- og filkryptering er vesensforskjellig fra kryptering av kommunikasjonsforbindelser. Lagrede krypterte data vil kunne bli lagret i lang tid, og man må sørge for å ha mulighet dekryptere data langt inn i fremtiden. Dette krever egne og gode nøkkelhåndteringsprosedyrer. I tillegg er det essensielt å velge krypteringsmodi som ikke er følsomme for enkeltebit-feil.

Det er aktuelt å vurdere former *key escrow* kryptering; dvs. at man har mulighet til å dekryptere data ved en master nøkkel dersom man ved et uhell skulle miste en dekrypteringsnøkkel.

I disk- og filkrypteringsverktøy avledes vanligvis en symmetrisk krypteringsnøkkel fra et passord. PKCS#5 er et eksempel på en slik avledningsmetode for DES. Bruk av passord er som nevnt forbundet med enkelte svakheter, og man kunne ønske å avlede nøkkelen fra f eks. en privat nøkkel i et smartkort ? forutsatt at disse nøklene skal ha samme levetid. Pr i dag finnes få disk- eller filkrypteringsverktøy med denne funksjonaliteten.

Et annet aspekt man må ta stilling til er hvorvidt man skal krypterediskdataene med en eller flere nøkler. En disk kan romme store mengder sensitiv informasjon, og det er mulig man vil unngå at kompromittering av én nøkkel kompromitterer hele disken. Siden en angriper med tilgang til disken har aksess til store datamengder, og man generelt kan forvente at mye av informasjonen også er tilgjengelig i klartekst fra andre kilder, har angriperen også et godt kryptoanalytiske utgangspunkt. Bruk av flere nøkler vil være sikrere, men kompliserer nøkkelhåndteringen.

Autorisasjon av mobile medarbeidere i hjemmebasen

Hjemmebasen vil kontrollere hvem og hvilke tjenester som utenfra får tilgang til interne ressurser; typisk vha. en passende sentral brannmurløsning. En medarbeider vil vanligvis kunne aksessere maskiner på bestemte adresser eller segmenter, og vil der operere ut fra tilgangsrettigheter definert

på den enkelte plattform eller applikasjon. Dette vil fungere i mindre og oversiktlige miljøer, men vil være vanskelig å vedlikeholde i større systemer. Det vil være bedre å innføre en egen database eller server som vedlikeholder disse autorisasjonene sentralt. Dette skalerer bedre og gjør det enklere å oppfylle en organisasjons sikkerhetspolicy i praksis.

Slike autorisasjonsfunksjoner er ofte innebygd i større og altomfattende sikkerhetssystemer, som CA Unicenter og andre, men det finnes få selvstendige produkter som tilbyr bare dette.

Beskyttelse mot ondsinnede programmer og program-moduler

Vi har i det senere sett en tendens til utvikling av mer objektorienterte og modul-baserte applikasjoner. Det er spådd at denne utviklingen vil fortsette og at vi etter hvert vil se applikasjoner som i større grad vil kunne tilpasses etter behov. Man vil da laste ned og sette sammen kun utvalgte program-moduler. Dette passer mobilt arbeid godt, siden mobil terminaler forventes å ha lagrings- og prosesseringsbegrensninger. Sikkerhetsmessig er det imidlertid vanskelig å kontrollere opphavet til slike nedlastbare program-moduler, og det er ønskelig at slike program-moduler er signert av noen man kan stole på. Offentlignøkkel-teknologi kommer til anvendelse også her. Kode-signering er et relativt nytt problemfelt, men det vil være avgjørende å implementere ved utstrakt bruk av slike moduler.

Det vil også være aktuelt å la mobil medarbeidere signere eventuelle program-moduler eller scripts de sender til hjemmebasen for å få utført oppgaver.

Generelle sikkerhetsløsninger og –standarder

Vi skal kort diskutere de mest sentrale sikkerhetsstandardene som er aktuelle som byggeklosser i en mobil systemløsning. I tillegg skal vi omtale diverse smartkortstandarder.

