AALBORG UNIVERSITET

IT-afdelingen
Fredrik Bajers Vej 5
9220 Aalborg Øst
Tlf. 9635 9451
Fax 9815 6970
www.aau.dk/itafd

IT chef
Klaus Kilt
Tlf. 9635 9450
Mobil: 2062 9060
Email: kilt@adm.aau.dk

Notat til forretningsudvalget i RK ikt-gruppe

Dato: 5. december 2005 Ref.: KILT J.nr.: 2005-060/01-0012

Betænkeligheder ved at acceptere TDC tilbud om udlevering af Digital Signatur (cd-udgaven) til alle ansatte og studerende på landets universiteter

I forbindelse med projektet Digital Signatur, under VTU's Digital Forvaltning, har vi været tæt inde på problematikken omkring anvendelse af forskellige medier, for at undersøge mobiliteten af digital signatur.

I den forbindelse har vi også stiftet bekendtskab med en TDC-løsning, hvor der anvendes en cd som medie, kædet sammen med brugerens personlige kode. Det der bekymrer os i denne løsning er, at certifikatet for digital signatur nu opererer i 2 forskellige sikkerhedsniveauer.

It-specialist Peter Lind Damkjær fra TDC-erhverv har ved et RK ikt-gruppemøde udtalt, at han ikke ville anvende cd-løsningen på en pc stående på et ikke sikkert sted. Dermed sagt, at løsningen kun kan anvendes på pc'er som står under trygge rammer. Dette er sikkert også forklaringen på, at TDC på nuværende tidspunkt kun har tilbudt denne løsning til medarbejdercertifikater. På den måde er det op til firmaet selv at sikre sig de trygge rammer.

Der er 2 elementer i denne problematik:

1) Digital signatur har nu fået flere sikkerhedsniveauer. Jeg tror ikke, at hr. og fru Hansen kan skelne mellem den ene eller anden sikkerhed. Oplever de først, at deres certifikat er misbrugt, vil der opstå mistro til digital signatur, og de vil sandsynligvis ikke bruge det igen.

2) Jeg tror ikke på, at it-miljøet på de danske universiteter har en sikkerhed, som kan modstå misbrug af cd-løsningen.

Derfor ser jeg det meget problematisk, hvis RK accepterer tilbudet fra TDC, om at få udleveret digital signatur på et cd-medie. Jeg opfatter TDC-tilbudet som at få universiteterne til at blåstemple løsningen. TDC bør derimod have besked på at videreudvikle andre løsninger, hvor sikkerheden er i top, og med fokus på mobilitet. Se vedhæftede notat om udvikling af chip-løsninger.

For en mere teknisk udredning, omkring brugen af cd-mediet, har jeg vedhæftet et notat fra projektleder Henrik Findsen, som arbejder med projektet omkring mobiliteten af digital signatur.

Med venlig hilsen

Klaus Kilt

Notat vedr. digital signatur og sikkerhed (sammenfatning)

Indledende finder jeg det vigtigt, at klarlægge grundene til, at sikkerhed er blevet et issue i projektet.

Under et af de første møder, fremgik det klart, at interessenterne i projektet var meget i tvivl om, hvordan brugen af digital signatur ville komme til at påvirke den lokale infrastruktur og sikkerhed.
Enkelte af interessenterne havde dog i forvejen kendskab til brugen af digital signatur i netværket, og fandt ikke at der var belæg for bekymring.

For at implementere en eventuel testløsning, så optimalt som muligt, i forhold til at få flest brugere til at benytte løsningen så ofte som muligt, blev der i projektet besluttet, at det ville være hensigtsmæssigt at undersøge brugernes (de studerendes) præferencer for brugen af digital signatur gennem en spørgeskemaundersøgelse.

Under et indledende møde med Ulf Preisler, der er direktør for den virksomhed, som vi entrerer med, i forbindelse med udformning og distribution af spørgeskemaundersøgelsen, blev det i forbindelse med udformningen af spørgsmål til spørgeskemaet, klart for os, at der kunne være sikkerhedsmæssige problemer med 2 af de medietyper, vi var kommet frem til burde eftertestes i forbindelse med mobiliteten.

Vi vurderede, om vi skulle lade dette ligge, idet det ikke falder ind under projektets "scope", og tage det sikkerhedsmæssige aspekt op på et senere tidspunkt.

Jeg valgte at belyse sagen på det efterfølgende arbejdsgruppemøde, hvor Allan Pletner var indbudt.

Allan Pletner informerede indledningsvis arbejdsgruppen, om forskelle i chiptyper / producenter, og de produktspecifikke add-on der fremstilles til understøttelse heraf (inkl. Aladdin, der er TDC's produkt).
Idet projektet har til opgave at teste mobilitet, finder arbejdsgruppen det vigtigt, at de medier der skal testes fungerer optimalt i et givent miljø - og her kommer de produktspecifikke add-on ind i billedet.

