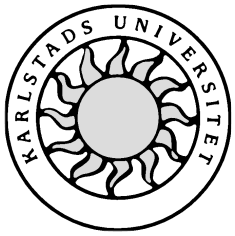

Datavetenskap

Opponent:

Andreas Lavén

Respondenter:

Anders Ellvin, Tobias Pulls

Implementing a Privacy-Friendly Secure Logging Module into the PRIME Core

---

Oppositionsrapport, E-nivå

2005:xx

1 Sammanfattat omdöme av examensarbetet

Examensarbetet är intressant, speciellt med tanke på den utveckling som pågår på internet. Examensarbetet är av hög kvalité, där lösningarna till problemen är väl motiverade. God presentation av lösningarna.

Dock kan designen beskrivas med annan struktur i uppsatsen.

2 Synpunkter på uppsatsen knuten till examensarbetet

2.1 Titel

Titeln på examensarbete, “Implementing a Privacy-Friendly Secure Logging Module into the PRIME Core”, ger en bra bild av innehållet.

2.2 Uppsatsens disposition

Uppsatsen inleds med en introduktion följt av bakgrund, vilket är bra. Att sedan lyfta fram tidigare arbete, som är av stor vikt i examensarbetet, är en bra fortsättning. Därefter följer implementationen.

Kapitlet över tidigare arbete täcker till stor del designen över examensarbetet, men vissa delar saknas och refereras istället till en publicerad artikel. Denna design, tillsammans med den design presenterad i kapitlet innan hade kunnat presenterats i ett eget kapitel med namnet design. En jämförelse över skillnader i de båda designerna bör presenteras.

Efterföljande del av uppsatsen är bra uppdelat, vilket även hela uppsatsen är över lag.

2.3 Begreppsapparat

Respondenterna använder sig av termer som är relevanta och som de ger intryck av att behärska.

2.4 Argumentering och slutsatsdragning

Argumenteringen och slutsatsdragningen i uppsatsen är vettig, genom väl motiverade lösningar av givna problem i uppgiften.

2.5 Sammanfattningen

Sammanfattningen beskriver uppsatsen på ett bra sätt, då den tar upp de viktiga delarna av examensarbetet; dess mål, uppgift och resultat. Sammanfattningen lämnar inga frågor obesvarade i rapporten.

2.6 Språkbehandling

Det finns inga svårigheter att följa uppsatsens text. Däremot beskriver respondenterna mycket vad just de har gjort, genom att använda meningar som ”Vi gjorde ...”. Detta tar ibland bort fokus från vad som är ett måste att göra till vad just respondenterna gjorde. Dessutom används kontraktioner såsom ”wasn't” och ”doesn't”, vilket bör undvikas i skrift. Dessa kontraktioner tillsammans med vissa specifika meningar, exempelvis en som avslutas med ”and more...” (punkterna är med i uppsatsen), gör att uppsatsen kan få ett, felaktigt, dåligt intryck vid första anblick.

2.7 Referat och källförteckning

Uppsatsen innehåller en god motivering i form av bland annat referenser vid val av lösningar. En brist kan vara att flera referenser riktas mot Wikipedia, där ingen specifik författare är bunden till påståendena.

2.8 Övriga kommentarer

Bildtexterna kan sammanfattas i listan över figurer.

3 Genomgång av uppsatsen kapitelvis

3.1 Kapitel 1

Uppsatsens första kapitel är en introduktion till examensarbetet. Detta kapitel beskriver målen för examensarbetet. Dessa mål är uppdelade i ett primärt mål, och flera sekundära mål.

Det skrivs i uppsatsen att det primära målet genomgick vissa ändringar under tiden som uppsatsen skrevs. Detta bör inte stå med.

Bland de sekundära målen, var det endast ett som hanns med. Därav borde endast det målet stå med och de andra sekundära målen borde flyttas till framtida projekt. Att skriva att vissa mål inte hanns med ger ett dåligt intryck, till ett övrigt bra arbete.

I kapitlet finns även en tidslinje över examensarbetetet presenterad. Respondenterna säger sig inte kunnat ha följt denna, därav borde den antingen tas bort från rapporten eller skrivas om så att den stämmer med verkligheten.

3.2 Kapitel 2

I kapitel 2 finns en bra beskrivning av bakgrunden till examensarbetet. Här beskrivs de olika delarna och även ett exempel ges.

En beskrivning av kryptografi beskrivs i detta kapitel, men det påstås att man kan tryggt hoppa över detta stycke om man har grundkunskaper i ämnet. Frågan är då vad grundkunskaper i kryptografi är.

