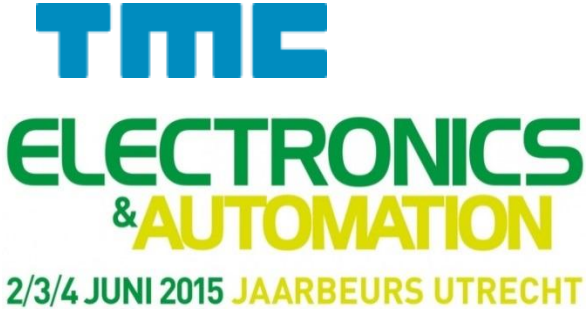
Internet of Things
Veiligheid en beveiliging



Over Technolution en mij

“Wij creëren technische systemen en producten en maken deze tot een aanwinst voor uw organisatie”

- Willem de Boer – security specialist

Technolution

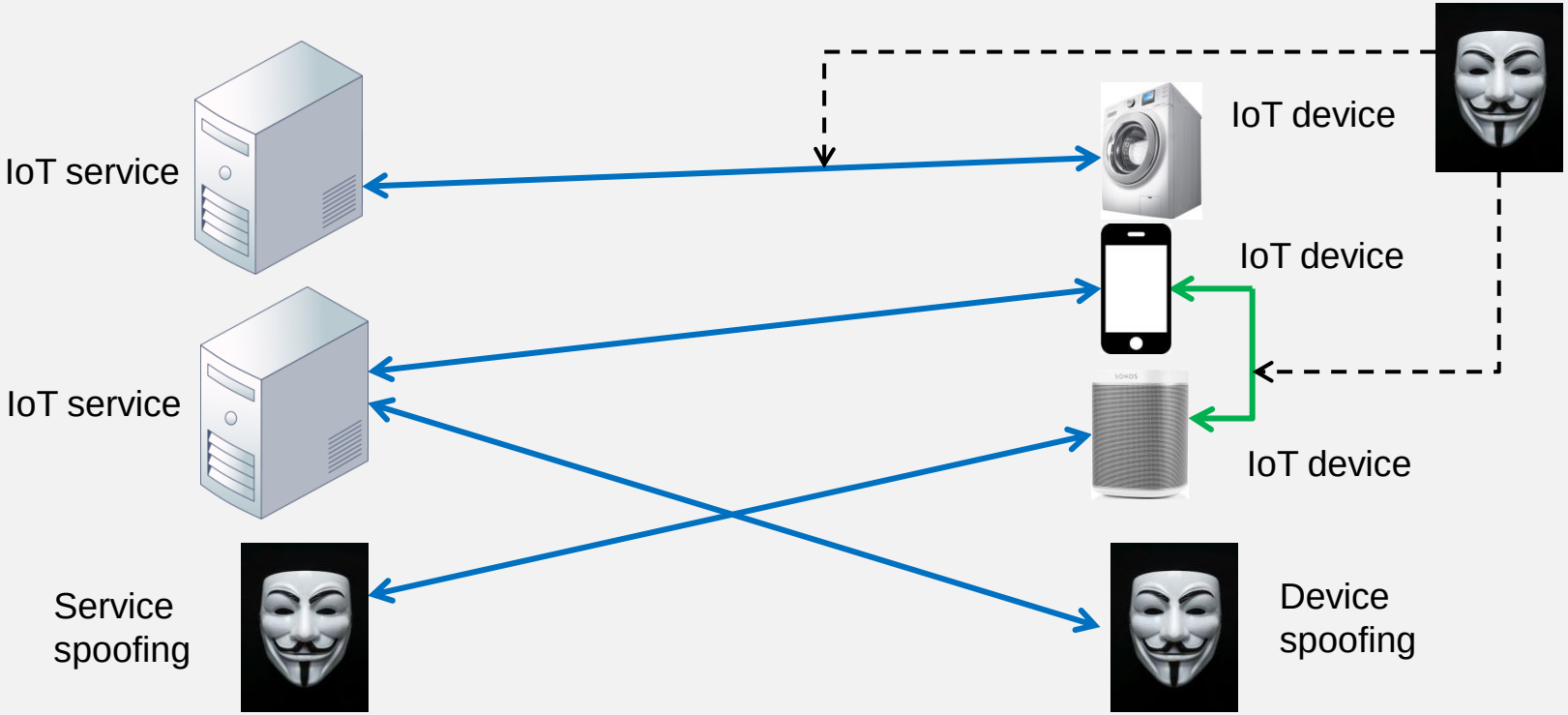
Index

- IoT security en key management
- Voorbeelden van huidige praktijk
- Lessons learned
- Wat dan wel?