Efterfølgende tog vi fat på belysning af eventuelle sikkerhedsmæssige problematikker.
Ulf Preisler og undertegnede, fremlagde hvad vi var kommet frem til:

Intro
I det følgende sammenholdes cd-rom og chip-baserede løsninger.
Der skelnes ikke mellem chip-kort eller tokens. Hvor der står 'kort' menes begge teknologier.

Generelt
Udfordringen er som sådan ikke at 'knække' krypteringen, (som er muligt, indrømmet, men progressivt mere og mere besværligt jo bedre teknologi der bliver brugt) men at stjæle en persons identitet.

Uanset hvilken løsning der vælges, deler de som udgangspunkt en 'point-of-failure', nemlig pinkodeindtastningen, i forbindelse med aktivering af et dokument m.v.
Hvis maskinen, hvorpå dette foregår, på en eller anden måde er kompromitteret, med eksempelvis en 'keylogger', kan denne fange pinkoden. En keylogger kan installeres af en trojansk virus eller lignende.

I forhold til universitetets systemer, er det muligt for systemfolk, uden videre at fange alle pinkoder (og alle andre kodeord, for den sags skyld) i systemet. Både cd-rom og chip-løsninger har en svaghed i dette tilfælde.

Cd-rom / installation på harddisk (HHD)
En af de grundlæggende forskelle mellem cd-rom / HHD og en chip-baseret løsning, er at cd-rom / HHD løsningen er softwarebaseret.

Dette medfører, at brugerens private nøgle, på et eller andet tidspunkt, er 'fri' i RAM. I det øjeblik er den læselig af andre programmer.

Dette betyder, at det er muligt, ved hjælp af et lille program (evt. i form af en virus), at aflæse den ukrypterede private nøgle.

Et cd-rom scenario, der ikke engang kræver en dekrypteret nøgle. Der kræves blot, at cd-rom'en aflæses i sin helhed.
I Windows kan dette være besværligt, idet der ofte er et sikkerhedssamspil mellem hardwaren, og de DLL'er der skal bruges til at læse cd-rom'en. Jeg antager, at cd-rom'en er i et unikt format, hvilket ville være svært at læse med almindelige metoder.

I *NIX, derimod, er det relativt let at læse den rå data, som den ligger. For efterfølgende at benytte data, kræves det end ikke, at der brændes en ny cd. Der genereres blot en image-fil, der enten kan 'mountes' (tilføjes computeren som, eksempelvis, et virtuelt cd-rom drev), derefter kan man bruge pinkoden til at generere en helt valid engangssignatur.

Det er næsten ligegyldigt, hvilken beskyttelse der er på cd-rom'en, idet det er et krav, at et almindeligt cd-rom drev skal kunne aflæse den (ellers kan den jo ikke bruges).

Idet signaturer typisk er datostemplet, vil tyveri af en digital signatur betyde, at alle signaturer, genereret af nøglen, vil være invalide efter den dato tyveriet er anmeldt.

Da der kun er taget en kopi, vil brugeren ikke vide, at et tyveri af både pinkode og signatur er sket, og derfor vil der gå længere tid før anmeldelsen.

Det skal desuden bemærkes, at signaturen på en cd-rom, ligger som en image-fil. Det betyder, at den sammen med pinkoden kan sendes ud over hele Internettet, lægges på en ftp-server, o.s.v.

Denne form for kompromittering kan let skaleres, når man er kommet forbi cd-rom kopieringen.
Metoden / systemet vil med lethed kunne automatiseres, og derefter vil det ikke kræve menneskelig indblanding at aflæse pinkoder/cd-rom'er og sende dem videre ud i systemet.

Chip-løsning
Chip-løsningen (kort/token), er en hardware-baseret løsning. Den frigiver aldrig selve den private nøgle, men genererer en engangsnøgle, der kun kan bruges en eneste gang.

Chippen kan forestilles som en separat pc i pc'en, der kun har nogle få funktioner, men har meget paranoide sikkerhedsforanstaltninger, der gør det meget sværere at kompromittere systemet.

Den simpleste måde er at aflæse pinkoden, og derefter stjæle kortet. Men idet der kun er et kort (som er *meget* svær at kopiere - for ikke at sige praktisk umuligt), vil det for-

modentlig hurtigt gå op for brugeren, at kortet mangler, og derefter alarmere myndighederne.

Teoretisk kan kortet 'lånes', og man kan analysere det (kræver nok en VLSI ingeniør), men praktisk er det uladesiggøreligt i nogen effektiv skala.

Konklusion
Det er vigtigt at forstå forskellene i skalerbarhed i de to fremgangsmåder.

Det er egentlig ligegyldigt, hvor svært det er at kopiere cd-rom'en. Er der først lykkedes én gang at kopiere en cd-rom, kan den genbruges igen og igen.
En mulig delvis lappeløsning kunne være at implementere logging på brugen af den digitale signatur. Det forhindrer ikke misbrug, men gør det muligt for en bruger at se, at vedkommendes digitale signatur er kompromitteret, og herefter handle på det.

Chip-løsningen er mig bekendt ikke skalerbar.
Der er således kun ét kort og én signatur, hvilket betyder, at jeg fysisk skal være i besiddelse af chipkortet, for at være i stand til at trække data ud og bryde krypteringen.

