Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Sosiale Medier, e-IDer og Personvern

Innføring i begrepene og tema til e-Me oppstartmøte

Dr. Lothar Fritsch

Norsk Regnesentral

Oslo

2. September 2010

Lothar Fritsch

- Forsker innenfor IKT Sikkerhet, Personvernsteknologi og e-ID hos Norsk Regnesentral
- Mastergrad i informatikk, spesialist i informasjonssikkerhet
- Industrierfaring som Product Manager
- Doktorgrad i Frankfurt's Goethe-Universitet innenfor "Information Systems"-avdeling i økonomisk fakultet. Fokus på personvern i mobilapplikasjoner
- Jobber med forskjellige prosjekter i Norge og EU-sammenheng

Web: ***http://www.nr.no/ ~lothar***

Agenda

1. Sosiale medier og sosiale nettverk
   – hva er det egentlig?
2. Kort innføring i elektroniske identiteter
   - spesielt med fokus på sikkerhet og personvern
3. Personvernsøkende teknologi (PET) – hva fins, og hva skjer i forskning?

Sosiale nettverk, sosiale medier

- "The term social software characterises infrastructures, platforms and applications that enable users to communicate, collaborate and coordinate themselves via networks, to establish and maintain relationships and thus in some way map social aspects of real life to an online environment."
- Its main functions are:
  - Information Management: finding, evaluating and administration of information
  - Self Management: present aspects of yourself on the Internet
  - Relationship Management: represent and maintain contacts to others via Internet"

(A comparison of privacy issues in collaborative workspaces and social networks, Martin Pekárek & Stefanie Pötzsch, IDIS journal 2009:2, PrimeLife project; Boyd/Ellison 2007)

Sosiale nettverk, sosiale medier

- "Regardless of the purpose of a WBSN, one of the main reasons for participating is to share and exchange information with other users. "

(Carminati et al: Enforcing Access Control in Web-based social networks, ACM Transactions on Information and System Security 2009:1)

Oppsummering Sosiale Nettverk

- Sosiale nettverk er plattformer på nett som krever personlig innlogging og opprettelse av et profil
- Transaksjoner på plattform er enten rettet til egne eller fremmede dataobjekter (”medier”), eller til andre bruker igjennom en modell av sosiale relasjoner og meldingstjenester
- Det fins muligheter til å beskytte sine egne medier med adgangskontrollregler for andre bruker eller grupper av brukere
- Formål til en sosjal nettverk er avgjørende for hvilke informasjoner fins, og hva de der brukt tila

Agenda

1. Sosiale medier og sosiale nettverk
   – hva er dette egentlig?
2. Kort innføring i elektroniske identiteter
   - spesielt med fokus på sikkerhet og personvern
3. Personvernsøkende teknologi (PET) – hva fins, og hva skjer i forskning?

Hva er en e-ID?

- …en liten bit digital data basert på algoritmer i programmvare eller i hardware som skal overbevise en datamaskin at en visst person sitter foran maskinen
- e-IDer kan være tilknyttet til en ”offisiell” identitet, for eksempel en pass eller en personnummer
- Mange e-IDer er tilknyttet til ”myke” identiteter: e-post-adresser, brukerpseudonymer, …
- E-IDer brukes til ulike formål
- E-IDer er tilknyttet til en kommunikasjonskanal, eller ikke
- E-IDer og silknytning til identitet kan være styrt av brukeren selv (valg av pseudonym eller ID i OpenID), eller påtvunget (pass fra staten, MinID)

Hvorfor brukes e-ID'er?

