



KTH Computer Science
and Communication

Kerstin Frenckner, tel 08-790 9754, e-mail: kfrenck@csc.kth.se

2
February 12, 2009

Copyright CSC, KTH

OPPONENT RECORD

Thesis compiled by

Joakim Uddholm Hjalmarsson

Title of thesis:

Voting Mix-Net

Implementing a mix.net for use in electronic voting system

Opponent:

Gustav Engström

Was it easy to understand the underlying purpose of the project? Comments.

Syftet är tydligt till viss del. Tydlig att en ett vote mix-net ska implementeras och någon slags prestandamätning. Skulle vara bra om vad denna prestandamätning innebär i inledningen så att det blir tydligare koppling till slutsatsen.

Do you consider that the report title justly reflects the contents of the report?

Titeln behandlar i och för sig endast implementationsdelen att en studie av prestanda ska göras framgår ej .

How did the author describe the project background? Was there an introduction and general survey of this area?

Bakgrunden tar upp vad mix-net används till, tidigare implementationer och sårbarheter/svårigheter med dessa i inledningen. Samt går mer på djupet i själva bakgrunden med exempel. Skulle ha varit intressant att beskriva mer tydligt vad skillnaderna är mellan de tidigare implementationerna är.

To what degree did the author justify his/her choice of method of tackling the problem?

Uddholm Hjalmarsson beskriver tydligt varför den version av mix-net som implementerats har valts, med fokusering på säkerheten i mix-net, som. Dock har han ej motivering utifrån den frågeställning han har om prestanda.

Did the author discuss the extent to which the prerequisites for the application of such a method are fulfilled?

Här är Uddholm Hjalmarsson väldigt tydlig med vad som implementerats, och vad som inte implementerats i den version av mix-net som valts. Vissa delar av metoden har valts bort då tidsramen för denna uppsats var begränsad och därför inte hunnit med. Han tar dock upp detta i diskussionen om prestanda resultaten.



**KTH Computer Science
and Communication**

Kerstin Frenckner, tel 08-790 9754, e-mail: kfrenck@csc.kth.se

2
February 12, 2009

Copyright CSC, KTH

Is the method adequately described?

Metoden och beskrivningen om hur Uddholm Hjalmarsson implementerat mix-net är grundligt beskriven. Beskrivningen av genomförandet känn motiverat även om det ibland kan vara lite svårt att hänga med i alla steg. Kanske skulle en tydligare grafisk representation av krypteringsflödet varit att föredra.

Has the author set out his/her results clearly and concisely?

Do you consider the author's conclusions to be credible?

Ja det tycker jag. Uppsatsen frågeställning var en undersökning om prestandan i en viss implementation av ett mix-net. Då han i slutsatsen nämner att det saknas delar i implementationen, men att prestandan ändå kan anses som effektiv anser jag att slutsatsen är korrekt och insiktsfull.

What is your opinion of the bibliography? What types of literature are included? Do you feel they are relevant?

Förutom referenser som är direkt kopplade till implementationer har Uddholm Hjalmarsson tagit upp ett flertal uppsatser som behandlar både Mix-net och den typ av kryptografiska som mix-net i fråga använder sig av, vilket får anses som relevanta källor. Jag anser även att Uddholm Hjalmarsson varit källkritisk i sitt val av källor.

Which sections of the report were difficult to understand?

Metoddelen är helt klart den mest krångliga delen av uppsatsen. Även om jag tycker att Uddholm Hjalmarsson har försökt skrivit beskrivningen av implementationen på ett pedagogiskt sätt, med att inte gå in för djupt i detaljer tycker jag ibland att det kan vara lätt att tappa tråden. Just i krypteringsflödet tycker jag att en tydligare grafisk representation hade varit ett bra komplement.

Other comments on the report and its structure.

Överlag tycker jag att uppsatsen är välskriven och tydlig. Formen är bra och lättläst och styckena är bra indelade. Hade dock önskat mer grafisk representation

What are the stronger features of the work/report?



**KTH Computer Science
and Communication**

Kerstin Frenckner, tel 08-790 9754, e-mail: kfrenck@csc.kth.se

2
February 12, 2009

Copyright CSC, KTH

Även om det kanske är den del som är svår att förstå tycker jag att metoden är bra beskriven. Att Uddholm Hjalmarsson inte försöker gå in på detaljer utan beskriver det på en högre nivå gör det lättare att förstå.

What are the weaker features of the work/report?

Jag hade önskat en tydligare frågeställning och syfte med uppsatsen.

What is your estimation of the news value of the work?

Jag tror nog att nyhetsvärdet i denna uppsats är bra. Val är alltid en känslig fråga för många länder och tittar man på "nya" demokratiska länder är det inte ovanligt med valfusk. Senast valet i Venezuela där valet var väldigt jämt och resultatet kritiserades. Det är såklart viktigt att ett val går rätt till och ett mix-net verkar vara ett bra verktyg för att säkerställa detta.

Summarize the work in a few lines.

Uddholm Hjalmarsson beskriver i sin uppsats hur han implementerat en version av ett "vote mix-net" med skydd mot ett antal attacker och sårbarheter. Uppsatsen förklarar ingående varje del i mixnätet och hur de interagerar med varandra. Uppsatsen diskuterar prestandan vad gäller tid det tar för mixnätet att behandla ett antal röster och jämför detta med tidigare implementationer av mixnät.

Questions to author:

- 1. Du nämner i texten att implementationen av mixnätet är skyddat mot CCA2 attacker. Vad är det?**
- 2. Du nämner att Röst-Servern (Vote server) har en stor inverkan på röstens säkerhet? Hur då? Du nämner också att det i din application inte är än säker röst server. Hur skulle man göra den säker?**
- 3. Används mix-net i svenska val? Om inte finns planer på det?**