

## Sikkerhed i Intelligente Hjem

Christian Damsgaard Jensen  
System Security Research Group  
Informatik og Matematisk Modellering  
Danmarks Tekniske Universitet

Christian.Jensen@imm.dtu.dk  
www.imm.dtu.dk/~cdj

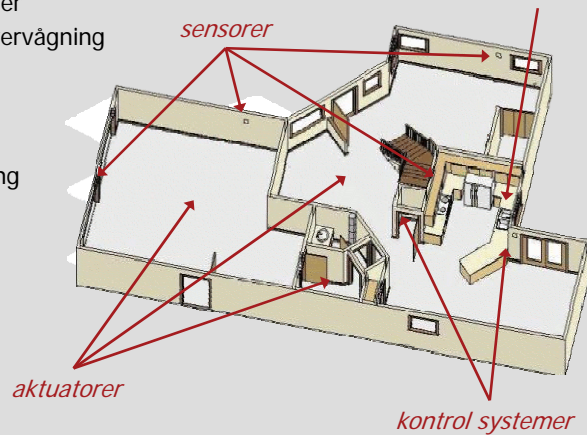
## Hvad Betyder Sikkerhed i Hjemmet

- Tryghed
  - Overvågning (tyveri-/overfaldsalarm, helbred, ...)
- Datasikkerhed
  - Hemmeligholdelse af opsamlede og lagrede data
    - Vanskeliggør overvågning udefra
  - Integritet af hjemmets intelligente systemer
    - Beskyttelse mod "spoofing" og "Man-in-the-middle" angreb
- Sikker kommunikation
  - Internt i hjemmet (intelligente systemer)
  - Eksterne leverandører af tjenester
- Privathed (privacy)
  - "Catch 22" situation
    - Skal opsamle personfølsomme data for at levere tjenester
    - Opsamling af personfølsomme data kompromiterer privathed



## Intelligente Hjem Konkurrerende Systemer

- Forskellige systemer
  - Alarmsystemer
  - Medicinsk overvågning
  - El-forbrug
  - Varme
  - Lys
  - Underholdning
  - Telefon
  - Internet
  - Etc.

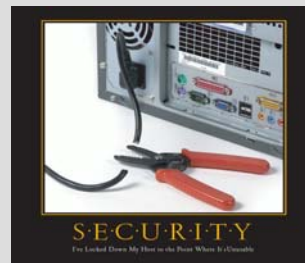


© Christian Damsgaard Jensen, 2007

3

## Tekniske Sikkerhedsudfordringer

- Sikker system Komposition
  - Udvælgelse af system komponenter
    - Service discovery
    - Device authentication
  - Konfiguration af system komponenter (hardware/software)
  - Opdatering af software komponenter
- Sikkerheds politikker
  - Specifikation
  - Integration
  - Evolution
- Interoperable sikkerhedsmekanismer
  - Autentifikation
    - User/Device authentication
  - Autorisation
    - Baseret på forskellige attributter i stedet for identitet



© Christian Damsgaard Jensen, 2007

4

## Praktiske Sikkerhedsudfordringer

- Mange forskellige konkurrerende systemer
  - Manglende standarder
    - For at sikre interoperabilitet benyttes normalt mindste fællesnævner
- Ringe efterspørgsel efter sikkerhed
  - Systemerne er endnu ikke udbredte nok til at sikkerheden er et synligt problem, så forbrugerne efterspørger den ikke
    - Vi er ved at gentage fejltagelsen omkring udviklingen af Internettet, f.eks. er problemet med SPAM et resultat af manglende autentifikation
  - Producenter udvikler ikke sikre løsninger uden dokumenteret behov
- Ringe opmærksomhed omkring sikkerhedsproblemer i hjemmet
  - Vi har ikke de rigtige abstraktioner til at tale om sikkerhed i hjemmet
    - Vi er ikke vant til at vore "møbler" snakker sammen
  - Systemudviklere er ikke uddannet til at tænke på sikkerhed
    - Datasikkerhed er ikke et obligatorisk emne på uddannelser til arkitekt, datalog, designer eller ingeniør

## Løsning af Sikkerhedsudfordringer

- Udvikling af åbne standarder til at sikre interoperabilitet
  - Forskellige devices og services skal kunne bruge hinanden
    - *Service oriented architectures?*
  - Sikkerhed skal inkluderes i standarder
- Udvikling af åbne systemer
  - Baseret på de åbne standarder
    - Sikrer interoperabilitet
  - Designet til at virke med fremmede komponenter
    - Sikkerhedsmodeller, politikker og mekanismer der understøtter dette
    - *"Autonomic computing" principper?*
- Privathed
  - Data skal kun distribueres når det er nødvendigt
    - I publish-/subscribe systemer skal data kun publiceres hvis der er abonnenter
  - Data skal behandles tæt på hvor de skal bruges
    - Ikke på en central server hos en ekstern tjeneste leverandør
  - Data skal slettes når de ikke længere skal bruges