Welcome to

Version2 evalg

Henrik Lund Kramshøj, internet samurai
hlk@solido.net

http://www.solidonetworks.com

Slides are available as PDF

Formål

Runde 1:
Oplæg ved Henrik Kramshøj: Kan man garantere stemmehemmelighed? (3 min)

Idag blyanten

Stemmehemmelighed idag er baseret på en stemmeseddel som udleveres ved et bord, en kort gåtur hen til stemmeboksen, valghandlingen med kryds, foldning og aflevering i en stor boks - under opmærksom overvågning fra valgtilforordnede.

Bryder man det ned i elementer er hvert enkelt komponent meget overskuelig.

Stemmehemmelighed ved blyanten

Under handlingen med den fysiske stemmeseddel er borgen istand til at skjule hvor krydset sættes, og afleverer sedlen i en boks med mange andre ens stemmesedler, som er krydset med samme blyant - ligner hinanden til forveksling.

Borgeren kan verificere processen nemt - overskuelige komponenter

Evalgsplatformen

Stemmehemmelighed på en evalgsplatform vil introducere flere nye komponenter, specielt hardware og software programmel.

Hardware idag findes i mange varianter og det er muligt at finde meget simple stykker hardware Programmel kan idag skrives i et utal af programmeringssprog og er idag typisk højniveau sprog.

Stemmehemmelighed bygger på at ingen kan se med under eller efter handlingen. Det betyder at de nye komponenter skal være resistente overfor truslerne og de fejl det kan medføre.

Computeren skal registrere og gemme data

Den elektroniske stemmeseddel bygger på at der registreres et valg i en computer, som skal gemmes til optællingen foretages. Det nærliggende når man registrerer data er at sikre integritet og tilgængelighed. Dertil kan vælges fortrolighed. Både hardware og programmel skal altså være udviklet for at tage højde for trusler.

Specielt sikring af stemmehemmelighed fordrer altså nøje kontrol med hardwaren - undgå aflytning, enten direkte med kabel eller over aflæsning af signaler fra udstyret. Hvis hardwaren er enkeltstående enheder skal der aflæses stemmer efter, og hvis det er et netværk af computere skal der sikres mod aflytning under transmissionen.

Aflytning af signaler

Tempest aflytning hvor man aflytter data på afstand findes og er demonstreret flere gange.

Aflytning af netværk

Aflytning af netværk eksempelvis Ethernet er demonstreret flere gange og kan også ske ved introduktion af bridges - som fysisk kan være meget små

Beskyttelse mod aflytning under transmission er typisk baseret på kryptering - men dette komplicerer yderligere setup og gør debugging sværere.

Indsamling og optælling af data

Indsamlingen af data skal sikre at alle data indsamles, og dette gøre korrekt.

Et netværk af valgcomputere vil således lette optællingen, fordi man ikke skal rundt til hver enkelt efterfølgende, men vil forværre risikoen for at der kan aflyttes. Enkeltstående computere vil være mere sårbare overfor nedbrud - hvis en computer dør vil stemmerne på denne være forsvundet. Processen til at indsamle stemmerne skal ligeledes kræve stærk autentifikation - hvilket vil komplicere processen for dem som skal indsamle.

Jeg vil slet ikke begynde at tænke på den risiko der introduceres hvis man tænker trådløse protokoller til kommunikation mellem stemmecomputere og optælling.

Aflytning i softwaren

Aflytning af softwaren skal sikre at der ikke gemmes data som senere kan bruges til at identificere borgere.

Programmerne på computeren skal kunne præsentere den elektroniske stemmeseddel til borgen og det kræver styreprogrammer til enhederne, data som skal vises på en skærm og modtagelse af tryk fra borgeren. Antager her en trykfølsom skærm fremfor mus og tastatur.

Det typiske miljø vi ser indenfor embedded computing idag er Windows CE, Windows NT4(Metroen i København) og diverse Linuxvarianter.

Allesammen vil efter min mening være svære at validere - altså sikre at de opfører sig som forventet.

Brugervenlighed

Evalgløsningen er mere avanceret end blyanten, og selvom en udvikler altid vil sige løsningen er nem at bruge så viser det sig ofte at der er problemer.

Mulige problemer - baseret på egne erfaringer:

- Kalibrering er forkert, trykket opfattes ikke samme sted som brugeren trykker
- Tryk registreres ikke grundet kolde eller tørre fingre
- Skærmene er ikke altid robuste nok til at håndtere ”hårde tryk”
- Skærmene er ikke altid lige gode - utydelige eller udtværede
- Selv det at bladre på skærmen (Scrolling) er et problem - så hvis der er mange kandidater kan det blive et problem

Hvis der er problemer med brugervenligheden skal man tilkalde assistance, og derved er stemmehemmeligheden røget.

Runde 3: Sikkerhed

Oplæg ved Henrik Kramshøj om sikkerhedskrav til e-valgssystemer og de problemer, det giver.

