NTNU | Norwegian University of Science and Technology

SODI - TESTING AV BRUKERDELEN AV SIKKERHETEN TIL ELEKTRONISKE IDENTIFIKASJONSPROTOKOLLER

Katrien De Moor **Ole Martin Edstrøm**
Kristian Gjøsteen Anna Storli Tveit

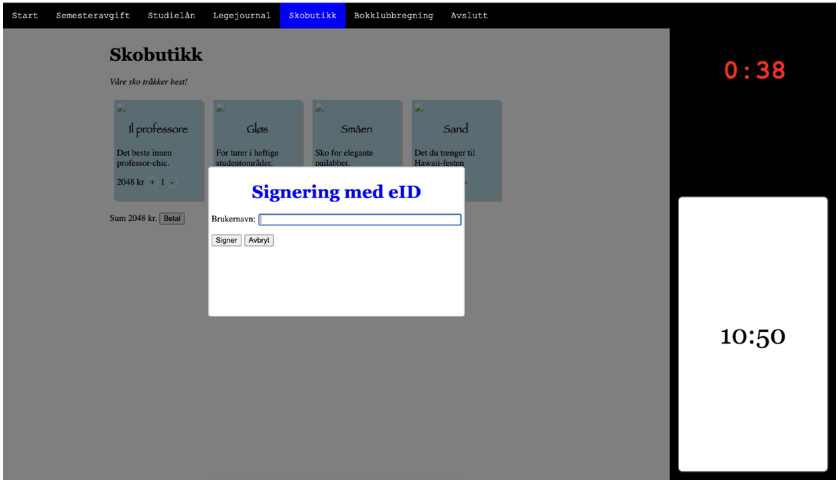
8. juni, 2023

eID-systemet

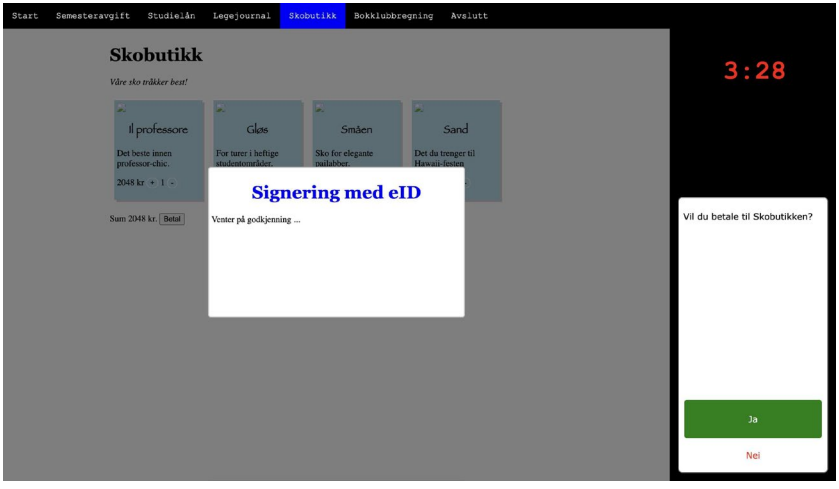
- Brukeren fyller først inn et brukernavn, og godkjenner deretter innloggingen/signeringen ved å trykke “Ja” på telefonen.
- Telefonen viser en melding som spør om brukeren vil gjøre det datamaskinen prøvde å gjøre.

Så det systemet vi testet, var en eID-protokoll som verken brukte passord eller kontrollsiffer.