Internet of Things

- Veel device worden connected
  - Met elkaar
  - Met services op internet
- Veel soorten IoT devices
  - High end (b.v. telefoons, laptops, etc.)
  - Low end (b.v. temperatuur sensoren, hartslagmeters, etc.)

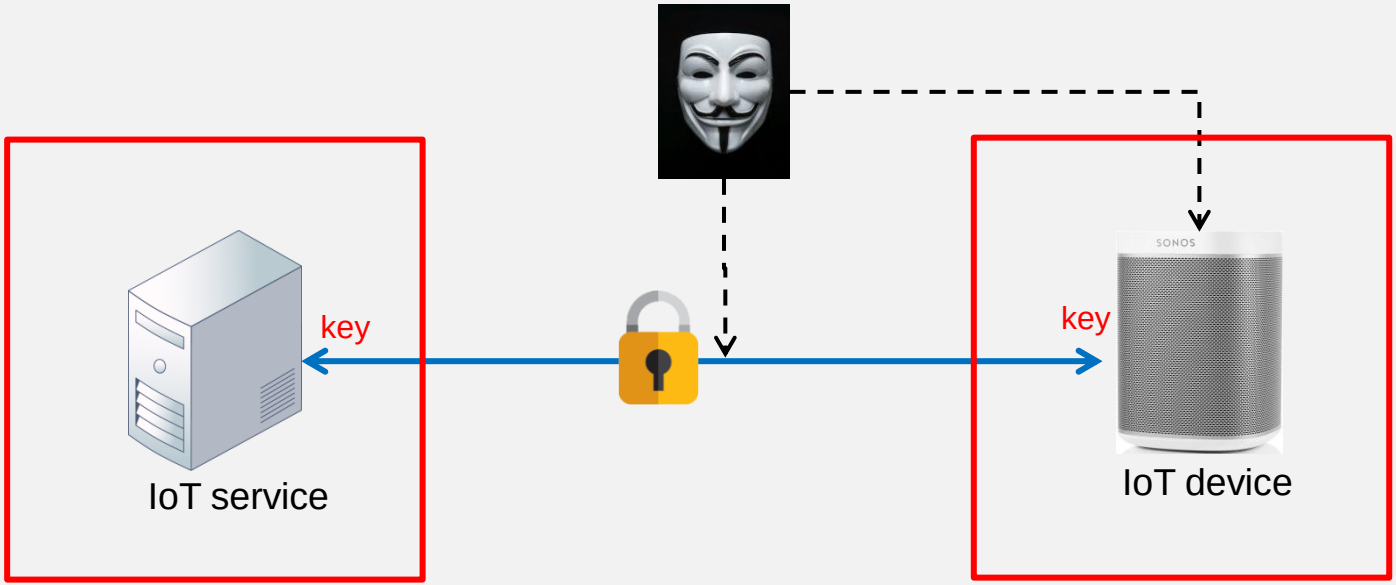
IoT security



Cryptografie

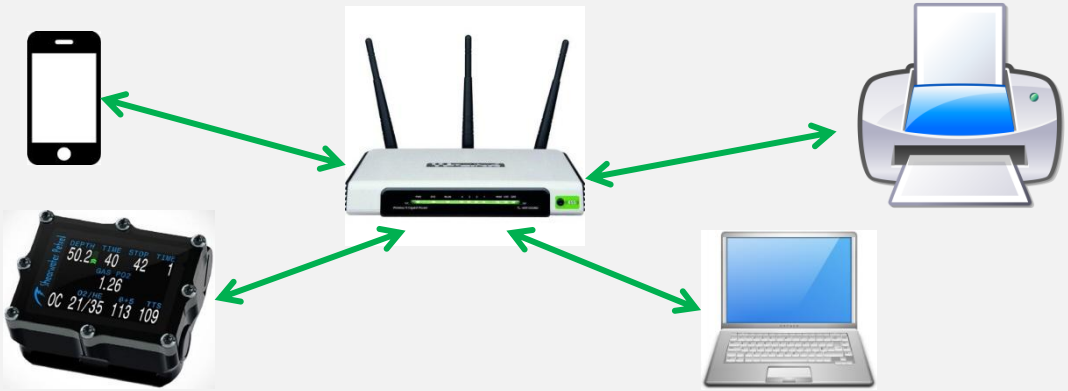
- Entity authenticatie
- Integriteit / authenticiteit van data
- Encryptie van data

