Stellingen

behorende bij het proefschrift

Reconciling Information Exchange and Confidentiality

A Formal Approach

van

Wouter Teepe

1. Privacybescherming en terrorismebestrijding zijn goed verenigbare belangen. (Hoofdstuk 8)
2. Het op de juiste manier koppelen van bestanden leidt tot een betere privacybescherming. (Hoofdstuk 7)
3. De BAN-logica is niet 'sound' (correct): het is mogelijk om uit ware aannames onjuiste conclusies te trekken. (Hoofdstuk 5)
4. Het tonen van de cryptografische hash van een bestand voldoet niet als bewijs van het kennen van de inhoud van het bestand. (Hoofdstuk 3)
5. Met slechts een niet-modificeerbaar, geauthenticeerd communicatiekanaal en een non-incrementele cryptografische hashfunctie is het mogelijk om een correct zero-knowledge interactief kennisbewijs te construeren. (Hoofdstuk 9)
6. Twee coöperatieve agents (A en B) met elk een verzameling (KB_A resp. KB_B) hoeven gemiddeld minder dan $3 \cdot |KB_A \cup KB_B| + k \cdot |KB_A \cap KB_B|$ bits te communiceren om de intersectie $KB_A \cap KB_B$ te bepalen, waarbij k een securityparameter is. (Hoofdstuk 10)
7. Men kan niet in alle redelijkheid van een persoon verwachten, dat wanneer hij een besluit neemt, hij daarbij hem bekende gegevens buiten beschouwing zal laten. (Frank Ankersmit, persoonlijke communicatie)
8. Wie confidentiële gegevens opslaat op een informatiedrager, moet bereid zijn afstand te doen van de fabrieksgarantie op die informatiedrager.
9. Het centrale RUG-emailadres is voor promovendi niet geschikt om als adres in een publicatie te gebruiken.
10. Als de faculteit GMW één euro bijdraagt aan het salaris van een promovendus, dan mag deze promovendus alléén bij de faculteit GMW promoveren. Inhoudelijke overwegingen doen hier helaas niets aan af.
11. De stemadviezen van de Stemwijzer zijn methodologisch gesproken slecht. Daarmee is de Stemwijzer een gevaar voor de democratie.
12. Stellingen die over stellingen gaan zijn altijd flauw.