Stycket om kryptografi är välskrivet, och ger en tillräcklig kunskap om kryptografi för att förstå uppsatsen. En del som dock är otydlig är det om Hash, MAC och HMAC, där det påstås att en hash måste som minimum ha både ”weak”- och ”strong collision resistance”. Av att döma av intuitiv känsla av namnen, samt även av de givna definitionerna, innefattar ”strong collision resistance” ”weak collision resistance”.

3.3 Kapitel 3

Kapitel 3 är en beskrivning av tidigare arbeten, vilket innefattar en protoyp implementerad under kursen ”Topics in Computer Security”. Denna prototyp beskrivs väl i kapitlet. Det enda som är något svårt att tyda, är ”i” och ”j” i figuren på sida 25.

I sammanfattningen av kapitel 3 står att den tidigare prototypen är långt från redo att användas seriöst i något system. Detta är dock inte beskrivet i kapitlet. Dessutom står det att det huvudsakliga målet med uppsatsen är att modifiera prototypen så att den följer den design presenterad i artikeln ”Adding secure transparency logging to the prime core”, vilket inte tydligt är beskrivet i kapitlet.

Att den publicerade artikeln innehåller vidare utvecklad design ges inte av någon tydlig beskrivning, bara en del av en mening i introduktionen. Denna mening berättar också att arbetet blev presenterat i IFIP Summer School, vilket stjäl fokus. Dessa skillnader framkommer mer tydligt framöver i uppsatsen, men en tydlig jämförelse i detta kapitel, eller än hellre ett eget kapitel över design, vore att önska.

3.4 Kapitel 4

Kapitel 4 beskriver implementation av examensarbetet. Implementationen var uppdelad i tre delmål, vilket ger en god struktur till både examensarbetet och uppsatsen.

Det första delmålet var att uppdatera loggningsmodulen, vilket gavs namnet ”Update Standalone”. ”Update the Standalone Prototype” eller ”Update the Standalone Logging Module” hade bättre beskrivit delmålet.

I stycket som beskriver det första delmålet står att läsa att vissa riktlinjer för hur man ska skriva koden inom projektet ignorerades, varav endast en utelämnad beskrivs. Även de andra bör beskrivas, och ges en förklaring varför de utelämnades. Dessutom står det att det är värt att nämna att andra delar av PRIME Core ignorerar riktlinjer, vilket borde ges en förklaring till varför det är värt att nämna. Resterande delar av det första delmålet är väl beskrivet, och här framkommer även skillnader jämfört med den tidigare prototypen.

Det andra delmålet beskriver integreringen av prototypen i PRIME Core. I stycket nämns att endast ett anspråk (”claim”) stöds i nuvarande implementation, men det beskrivs att flera kan returneras av en funktion. Vilka är de andra? En tvetydighet i detta stycke är att kommunikationen mellan PRIME kärnor sägs använda Transport Layer Security eller Secure Sockets Layer som default. Respondenterna nämner också att de känner att tidsstämplar är ett krav för all framtida loggning, vilket bör förklaras varför.

Det tredje delmålet är att utreda HSQLDB. I detta stycke skriver respondenterna att de har resultat som visar att typ av tabell är avgörande, och inte i vilket läge HSQLDB körs. Vad som avgörs, eller hur resultaten uppkom, beskrivs ej. Här beskrivs även att struktur samt vissa inställningar skrivs till en fil. Dessa inställningar bör anges.

3.5 Kapitel 5

Det femte kapitlet beskriver resultat och utvärderar examensarbetet. Här finns ett exempel som detaljerat beskriver hur delarna av PRIME Core fungerar, på ett tydligt sätt.

Utvärderingarna presenterade i kapitlet är bra, då de tar upp säkerhet utifrån olika perspektiv. Dessutom tas påverkningar på prestanda upp i utvärderingen.

De tester som är hänvisade till senare arbete, skulle dock räckt med att stå bland senare arbete.

3.6 Kapitel 6

Kapitel 6, slutsatserna, beskriver först hela uppsatsen på ett väl sammanfattat vis. Därefter utvärderas de sekundära målen för examensarbetet. Dessa bör istället endast nämnas som senare arbeten för PRIME Core. Respondenterna presenterar även tänkbara framtida arbeten för PRIME Core, vilka alla är nödvändiga.

Kapitlet, och således uppsatsen, avslutas med väl valda slutord.

3.7 Övriga kommentarer

Inga övriga kommentarer.

4 Slutliga kommentarer

Väl genomfört examensarbete, där några ändringar i språket och strukturen kan lyfta uppsatsen till arbetets nivå. I övrigt har uppsatsen bra förklaringar till både problem och lösningar. Lösningarna är dessutom väl motiverade.