Faglig ansvarlig / medveileder til følgende oppgave(r):

Professor Chunming Rong
rong@unik.no
Mobil: 4088 9897

Forslag Studentoppgaver

Dette notatet lister opp kort noen forslag til mulige studentoppgaver fra Abel DRM Systems relatert til smartkort/UICC/JavaCard og Mobil TV. For mer informasjon om Abel DRM System se www.abeldrm.com.

Oppgaver relatert til smartkort (JavaCard)

Sikker applet eksekvering i multi-applikasjons JavaCard/UICC

Dagens smartkort får bedre kapasitet mht. minne, lagring og prosesseringskraft. Dette brukes til å lage flerbruker applikasjonskort (JavaCard). Normalt har det vært en eller 2 leverandører involvert i produksjon av smartkort chip og applikasjon. Det blir flere leverandører av programvare til smartkortet og muligheter for innlastning av applikasjoner fra "vilkårlige" tredje part.

Oppgaven består av trusselanalyse av personalisering av JavaCard og hvordan flere leverandører av software til JavaCard kan påvirke total sikkerheten. Formålet er at personalisering av JavaCard kan settes ut til ikke tiltrodde partner for personalisering og distribusjon av JavaCARD. Utarbeide forslag til metodikk for hvordan å minimalisere disse truslene, samt konseptuelt forslag til sikker personalisering av JavaCARD.

Code Obfuscation technich (for Java)

Evaluering av alternative metoder, hyllevareprodukter, mm for å vanskeliggjøre reverse engineering av programvare (som inneholder nøkler og kryptoalgoritmer). Dette kan typisk være programvare av typen Cloakware som gjør "tilfeldige" transformasjoner på kildekoden slik at den funksjonelt har samme oppførsel som før men tilfører en rekke beregninger og endringer i kontrollflyt slik at lokale data (typisk kryptografiske nøkler) og betingelser i kontrollflyten spres utover i koden. Dette er en metode der forbetingelsen er at programvaren må kjøres i en relativt åpen (usikret) omgivelse.

Bruk av elliptisk kurve i smartkort

Trusselanalyse for "fallgruver" med bruk av elliptisk kurve I smartkort. Praktisk implementering av elliptiske kurve.

Høyhastighets smartkort I/O driver

Trenden innen smartkort er nå bruk av MMC, SDIO eller USB grensesnitt for høyhastighet (1Mbps) kommunikasjon med smartkortet. Dette kan brukes til prosessering av komplett DVB-H stream (maks 500Kbps) innen på smartkortet. Oppgaven består av analyse av hvilke SW driver som finnes for de forskjellige Mobiltelefon og PDA enheter. I tillegg praktisk oppgave med å lage en prototype av felles høyhastighets smartkort I/O driver for mobiltelefon/PDA.

Matrise av smartkort som Hardware Security Module (HSM)

Se på bruk av smartkort med høyhastighets IO (USB) i matrise som alternativ til dedikert HSM. Se på ytelse og skalering. Nøkler vil være lagret som krypterte "blob" i en database. Programmeringsgrensesnittet vil være f.eks. Java Crypto API.

Oppgaver relatert til Mobil TV (DVB-H)

For introduksjon og oversikt over Mobil TV (DVB-H) sjekk ut www.dvb-h.org og spesifikasjonene: www.dvb-h.org/PDF/**a100**.tm3455r3.cbms1476.IPDC_SPP.pdf

PVR/"PushVOD" løsning for Mobil TV på høykapasitest smartkort/Flash minne

Konseptuel løsning for DVB-H Mobil TV PVR/PushVOD til smartkort med høy lagringskapasitet (1Gbyte).

Design, implementering og lasting av KDA i DVB-H terminaler

Praktisk ingeniøroppgave for design, implementering av KDA i mobiltelefon og PDA basert på Java MIDP/ Java ME. Løsningen inkluderer også hvordan KDA applikasjonen kan bli lastet på forespørsel via SMS/mobil nettverket, fra DVB-H nettverket, MMC eller et smartkort med høy lagringskapasitet (1Gbyte).

Prototype av ISMACryp og OMA DRM container

Praktisk ingeniøroppgave for design og implementering av ISMACryp kryptering/dekryptering av filer iht. OMA DRM container.

Distribusjon av rettigheter via GSM SMS tekstmeldinger

Praktisk ingeniøroppgave for design og implementering for distribusjon av rettigheter via GMS SMS tekstmeldinger til mobil telefoner og UICC.