- Cryptografie verschuift probleem naar de keys
- Dus → Key management is belangrijk


key
IoT service
key
IoT device


Voorbeelden

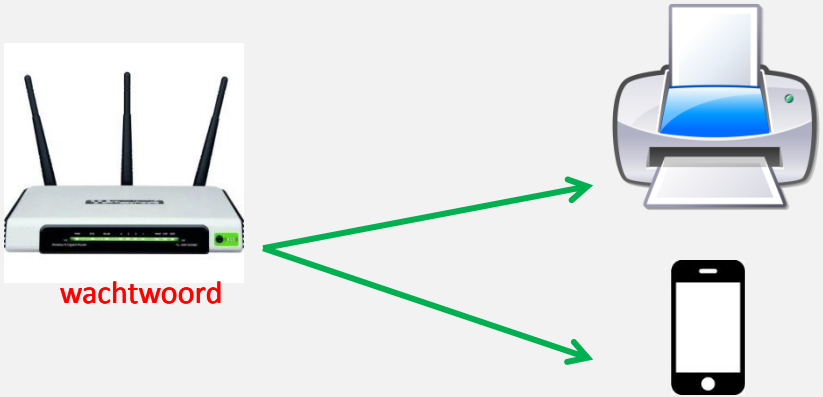
WIFI



- Eén key voor alle devices: het WiFi wachtwoord
  - Wat als deze lekt?
- Gebruiker verantwoordelijk voor het wachtwoord
  - Default wachtwoord op gateway
- Invullen wachtwoord op device is vaak lastig
  - Onveilige mechanismen als WiFi Protected Setup

WiFi Protected Setup (WPS)

- WiFi gateway heeft een drukkop.
- Druk op knop: gateway tijdelijk in de “uitdeel mode”.



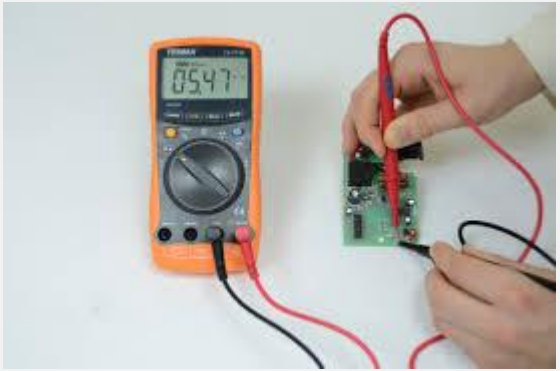
OV-chipkaart

- Gebruikt fabrikant specifieke crypto
- Tijd gestuurde Random Number Generator (RNG)
- Fouten in protocol implementatie

- Gevolgen: OV-chipkaart lekt keys

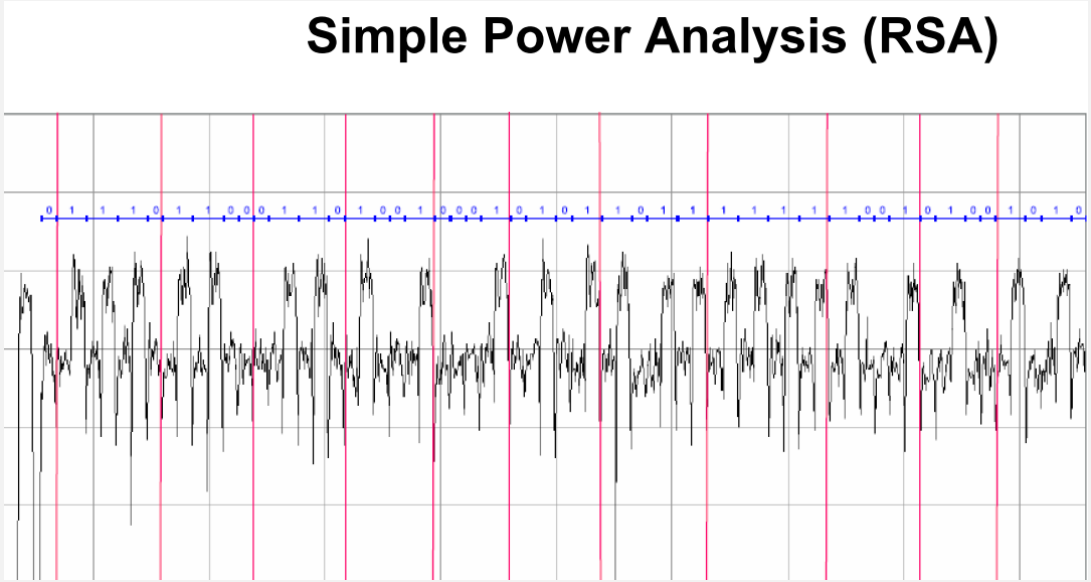
Key opslag

- Keys staan vaak in normaal geheugen
- Crypto niet bestand tegen “side channel attacks”
- Keys te achterhalen als hacker fysiek toegang heeft