eID-systemet



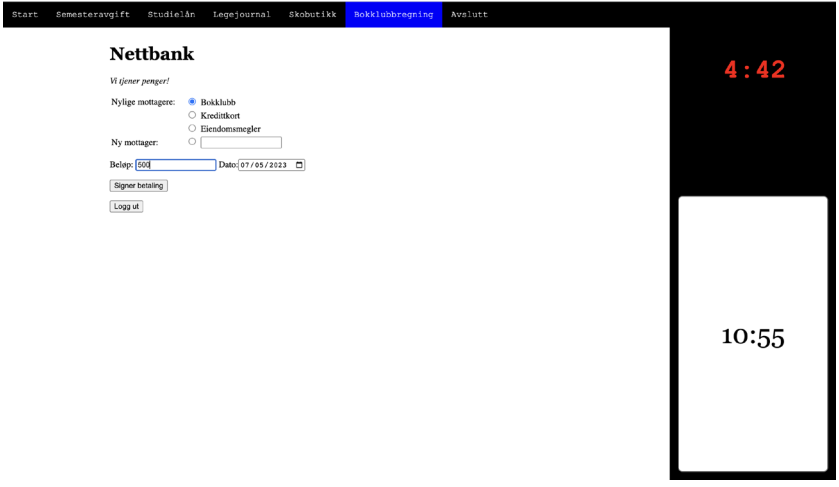
eID-systemet



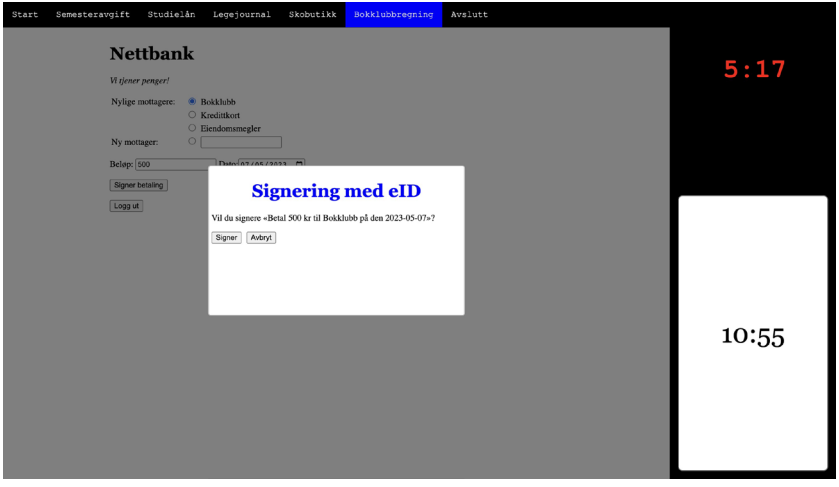
Det simulerte angrepet

- Vi simulerte et angrep hvor brukeren sin PC var kompromittert.
- Angriperen kunne kontrollere hva som vises på PC-skjermen.
- På PC-skjermen ville det se ut som om brukeren prøvde å gjøre en bankoverføring til “Bokklubben”, mens telefonen ville spørre om brukeren hadde lyst til å betale til “Eiendomsmegler”.
- Angrepet ville kun skje den første gangen brukeren prøvde å gjøre overføringen.

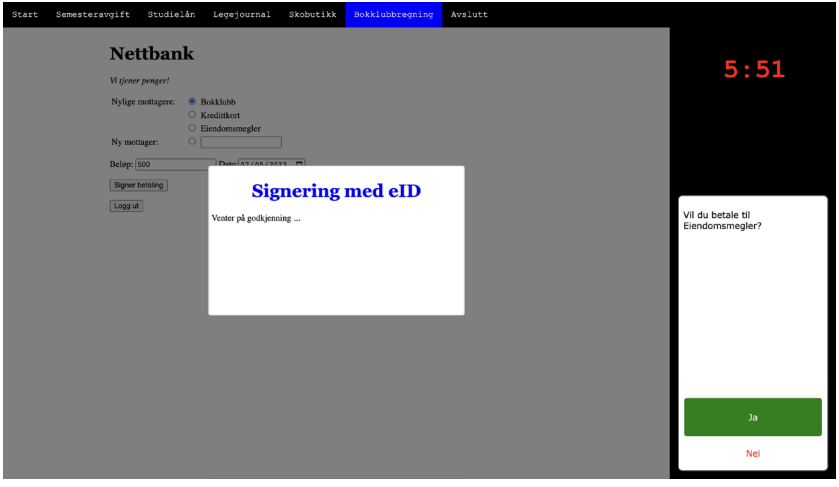
Det simulerte angrepet



Det simulerte angrepet



Det simulerte angrepet



Hva ønsket vi å teste

- Vi ønsket å teste hvordan brukerne ville reagere på angrepet, og om de ville reagere i det hele tatt.
- Vi ønsket at dette skulle simulere virkeligheten så nær som mulig ved å simulere:
  - Stress
  - Muskelminne