Hvad er sikkerhed?
Høje krav = dyrt/umuligt at lave helt sikkert og sabotagebeskyttet system.

TL;DR crowdsourcing og åbenhed er nødvendigt

To pointer

Terminologi

Sikkerhed og sikre valg - hvad betyder det, og for hvem

One size fits nobody!

Malice

Lad mig starte med at sige jeg ikke tror nogen af de nuværende parter har ondt i sinde.

Desværre sker der meget ondt i verden som følge af de bedste intentioner. Ligeledes har PHK for vane at henvise til Hanlon's Razor is an eponymous adage that reads:

> Never attribute to malice that which is adequately explained by stupidity.

Min opgave som sikkerhedsmand med viden om IT-sikkerhed og hacking er at gøre opmærksom på at enhver form for evalgshandling vil blive forsøgt hacker, subvertet, ændret og vi skal være forberedt på dette. Hvis man udelukkende fokuserer på goderne ved evalg og ignorerer advarslerne står vi en nær fremtid med valg vi ikke kan stole på.

Terminologi

Identifikation (identification) - dette er allerede introduceret i valghandlingerne, den elektroniske registrering virker og influerer ikke på selve valget.

Autentifikation (authentication) - er du den du påstår du er.

Autorisation (authorization) - har du lov til at udføre den handling der ønskes

CIA modellen

Sikkerhed ud fra CIA modellen

Fortrolighed (confidentiality) - at holde informationer hemmelige

Integritet (integrity) - er informationerne intakte, er der sket modifikation af data

Tilgængelighed (availability) - er information tilgængelig for dem som skal anvende den

Yderligere funktionalitet kan diskuteres om det er afledt eller selvstændige dele, eksempelvis Digitale signaturer, som medfører uafviselighed (non-repudiation)

One size fits nobody

Sikkerhed er en funktion af ressourcer og tid, mere tid - mere sikkerhed, flere ressourcer - mere sikkerhed 100

Et system til evalg vil naturligt kræve yderligere ressourcer end mange andre tilsvarende ”kioskløsninger” og billeteringssystemer.

Når vi så samtidig ser at selv et system til billetering i Danmark som har økonomisk incitament til at minimere svindel vælger en usikker teknologi er jeg ikke overbevist om at der afsættes passende ressourcer til en evalgsløsning som skal benyttes sjældent.

Åbenhed

Åbenhed om evalgsløsningen er et ufravigeligt krav til løsningen. Hvis der ikke kan fremlægges alle data, specifikationer for hardwaren og programmel der afvikles er det et usikkert system.

Usikkert fordi vi skal have tillid til producenten. Bemærk: tillid er ikke bare tillid til at de vil os det godt og gør deres bedste, men tillid til at deres kompetencer og anvendte teknologi på alle niveauer er fuldstænding og resulterer i de forventede resultater.

Forslag vær realistiske

Jeg melder mig gerne til en angrebsgruppe som pro-bono gennemlæser alle forslag til evalgsløsningerne - og jeg forventer at vi får lejlighed til at hacke på eksemplarer af evalgscomputere. Det vil være nødvendigt at inkludere hackere tidligt i arbejdsprocessen således at både åbenlyse og mere kreative muligheder for at influere på resultatet afdækkes.

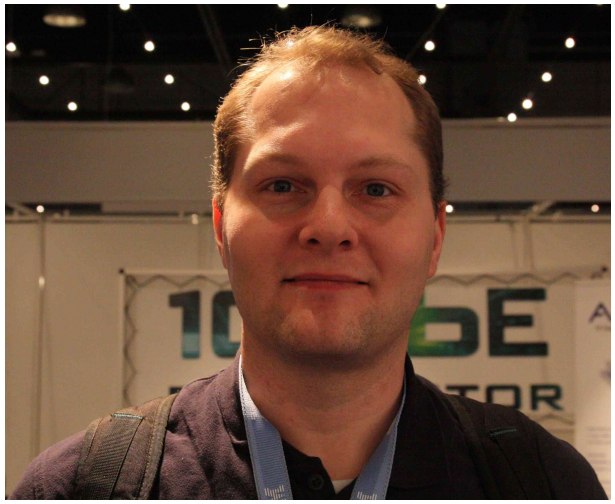
Alt andet vil være en større trussel og ingen valg med uafprøvede evalgscomputere vil være sikkert.

Non-disclosure

Mht. Nondisclosure vil det være umuligt, hvorimod en konkurrenceklausul måske kan komme på tale. Aka, du må læse alt og referere hvis sikkerheden skrider, men du må ikke bruge din viden til at starte en konkurrent.

Eksempler på hacks findes fra mange sikkerhedskonferencer og mange hacks er forbløffende simple at udføre i praksis http://hackaday.com/2005/12/25/tempest-for-eliza/ http://hackaday.com/tag/tempest/

Contact information



- Henrik Lund Kramshøj, IT-security and internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- CISSP certified
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS