Open standaarden voor security en privacy

Bart Jacobs

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

Open Overheid Congres, 31/5/2012

Outline

Openheid & Security

Openheid & privacy: project "Irma"

Conclusies

Auguste Kerckhoffs (1835 – 1903)

Nederlands cryptograaf, werkzaam als hoogleraar in Parijs.

(Gezamelijke computer security master programma van Eindhoven, Twente & Nijmegen is naar hem genoemd.)

Publiceerde in *La Cryptographie Militaire* (1883) het beroemde Kerckhoffs' principe:

> *La sécurité d'un cryptosystème ne doit reposer que sur le secret de la clef.*

- De kracht van een cryptosysteem mag slechts berusten op de vertrouwelijkheid van de crypografische sleutel
- Dus niet op: geheimhouding van het systeem zelf!

Analogie met gewone sloten

In welke slotenmaker heeft u meer vertrouwen?

1. in degene die de werking van zijn sloten geheim houdt, zodat dieven die kennis niet kunnen misbruiken?
2. of in degene die de werking van de sloten publiceert, waarbij:
   - iedereen kan zien hoe goed/slecht ze zijn;
   - u vertrouwt op de complexiteit van de sleutel voor bescherming.

Eenzelfde discussie bestaat voor ICT-standaarden / designs / protocollen / software (implementaties).

Moderne versie van Kerckhoffs' principe

Het openlijk publiceren van designs en protocollen draagt bij aan de beveiliging van systemen die er op gebaseerd zijn.

No security through obscurity.

Dit is tegen-intuitief, maar wordt inmiddels breed gedeeld binnen de computer security gemeenschap.

Bekende "security through obscurity" blunders

- Mifare Classic chip oa. in OV-chipkaart en (oude) rijkspas
  - ontwerp van begin jaren 90, vol cryptografische stupiditeiten
- Content Scrambling System (CSS) waarmee DVD's alleen op speciale apparaten afgespeeld konden worden
  - werd snel ge-reverse-engineerd, resulterend in DeCSS
  - CSS implementatie bleek vol fouten en zwakheden te zitten
  - uiteindelijk helemaal opgegeven.
- GSM: ontwikkeld in het geheim
  - A5 stream cipher and A3/A8 hash algorithmen lekten toch uit
  - Vervolgens bleken ze makkelijk te breken
  - GSM is nu relatief eenvoudig af te luisteren: gebakken peren!
  - (opvolger UMTS werkt wel met open standaarden/protocollen)

Argumenten *voor* openheid (van software)

- Snelle detectie en correctie van fouten (*bugs*)
  - tenminste voor actief gebruikte en ondersteunde systemen
- Programmeurs produceren betere code wanneer iedereen hun werk kan zien
- Minder risico op *backdoors* (zeer actueel!)
- Flexibiliteit:
  - minimale & afgeslankte installaties mogelijk (bijv. in embedded systems)
  - onafhankelijkheid van leverancier, ook voor patching
  - iedereen kan de de kwaliteit beoordelen — in principe

Argumenten *tegen* geslotenheid

- Geslotenheid geeft een vals gevoel van veilighied: security by obscurity werkt niet
- Impliciet gebruikte assumptie: het verborgene is correct (niet onze ervaring ☹)
- Maar *bugs* worden iedere dag gevonden in gesloten software
- source code lekt vaak toch uit: hooguit tijdelijk voordeel van niet-openbaarheid.
- Vertrouwen in wat de software werkelijk doet is een probleem

Zie ook: J.-H. Hoepman, B. Jacobs, *Increased security through open source*, Communications of the ACM 50, 2007.

Acceptatie van nieuwe cryptografische algoritmen

- Een nieuw cryptografisch algorithm wordt enkel nog als standaard geaccepteerd na een publieke competitie
- Organisator: Amerikaanse NIST = National Institute for Standards and Technologies
- Deelnemers: wie maar wil; bijdragen zijn openbaar, en de langdurige beoordelingen ook.
- Bekendste uitkomsten:
  - AES = Advanced Encryption Standard, ontworpen door Leuvense collega's
  - SHA-3, het nieuwe hash algorithme, met nog 5 overblijvers in de laatste ronde; besluit later in 2012

Wie bent u? Identiteiten en attributen

- Wanneer u een fles whiskey wil kopen, moet u laten zien dat u boven de 18 bent.
- In de (offline) praktijk, zwaait u even met een identiteitsbewijs voor de ogen van de slijter
- Maar wat als de slijter een copie maakt van uw ID?
  - online is dit nog veel problematischer