- Identifisering
  Hvem er brukeren – ved innlogging eller forvalting av personopplysninger i databaser
- Autentisering
  Er det virkelig brukeren? Bevis det!
- Autorisering
  Legitimering av transaksjoner basert på en e-ID. Betyr ofte at man kan ikke nekter transaksjon.

e-ID og Datasikkerhet

- ID-tyveri og andre trusler for e-IDer er avhengig av:
  - Kan e-ID kopieres?
  - Kan e-ID brukes fra en annet sted?
  - Kan e-ID brukes uten videre, hemmelige utlysninger (for eksempel PIN-koder)?
  - Flyttes det avgjørende informasjoner sikker over åpne nettverk (for eksempel SMS-meldinger med PIN-koder)?
  - Kan e-ID verifiseres mot brukeren slik at det oppdages bruk av stjalet e-ID?

e-ID og Personvern

- e-IDer kan på forskjellige måter skape personvernsrisiko:
  - e-IDer kan inneholder navn, fødseldato eller andre opplysninger som ikke er nødvendig for alle transaksjoner
  - Bruk av samme e-ID kan sammenknytte forskjellige databaser, applikasjoner og organisasjoner slik at personopplysninger kombineres veldig lett
  - Data som IP-adresser forvandles til en e-ID med stor sporingspotensial hvis tjenesteleverandøre og applikasjonseiere tar de i bruk som ID
  - Tilknytting av nye informasjonereller nye tjenester til en e-ID kan skape store personvernsutfordringer (for eksempel name-tagging i digital fotoalbum, bruk av Google-konto igjennom Facebook)

Oppsummering e-ID

- e-ID brukes til forskjellige formål i applikasjoner og tjenester på nett
- Hvilke opplysninger må tilknyttes til en e-ID for å lage en trygg transaksjon er helt avhengig av applikasjoner som tar i bruk e-IDer
- En e-ID system som utvider bruksområdet til nye applikasjoner kan skape trusler både for den opprinelige applikasjon, den nye område, eller for brukerens personvern
- Løsninger på marked tilbyr varierende sikkerhets- og personvernsegenskaper

Agenda

1. Sosiale medier og sosiale nettverk
   – hva er dette egentlig?
2. Kort innføring i elektroniske identiteter
   - spesielt med fokus på sikkerhet og personvern
3. Personvernsøkende teknologi (PET) – hva fins, og hva skjer i forskning?

Personvernsøkende Teknologi

- Forskningsfelt som baserer seg på å utvikle IKT for å implementere personvernsegenskaper i IKT-systemer
- Bruker vanligvis kryptografi og sikkerhetsteknologi for å lage spesielle protokoller og metoder for interaksjon på nett og databehandling
- Omhandler anonymitet, pseudonymer, usporbarhet på nett, transparens i databehandling, og metoder til datapolicy-enforcement

Anonymisering og Usporbarhet

- Anonymisering av internett-trafikk
  - Heter ”MIX”, oppfunnet i 1980-tallet av David Chaum
  - Mange forskjellige implementeringer, e.eks. AN.ON or TOR.
  - Kommersielle produkter: JONDONYM-proxy, XEROBANK-nettleser
- Anonymisering av e-post
  - MixMaster-tjener bruker kryptografi og MIX-konsept for å levere anonyme, krypterte e-poster
  - Mulighet til å bruke krypterte svaradresser

Pseudonymer, ID og sporbarhet

- Mange applikasjoner, kommunikasjonsmetoder og databaser baserer seg på en persons identidet
  - E-post-adresser eller fødselnummer er eksempler
  - Bruk av samme IDer gir mulighet til å spore og profilere hva en person gjør
- Det anbefales bruk av forskjellige pseudonymer og roller i forskjellige applikasjons- og livssammenheng.
  - Dette heter ”identitetsforvalting” (Identity Management – IDM)
  - IDM som inneholder PET og tilbyr gode personvernsegenskaper og god sikekrhetsnivå heter ”personvernstøttende identitetsforvaltning”

Oppsummering PET

- Det fins mange løsninger som øker personvern og sikkerhet i e-ID-systemer
- Mange løsninger er lite brukt utenfor laborer – det trengs utforskning i praksis
- Dagens valg av e-ID i applikasjoner er lite basert på personverns-hensyn
- Dagens e-ID-systemer er sjelden valgt med brukerinvolvering eller -evaluering