



Geheim!

FACULTY OF SCIENCE

Bart Jacobs

Geheim!

Radboud University Nijmegen



Jacobs – Parallele Werelden, 8/12/08 – p.1/26



Geheim!

## Inhoud

- I. Achtergrond (mn. informatiebeveiliging)
- II. Parallelen
- III. Geheimhouding van ontwerp
- IV. Geheimhouding van fouten
- V. Conclusies



Jacobs – Parallele Werelden, 8/12/08 – p.1/26



## I. Achtergrond

## Wie is die man eigenlijk?

- Hoogleraar computerbeveiliging, in Nijmegen & Eindhoven (studie: wiskunde + filosofie)
- Wetenschappelijke achtergrond in logica, categorieëentheorie, semantiek van programmeertalen, security
- Betrokken oa. bij **e-paspoort**, **OV-chip**, **rekeningrijden**, **elektronisch stemmen** (lid cie. Korthals Altes over herinrichting stemmen)
- Auteur van online boek *De Menselijke Maat in ICT*, zie [www.cs.ru.nl/B.Jacobs/MM](http://www.cs.ru.nl/B.Jacobs/MM)

Jacobs – Parallele Werelden, 8/12/08 – p.2/26

Jacobs – Parallele Werelden, 8/12/08 – p.3/26



Geheim!

## Computerbeveiliging

- Regulering van toegang tot gevoelige digitale gegevens, zoals:
  - militaire of industriële gegevens
  - privacy-gevoelige gegevens, bijv. over gezondheid (EPD), communicatie, financiën
- Vereist juiste mix van technologische, organisatorische & juridische maatregelen
- Toegang tot informatie (ICT-architectuur) in hoge mate politiek (bijv. bij OV of rekeningrijden)
- Focus niet op functionaliteit van ICT, maar mogelijk misbruik

Jacobs – Parallele Werelden, 8/12/08 – p.4/26



## II. Parallelen

Jacobs – Parallele Werelden, 8/12/08 – p.5/26



Geheim!

## Wisselwerking met Wiskunde

- Belang van **Math** voor **CS** onomstreden
  - primair discreet & logisch, voor specificatie & verificatie van systemen met veel toestanden
  - ook continu & probabilistisch, voor externe interactie & patroonherkenning
- In CS security mn. getaltheorie, in bijv. priemfactorisatie (RSA) en elliptische krommen (Zie bijv. **EIPSI** samenwerking in Eindhoven)
- Ook invloed **CS** → **Math**, bijv. via tools als Mathematica (meer experimentele Math)

Jacobs – Parallele Werelden, 8/12/08 – p.6/26



Geheim!

## Wisselwerking met Sterrenkunde

- **CS** → **Astro** vooral algemene e-science:
  - beheer & gebruik van giga-data collecties
  - data omvang vergt real-time filtering voor opslag
  - **Astro** “zorgvuldig” met data (alleen observatie, geen reproduceerbaarheid)
- Andersom, **Astro** → **Cs**
  - deep space internet (Disruption-Tolerant Networking, door Vint Cerf)
  - ...

Jacobs – Parallele Werelden, 8/12/08 – p.7/26



Geheim!

## Security issues in *Astro*?

- Communicatie met satellieten is beveiligd, ivm. militaire en commerciële belangen
- Ook met ruimtesondes?  

  - überhaupt crypto? bestuurbaar van thuis uit?
  - vereiste grote schotel biedt bescherming (kunnen landen onderling verzieken?)
- **Anomaly detection** tbv. herkenning van terroristen & galactische explosies

Jacobs – Parallele Werelden, 8/12/08 – p.8/26



## III. Geheimhouding van ontwerp

Jacobs – Parallele Werelden, 8/12/08 – p.9/26



Geheim!

## Wetenschap en geheimen

- Slechte mix: wetenschap juist gericht op het onthullen van “geheimen van de natuur/...”
  - bedoeld: geheim als onbekendheid
  - Focus hier op: “niet-onbekende” geheimen
- Wel geheimen in wetenschappelijke proces:
  - bij beoordeling van artikelen
  - voordat ideeën gepubliceerd zijn (soms)
  - voordat patenten toegekend zijn
- Ook geheimen bij “strategische” kennis, bijv. over NBC wapens

Jacobs – Parallele Werelden, 8/12/08 – p.10/26



Geheim!