De transaction vereist enkel het attribuut "boven de 18"

- en niet uw precieze identiteit (wat dat ook moge zijn)
- alle additionele informatie, behalve "boven de 18", is overbodig en kan misbruikt worden (identiteitsfraude, profilering)
- gebruik van attributen is privacy-vriendelijk en past uitstekend bij data minimalisatie vereisten

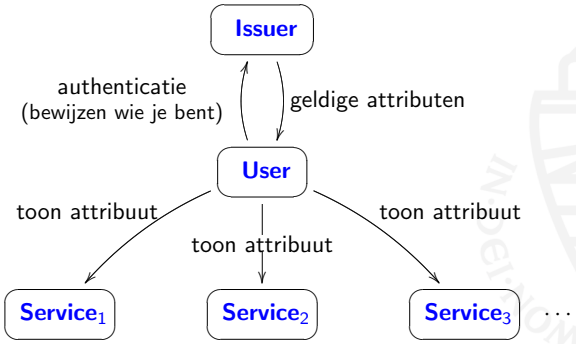
Attribuut-gebaseerde authenticatie & authorisatie

- Veel transacties kunnen plaatsvinden op basis van attributen:
  - goedkopere knipbeurt voor studenten, of goedkoper met de bus voor bejaarden
  - deelname aan een locaal referendum
  - online games kopen ("boven de 12/16"), of sommige items bekijken op `uitzendinggemist.nl`
  - bezorgadres bij online aankopen
- Bij veel digitaliseringsprojecten zijn attributen vervangen door identiteiten
  - bijv. in openbaar vervoer, via OV-chipkaart
  - kaart heeft uniek nummer, dat aan een persoon gekoppeld is (of kan worden)
  - attributen zijn flexibeler: sommige zijn identificerend, en anderen niet

Project **Irma** = I reveal my attributes

- **Idee**: gebruik moderne cryptografische technieken voor het beheer van persoonlijke attributen op eigen chipkaart
- Per transactie zijn bepaalde attributen nodig: alleen die attributen worden getoond — en verder niks
- De kaarthouder kan nieuwe, geldige attributen op de kaart downloaden, en later tonen, bijv. bij een webshop
  - die attributen zijn afkomstig van een issuer
  - ze worden getoond bij een dienstverlener, binnen een transactie

Attribuut issue/gebruik model



Typisch zijn er meerdere issuers (bijv. overheid, banken, isp's, ...)

Onder de motorkap van Irma

- Er zijn twee cryptografische technieken beschikbaar
  - U-Prove van Microsoft
  - Idemix van IBM
- Nijmeegse bijdrage: snelle implementaties op chipkaarten, van beide systemen
  - transactietijden in de orde van 1-2 seconden
- Beiden zijn open technologieën, met vrij beschikbare voorbeeld implementaties en documentatie
- Beiden realiseren ze basale security & privacy-bescherming:
  - attributen zijn niet overdraagbaar (gekoppeld aan de kaart)
  - issuer kan niet volgen waar je welke attributen gebruikt
  - bij Idemix: meervoudig gebruik van hetzelfde attribuut kan ook niet gekoppeld worden

Irma pilot project plannen

- Na de zomer 2012: uitreiking van ±100 kaarten aan (Kerckhoffs) master studenten
- Bruikbaar voor gratis printen, goedkopere koffie, toegang tot afgeschermde webpagina's, ...
- Huidige partners: Radboud Universiteit Nijmegen, Surfnet, TNO, Novay
- Bent u serieus geïnteresseerd om aan deze pilot bij te dragen?
  - bijv. als attribuut issuer of attribuut gebruiker (dienstverlener)?
  - dit vereist forse eigen inzet, en financiële bijdrage (bijv. voor extra kaarten, kaartlezers, programmeerwerk)
  - ook vereist: ondersteuning van open technologie aanpak
  - in dat geval, stuur een email naar bart@cs.ru.nl

Afsluitende opmerkingen

- Openheid van technologie is de norm voor grote ICT-projecten
- Geslotenheid leidt to zwakke security, door onvoldoende kritistische toetsing
- Openheid/transparantie is vereist voor geloofwaardige privacy bescherming
- Attributen zijn "the next thing" in flexibel en privacy-vriendelijk identity management

Tenslotte: Hoe ziet een open overheid er voor u uit?

met in het volgende kabinet een bewindspersoon voor ICT,
die open standaarden en transparantie tot regel verheft,
bij (semi)publieke ICT-infrastructuur.