IPSEC

IPsec er en velkjent foreslått sikkerhetsprotokoll som tilbyr kryptering samt integritets- og autentisitetstjenester på IP-nivå, altså lag 3. IPsec baserer seg på bruk *Authentication Header* (AH) for integritet og autentisitet og *Encapsulating Security Payload* (ESP) for kryptering. IPsec synes å være svært velegnet for sikring av mobilt arbeid. En mobil medarbeider kan eksempelvis autentisere seg overfor en *IPsec Security Gateway* i hjemmebasen ? som typisk vil være en komponent i en brannmur-løsning? og/eller kommunisere kryptert fram til denne. Det vil si at man oppretter en sikker tunnel fram til gatewayen i hjemmebasen og kommuniserer med ønskede maskiner i det interne nettet gjennom denne. Man kan også utnytte *tunneling* i flere ndre. F eks. kan man opprette en innenforliggende tunnel til en bestemt maskin i det interne nettet dersom man eksempelvis ønsker en IPsec kryptering og/eller autentisering av medarbeideren mot denne maskinen spesielt.

IPsec har fordelen av å dekke alle applikasjonsprotokoller over IP. Den vil basere seg på anerkjente og sikre algoritmer og er en fleksibel standard. Den kan basere seg både på asymmetrisk og symmetrisk nøkkelfordeling, hvilke begge kan være aktuelle i en mobil arbeidssituasjon.

IPsec dekker både IPv4 og IPv6 og begynner å bli etablert standard. Selv om det generelt er vanskelig å spå i dataverdene, ser vel mange på IPsec som den fremtidige, generelle sikkerhetsstandarden for Internet og andre IP-nett.

TLS

Transport Layer Security (TLS), som essensielt er ITEFs versjon av SSLv3, er en lag 4 protokoll. Den krever *reliable transport*, pr i dag i praksis TCP, og tilbyr kryptering og integritets- og autentisitetstjenester for kommunikasjon mellom en klient og tjener. TLS, eller egentlig SSL, er mest kjent som Netscapes beskyttelsesprotokoll for HTTP, men tilsvarende implementasjoner for NNTP, FTP, TELNET, LDAP og POP begynner etterhvert også å komme. TLS/SSL baserer seg på

bruk av sertifikater og asymmetrisk krypteringsteknologi, slik at man må tilknyttes en PKI. TLS/SSL er i utgangspunktet definert med sikre, anerkjente algoritmer, men eksportvarianter er typisk begrenset til å bruke for korte nøkkellengder.

TLS/SSL begynner å bli svært utbredt. Siden en browser vil være et viktig element i en mobil terminal, vil TLS/SSL veldig enkelt og godt kunne utnyttes for å sikre bestemte protokoller, f eks. HTTP. TLS/SSL krever imidlertid visse endringer i de applikasjonsprotokoller den støtter, og den dekker heller ikke UDP-baserte applikakasjoner.

WAP WTLS

WAP Wireless Transport Layer Security Specification (WTLS), er en versjon av TLS tilpasset WAP-protokoller og miljø. WTLS legger seg mellom WTP og WDP laget og tilbyrTLS-sikkerhetsfunksjonalitet. WTLS er veldig lik TLS, men det er gjort enkelte endringer for at den skal fungere over GSM, med de begrensninger det innebærer. Disse endringene kan også ha sikkerhetsmessig betydning. F eks. benytter TLS to hash-algoritmer i kombinsjon, slik at man garderer seg mot at eventuelle svakheter som avdekkes i den ene, ikke kompromiterer sikkerheten. WTLS benytter kun én hash-algoritme alene og oppnår altså ingen slikekstra-garanti.

PPTP

Point-to-Point Tunneling Protocol (PPTP) er en svært utbredt sikkerhetsprotokoll som benyttes mye for oppsett av *Virtual Private Networks* (VPNs). PPTP er også klient-tjener-basert og sikrer mer konkret PPP-forbindelser over TCP/IP. Den er blitt vanlig ikke minst fordi den er en del av Windows NT Server. Klient-versjoner er også bl a. tilgjengelig for Windows NT, Windows 95 og Windows 98. PPTP kan lastes ned fritt for Microsofts web-sider. PPTP innkapsler VPN-pakker inn i PPP-pakker som til slutt sendes over IP mellom PPTP-klient og PPTP-server. PPTP-serveren befinner seg typisk i en gateway.

PPTP tilbyr også kryptering og integritets- og autentisitetstjenester. Den spesifiserer ikke bestemte algoritmer, men utgjør essensielt et rammeverk for forhandling av valg av ulike algoritmer. De fleste PPTP-implementasjoner er basert på Microsofts PPT_implementasjon, også flere andre kommersielle produkter. Microsoft tilbyr flere nivåer av sikkerhet, bl a. for autentisering. Her tilbys vanlig passord-autentisering, hashet passord og *challenge/response*-autentisering. Microsoft baserer seg imidlertid på egne algoritmer og ikke på anerkjente algoritmer, bl a. ikke for*hashing*. Det er i det senere avdekket flere og tidels grove mangler i Microsofts PPTP-implementasjon.

PPTP er imidlertid velegnet for mobilt arbeid og kan relativt enkelt settes opp. Pr i dag er det imidlertid grunn til å være kritisk tilMicrosofts PPTP-implementasjon.

H.235

H.235 er den foreslåtte sikkerhetsstandarden for beskyttelse av H.323-familien av protokoller. H.235 sikrer både kall-signaleringen (H.225.0 *Call Signalling*), kontroll-kanalen (H.245 *Call Control*) og delvis registreringskanalen (H.225.0 RAS *Control*). H.235 foreslår og bruke TLS og/eller IPsec til å autentisere motpartene og å kryptere disse kanalene, for så å fremforhandle valg av krypteringsalgortimer og -nøkler til beskyttelse av selve data-, audio- ellervideo-trafikken.

H.235 er ennå ikke kommet gjennom standardiseringsprosessen, og endringer vil fortsatt kunne påregnes. Dersom man ønsker å unytte H.323 fult ut, og ikke bare til IP-telefoni, kommer man imidlertid neppe utenom H.235. Hvor ressurskrevende H.235 vil være, er foreløpig for tidlig å si.

PKCS#12

Public Key Cryptographic Standards (PKCS) er forslag til ulike standarder knyttet til asymmetrisk krypteringsteknologi laget av RSA *Data Security Inc*. Selv om disse ikke er underlagt en vanlig

standardiseringsprosess, men bearbeides av RSA selv, har flere av disse hatt godt gjennomslag. PKCS#12 er et forslag til et portabelt format for lagring av private nøkler, sertifikater eller spesielle hemmeligheter. Utviklingen av PKCS#12 følges i dag med interesse. Tilsvarende funksjonalitet finnes delvis inkludert i ulike sikkerhetsprodukter, men ved å standardisere på formatet kan flere applikasjoner kunne dele sikkerhetsattributter, som f eks. brukerens private nøkler. En mobil terminal må kunne lagre nøkler og andre hemmeligheter lokalt, og PKCS#12 er klart et interessant alternativ dersom standarden får forventet gjennomslag.

Smartkortstandarder

Det er mange standarder knyttet til smartkort og ulik bruk av smartkort. Generelt kan man si at fysiske og mekaniske aspekter, samt øvrige laverelags protokoller er godt standardiserte, men at det er flere standarder å velge mellom for øvrelags protokoller, f eks. for valg rundt API.

ISO 7816, som nå er noen år gammel, er den sentrale standarden i førstnevnte kategori. Den dekker fysiske karakteristika, posisjoner for elektriske kontakter, hvordan lese og skrive data samt koding av grunnleggende attributter.

Pga. at ISO 7816 ikke omhandler nok om grensesnitt og behandling av mer applikasjonsspesifikke data, har flere aktører definert egne utvidelser. Et eksempel her er EMV, som ble utviklet av Europay, Mastercard og VISA.