## Typisch voor informatiebeveiliging

- Topic: scheppen en onthullen van geheimen
- Veel mechanismen zijn geheim
  - Math/Astro doceert al het bekende
  - Veel beperkingen in security: bijv. werking e-autosleutel / e-bank calculator. . . onbekend.
- “Functionele” geheimen: geheimhouding onderdeel van beveiligingsmechanisme

Security through Obscurity !?!

- Al of niet openheid is hot topic

Jacobs – Parallele Werelden, 8/12/08 – p.11/26



Geheim!

## Slotenmaker voorbeeld

Welke slotenmaker vertrouw je meer? Beiden zeggen: ik heb hier een fantastisch slot,

- I. maar ik kan **niet vertellen** hoe het werkt, want dan weten de *bad guys* het ook, en kunnen ze dat misbruiken, maar vertrouw mij maar als specialist;
- II. **kijk maar**, iedereen kan zelf zien hoe (goed) het werkt; de beveiliging hangt enkel af van de kwaliteit van de sleutel.

Ipv. 'slot' ook 'OV-chip' of 'stemmachine' of ...

Jacobs – Parallele Werelden, 8/12/08 – p.12/26



Geheim!

## Geslotenheid: pros en cons

- + Bad guy wordt vertraagd
- Geen/nauwelijks kritische feedback
- Absoluut vertrouwen vereist in (geclaimde) professionaliteit
  - Grens professionaliteit–marketing onduidelijk
  - eventuele onafhankelijke evaluatie is noodzakelijkerwijs ook weer gesloten
- *Secrecy of convenience*: eigen zwakheden / fouten blijven langer verborgen
- + (Bescherming van *Intellectual Property*)

Jacobs – Parallele Werelden, 8/12/08 – p.14/26



Geheim!

## Openheid: pros en cons

- + Klant kan zelf (laten) oordelen
- + Systeemfouten worden sneller opgemerkt en verholpen (idealiter)
- Bad guys weten inderdaad meer
- + Mechanisme kan sowieso in “vijandige” handen vallen en achterhaald worden (Reeds gezien door Auguste Kerckhoffs, 1883)
- + Ontwerpers presteren beter wanneer ze weten dat hun resultaten openbaar zijn

Jacobs – Parallele Werelden, 8/12/08 – p.13/26



Geheim!

## Openheid op 4 niveaus

- I. Cryptografische algoritmen: bijna altijd open
- II. Systeemarchitectuur: meestal open
- III. Software: groeiende openheid via *open source*
- IV. Hardware: nauwelijks open

Jacobs – Parallele Werelden, 8/12/08 – p.15/26



Geheim!

## Obfuscatie (opzettelijke verwarring)

- Schrijf eerste “goede”, begrijpelijke software
- Haal dit door een obfuscatie tool: resultaat is onbegrijpelijke “spaghetti code” die hetzelfde doet; zet dit in een product
- Bemoeilijkt “reverse engineering”
- Gebruikt omwille van:
  - Security (through obscurity), mn. voor hardware
  - Bescherming intellectueel eigendom

Jacobs – Parallele Werelden, 8/12/08 – p.16/26



## IV. Geheimhouding van fouten

Jacobs – Parallele Werelden, 8/12/08 – p.17/26



Geheim!

## Medicijnen onderzoek analogie

- Medicijnonderzoekers willen natuurlijk effectieve middelen vinden
- Maar mogelijk blijkt dat veelgebruikt middel schadelijke bijwerkingen heeft.
- Wat dan?
  - Achterhouden moreel onacceptabel
  - Publicatie geeft spanning met producent en maatschappelijke onrust.
- Rug rechthouden en publiceren!

Jacobs – Parallele Werelden, 8/12/08 – p.18/26



Geheim!