En anden måde at sige det på, er at cd-rom'en er sin egen API. Alle der kan læse til den, har adgang til den. Chippen derimod, har en logisk API, der kun lukker få ting ind, og "kun" sender engangssignaturer ud.

Det andet kan styres af en mand uden at spendere meget tid på nettet.

Det er det som skræmmer mig ved software- modsat hardware-baserede løsninger: Skalerbarhed.

Jeg har fremstillet en lille case.

1. Jeg skaber en virus, der kun har til formål at lave 'bots - altså computere under min kontrol. Der installeres en bagdør i disse bots.

   Når jeg har 10-100 tusind af dem under min kontrol, uploader jeg et script, der er en kombination af en keylogger og certifikat/signaturlæser.

2. For at undgå at jeg skal være på nettet hele tiden under uploaden, uploader jeg bare til 10. Disse får besked på at uploade 10 til andre i botnettet o.s.v. (indtil videre er det ikke meget anderledes end det som spammere gør.)

3. Computerne kører nu i cyklus, og (i modsætning til spammere) gør de ikke noget på nettet.
   Periodisk (eller når der er noget at uploade) kontakter de en server (ftp, http, p2p, bittorrent eller andet). Ikke alle har kontakt til de samme servere. En elegant metode er, at køre en smtp server på en ikke-standard port.

4. Idet SMTP er 7-bit, kan jeg, for at forvirre evt. sporhunde, periodisk køre et telnet script, som springer igennem 10-20 gratis konti på forskellige kontinenter, gå ind i de forskellige servere og 'støvsuge' informationen. Idet jeg har sikretl, at der er tidsstempel, når noget tages fra en pc, kan jeg korrellere loginkoden og certifikaterne/signaturerne.

   Et andet godt opsamlingssted er f.eks. at kode informationen som jpg'er, og uploade dem til et fotosite, som har meget trafik, som f.eks. flickr.com.

5. Jeg har nu alt, som digital signatur programmet skal bruge, og jeg kan nu f.eks. bruge informationen til at finde de personer der er 'interessante'. Jeg tænker her

på at gå ind og se en forskudsselvangivelse eller lignende.

Hvis der er tale om store beløb, kan jeg se hvilken netbank aktivitet eller lignende der har været.

- Casen fokuserer og tager udgangspunkt i cd-rom / HHD problematikken.

- I forhold til chipkort, vil det med metoderne i casen være næsten umuligt at gøre noget, selvom jeg høster pinkoder.
  Jeg behøver den private nøgle, der ikke kan hentes / aflæses, hvorfor den eneste mulighed er at genskabe nøglen med den krypterede engangssignatur og pinkoden - det er ikke umuligt, men ressourcemæssigt meget meget dyrt.

På baggrund af dette, vil vi lade arbejdsgruppemedlemmerne individuelt afgøre, hvilke medietyper der er teknisk forsvarlige at benytte.
Det er essentielt, i sammenhængen, at huske på, at universitetsmiljøet, sikkerhedsmæssigt er betydeligt mere udsat, i relation til hacking, idet det interne miljø er legepladsen for de studerende.

Jeg ser personligt et stort problem i, at arbejde med flere sikkerhedsniveauer på det som med tiden gerne skulle udvikle sig til en borgersignatur.

- Der investeres både fra offentlig- og privat side store beløb i at få gang i den digitale signatur. Hvis brugerne mister tilliden til digital signatur, vil store beløb være spildt.
- Idet det handler om beskyttelse af personlige data, er jeg af den opfattelse, at "discount" løsninger ikke kan accepteres.
- Det vil kræve enorme summer at lære familien Danmark hvor og hvordan man, uden at kompromittere sin egen sikkerhed, kan benytte en cd-rom løsning.
- Jeg mener, at der bør findes en løsning, således at en signatur, installeret på en HHD, opbevares krypteret. Dette er ingenlunde umuligt.

Jeg mener ikke, at det er urealistisk at se sådan på tingene, idet der er tale om en digital personlig underskrift.

Jeg har fremlagt ovenstående for TDC, der henfører til, at de har fået godkendelse til at anvende cd-rom løsningen af Datatilsynet, og at de i øvrigt ikke kan se nogen problemer i relation til sikkerhed og cd-rom.

Jeg er udmærket klar over, at man ikke kan forvente, at en kommerciel virksomhed tænker borgersikkerhed på samme måde som man må forvente det af Staten.
Set i lyset af, at sikkerhed koster penge, og produkterne (her digital signatur) bliver dyrere for den enkelte borger at erhverve (på chipkort eller token) mindskes indtjeningsmulighederne. Det er derfor nærtliggende at gå på kompromis med sikkerheden for at øge indtjeningsmulighederne.
Jeg mener blot, at der her ikke bør herske tvivl om, at sikkerheden i forhold til omhandlende bør være i fokus.

Med venlig hilsen

Projektleder Henrik Findsen
Aalborg Universitets IT-afdeling