PC/SC er et sentralt initiativ som bygger videre på disse arbeidene. PC/SC fokuserer på bruk av smartkort i PCer og andre arbeidsstasjoner, og støttes bl a. av Bull, HP, IBM, Microsoft, SNI og Toshiba. PC/SC synes å bli en sentral standard, bl a. fordi Windows 98 og NT 5.0 vil inkludere støtte for den. PC/SC støtter bruk av smartkort og smartkortlesere fra ulike leverandører.

Andre tilsvarende standarder er PICA, som baserer seg på PKCS-standardene og støttes bl a. av IBM, Netscape og RSA, og CSDA fra *The Open Group*. Vi kan også nevne JavaCard fra Sunsoft og *The OpenCard Framework*. Sistnevnte retter seg mot bruk av smartkort i NCer og støttes bl a. av IBM, Netscape, Oracle og Sun.

Smartkort kan være ferdigprogrammert med fast kode i *read-only*-minnet på kortet. Men smartkort kan også være programmerbare, slik at eksekverbar kode kan legges til etter hvert. Blant disse er særlig de såkalte multiapplikasjonkortene mye omtalt. Disse gir mulighet for flere applikasjoner på samme smartkort. MULTOS er det viktigste operativsystemet for multiapplikasjonskort i dag. MULTOS bygger bl a. på ISO 7816 og EMV slik at produkter fra mange aktører kan koeksistere på kortet. MULTOS og JavaCard går foreløpig ikke sammen. Bl a. Sun studerer nødvendige spesifikasjoner for å bøte på dette.

Tilgjengelige sikkerhetsprodukter

Det finnes en stor mengde sikkerhetsprodukter som kan benyttes til å sikre en mobil systemløsning. Vi skal ikke gå inn på sikringen av hjemmebasen, med brannmurer etc. Men selv på terminalsiden er det mange produkter tilgjengelig og vi kan bare nevne et fåtall.

NORMAN ACCESS CONTROL FRA NORMAN DATA DEFENCE SYSTEMS

Dette produkter tilbyr en adgangskontrollbeskyttelse til PCer og mobile terminaler. Adgangen kan basere seg på bruk av smartkort, og inneholder både en boot-kontroll og en låsefunksjon. Verktøyet tilbyr også filkryptering.

F-SECURE FRA DATA FELLOWS

F-Secure er egentlig et sett av sikkerhetsprodukteter fra Data Fellows . Produktene er basert på asymmetrisk krypteringsteknologi og støtter bl a både oppsett for VPN og fil-kryptering. F-Secure

VPN+, som er deres siste VPN-verktøy, baserer seg på IPsec. F-Secure Crypto er navnet på deres disk-krypteringsverktøy.

F-Secure er utviklet i Europa og er ikke begrenset av amerikanske eksportrestriksjoner.

DISCLOCK OG YOUR EYES ONLY FRA SYMANTECH

Dersom man kun er interessert i rene disk- og filkrypteringsverktøy, er de nevnte produktene fra Norton mye benyttet og et av mange aktuelle alternativer. En ulempe her er at krypteringsstyrken er begrenset pga. de amerikanske eksportrestriksjonene.

ENTRUST/ICE FRA ENTRUST TECHNOLOGIES

er et av flere velkjente sikkerhetsprodukter fra Entrust. Dette tilbyr bl a. sikring filkryptering. Men krypteringsstyrken er begrenset også her pga. de omtalte eksportrestriksjonene.

SECURE ATTACHÉ FRA SECURITY DOMAIN

er et eksempel på et australsk filkrypteringsverktøy, og dette har følgelig ingen begrensninger i krypteringsstyrke som følge av eksportrestriksjoner. Men merk altså at det finnes mange tilsvarende verktøy.

HP MOBILE SECURITY SUITE FRA HEWLETT-PACKARD

Flere av de største dataleverandørene ser for seg et marked inne mobile systemer. Eksempelvis har HP lansert det nevnte produktet. Løsningen tilbyr en smartkortbasert adgangsbeskyttelse av mobile terminaler, samt filkrypteringsbeskyttelse. Smartkortet utfører nødvendige kryptografiske operasjoner og støtter 128 bits kryptering i USA og Canada, men kun 40 bit utenfor.