## Mifare Classic chipkaart

- 85% v/d markt; wereldwijd  $\pm 1$  miljard verkocht, vnl. voor OV-betaling en toegang (OV-chip, Londen's Oyster, NL Defensiepas, . . .)



- Begin 90s ontwikkeld, met beperkte rekenkracht, encryptie met 48 bit sleutel, geheim algoritme (“crypto1”)

Jacobs – Parallele Werelden, 8/12/08 – p.19/26



Geheim!

## Mifare Classic is stuk

- 03/08 eerste aanval op RU-pas; overheid & NXP ingelicht; minister maakt openbaar
- Zeldzame combinatie van sterk wetenschappelijk werk & giga-impact
- “Security event of the year”
  - BBC world / Science / Times / Guardian / . . .
  - Ongeveer alle NL media
  - Politieke onrust rond OV-chipkaart, inclusief motie van wantrouwen voor staatssecretaris
- Nu ook “card-only” aanvallen: open geheugen

Jacobs – Parallele Werelden, 8/12/08 – p.20/26



Geheim!

## Wat te doen?

- RU strategie: *responsible disclosure*
  - Waarschuw: additionele maatregelen nodig
  - Wetenschappelijke publicatie later, na 7 mnd
  - Wel wiskundige details; geen attack software
- NXP strategie: *damage control*
  - 03/08: “Klant kiest zelf goedkoopste chip”
  - 07/08: “Publicatie onverantwoord”; kort geding
  - 10/08: Gebruik chip ontraden, voor nieuwe toepassingen

Jacobs – Parallele Werelden, 8/12/08 – p.21/26



Geheim!

## Deze fouten publiceren: pros en cons

- + Publiek heeft “right to know”; gegrond oordeel door specialisten nodig
- Geen vervanging mogelijk op korte termijn
- + Signaal bij publicatieverbod: bedrijven kunnen weggomen met zwakke producten
- Hoge kosten voor additionele maatregelen en vervanging
- + Zo werkt security onderzoek: negatieve resultaten zijn essentieel, bij gebrek aan wiskundig bewijs

Jacobs – Parallele Werelden, 8/12/08 – p.22/26



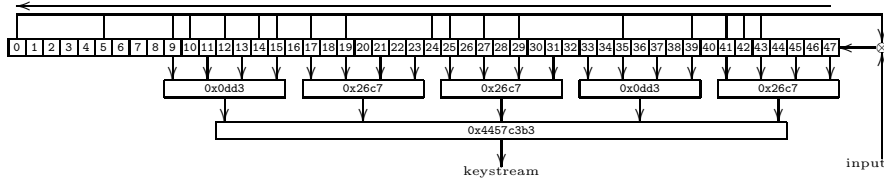
Geheim!

## Kort geding rechter, Arnhem, 18/07/08

- Geen publicatieverbod:
  - in abstracto vanwege: “freedom of expression”
  - in concreto vanwege: “economische en sociale ontwikkeling van de democratische maatschappij wordt in belangrijke mate mede bepaald door wetenschappelijk onderzoek”
- “. . . kans op schade in hoge mate toegerekend moet worden aan het produceren en in het verkeer brengen van een chip met intrinsieke manco’s, wat de verantwoordelijkheid van NXP is en niet van RUN c.s. die die manco’s slechts door onderzoek bloot hebben gelegd”

Jacobs – Parallele Werelden, 8/12/08 – p.23/26

## En toen mocht dit verschijnen ...




Jacobs – Parallele Werelden, 8/12/08 – p.24/26

## V. Conclusies

Jacobs – Parallele Werelden, 8/12/08 – p.25/26

## Belangrijkste punten

- Rechterlijke helderheid over:
  - belang onafhankelijk onderzoek
  - openheid èn zorgvuldigheid bij fouten
- Credit voor eigen onderzoeksgroep en dank voor steun van RU-CvB en anderen
- Mifare Classic in grote problemen:
  - gesloten en zwak ontwerp
  - OV-chipkaart is open portemonnee 
- Geheimen hebben beperkte houdbaarheid en beperkte rol!

Jacobs – Parallele Werelden, 8/12/08 – p.26/26