Side channel attacks

- Timing
- Stroomverbruik
- EM straling
- Geluid
- Licht



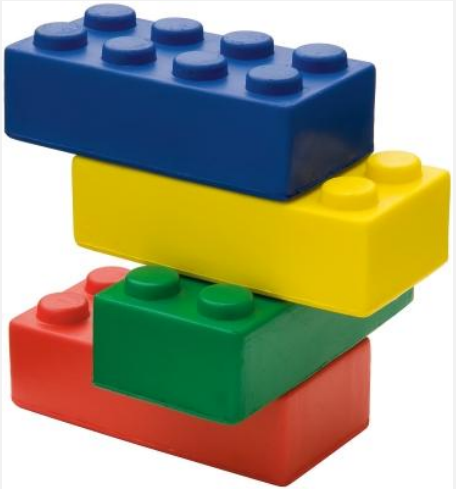
Lessons learned

- Gebruik bewezen en open crypto algoritmen
- Meer aandacht voor fysieke aanvallen op devices
- Random nummer generator is lastig
- Gebruik één key tussen max. twee partijen
- GEEN shortcuts (b.v. WPS)
- Gebruiker NIET “opzadelen” met key management


Wat dan wel?

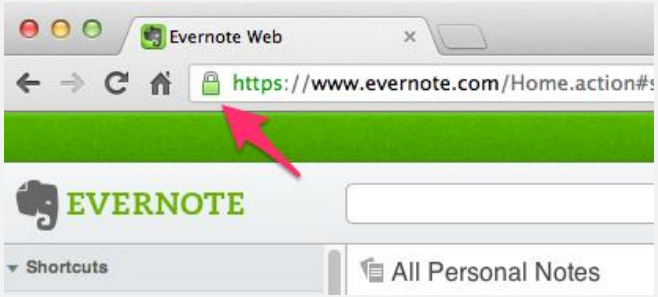
Crypto bouwstenen voor IoT devices

- Tamper proof key opslag
- Cryptografische algoritmen
- Random nummer generatoren
- Protocol implementaties



PKI voor IoT devices?

- Public Key Infrastructure (PKI)
  - Bekend van browser (HTTPS)
  - Werkt met certificaten
  - Trusted parties
- Certificaten
  - €10,- tot €50,- per device
  - Beperkt geldig (1 à 2 jaar)
  - Datum/tijd nodig op device voor validatie
  - Kostbaar……

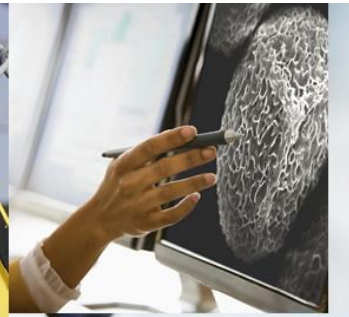


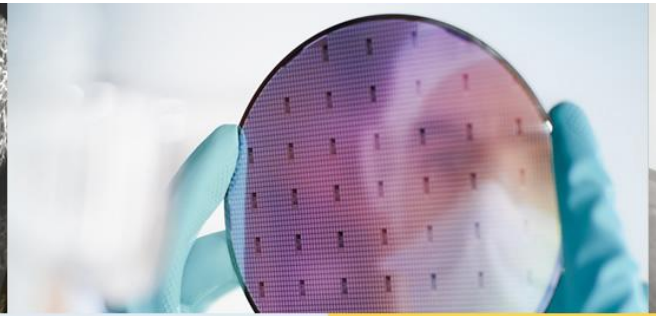
Wat is nodig en zijn onze speerpunten

- Ontzorgen gebruikers en leveranciers van IoT devices
- Trusted parties voor key management
- Nieuwe businessmodellen
- Onafhankelijke toetsing en keurmerken
- Open standaarden

Technolution

/ the right development





Willem de Boer
Security specialist
willem.de.boer@technolution.nl
Technolution – Stand 8A050