Hvordan simulerte vi dette i lab

- For å simulere en liten mengde med stress:
  - En stoppeklokke øverst i høyre hjørne som tok tiden de brukte på eksperimentet.
  - De kunne gå når de var ferdig med eksperimentet.
- For å simulere muskelminne, fikk vi dem til å gjøre totalt fem oppgaver som inkluderte seks bruk av eID-protokollen.
- Vi simulerte mobiltelefonen som en del av PC-skjermen, men tvang dem til å bruke touch-skjerm.
  - Vi tenkte dessverre ikke på venstrehendte da vi satte opp simuleringen.

Gjennomføring av eksperimentet

- Rekrutteringen foregikk i pausen til en Matematikk 3-forelesning ved NTNU.
- 40 meldte seg på. 35 møtte opp. 19 kvinner og 16 menn. Alle i en alder mellom 19 og 22.
- Vi startet med å "forklare" eksperimentet til brukerene.
- Vi fikk dem til å lese igjennom og signere et informasjonsskriv.
- Deretter svarte de på to spørreskjemaer og gjennomførte de fem oppgavene. Mens de gjorde oppgavene prøvde vi å gjøre oss mest mulig usynlig.

Resultater og Diskusjon

- Resultatene fra to av deltagerne ble forkastet ettersom de ikke ble utsatt for angrepet.
- 22 godkjente betalingen (15 kvinner, 7 menn), og 11 godkjente den ikke (3 kvinner, 8 menn).
- Av de 11 som ikke godkjente, tenkte 4 av dem ikke på det som et angrep.
  - "Tolket ikke feilen som et angrep, men som en feil"
  - "Av og til ble det oppgitt feil motaker på godkjenning av bank-id. Ellers veldig lett"
  - Noen av dem kom med kommentar underveis i eksperimentet at de hadde funnet en bug i programmet vårt.

Resultater og Diskusjon

- Av de 22 som godkjente, sa 7 av dem at det var et angrep, eller at de var usikre, men ga en kommentar (2 til var usikre, men kom ikke med noen annen kommentar).
  - "Vanskelig å si, men det kom opp eiendomsmegler i nettbanken da jeg hadde trykket at jeg skulle betale bokklubben, så det fikk meg til å bli litt usikker. Det kan dermed kanskje tolkes som et slags "angrep""
- 1 av dem kommenterte helt feil ting som angrep.
- Minst 2 så at det var feil rett etter at de hadde trykket "Ja"-knappen.
  - "var for rask til å trykke ok, men rakk akkurat å se at jeg trykket ok til eiendomsmegling i stedet for bokklubb i siste oppgave"
- Minst 3 som aksepterte kun fordi de trodde det var en feil fra vår side.

Fler Resultater og Diskusjon

- Brukerne følte oppgavene var veldig enkle, gjennomsnitt på 4.84 av 5.
  - "veldig lett og enkelt konsept"
- De ville ikke sett det på som om de var distraherte, ble et gjennomsnitt på 1.33 av 5.
- På sikkerhetsfølelsen, varierte svarene veldig (men varierte ikke på om folk så angrepet eller ikke) 2.76 av 5. De fleste klagde på mangelen av passord.
  - "Det føles noe usikkert når man ikke må skrive inn noen passord. Altså kan hvem som helst godkjenne fra min mobil."
  - "Det var litt uvant å ikke måtte skrive inn passord eller lignende, men med tanke på 2-faktor bekreftelsen med mobilen, så føltes det egentlig ganske greit. Jeg tror ikke jeg hadde tenkt over at det var utrygt hvis jeg ble bedt om å betale eller verifisere meg på denne måten."

Spørsmål?