Year 2 Review
Paris, November 8th and 9th, 2006

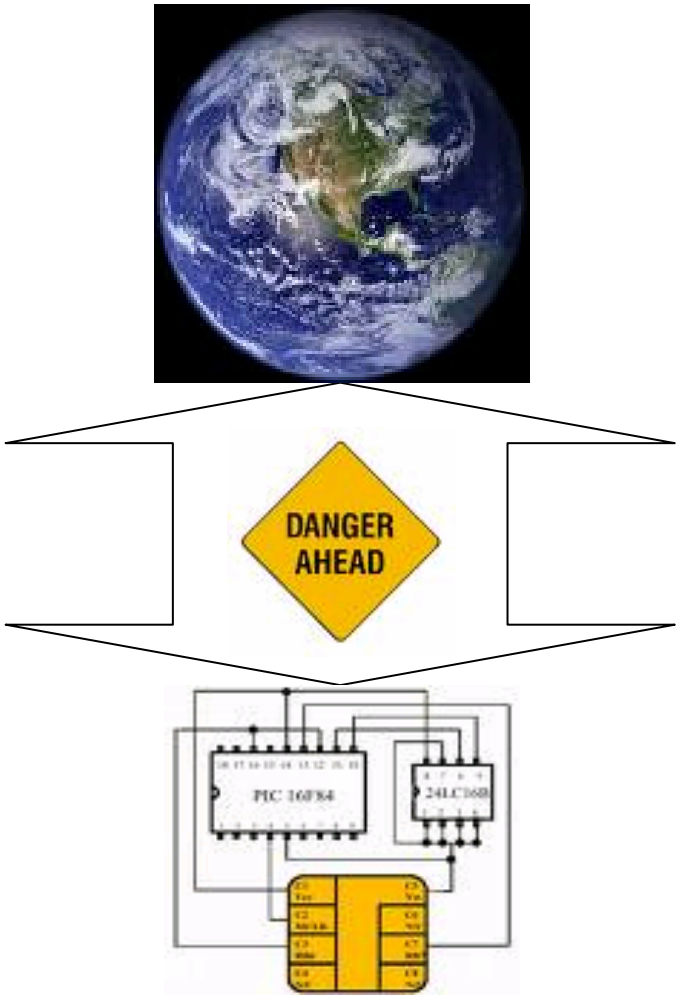
Verification of Security Protocols

Cluster Testing and Verification

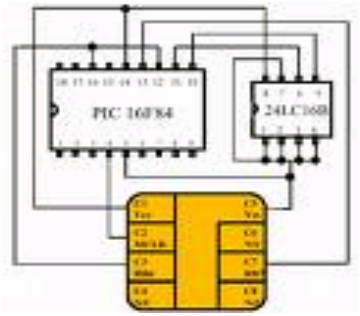
Sandro Etalle

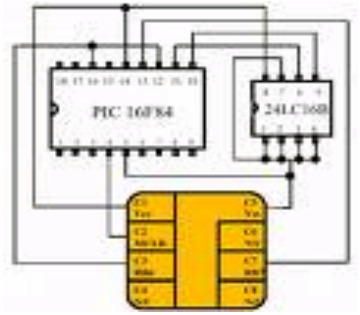
University of Twente

Goal of the Activity



Present and Future





Properties:
Authentication, Secrecy

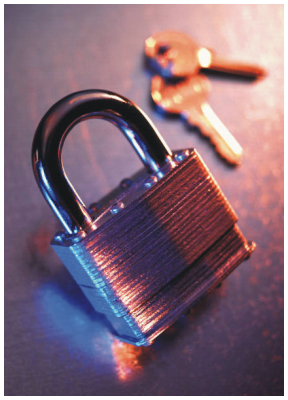
Adversary:
Formal

Trust & Services

Computational adversary

Computational

One Higlight
complete decision procedure for protocols using XOR



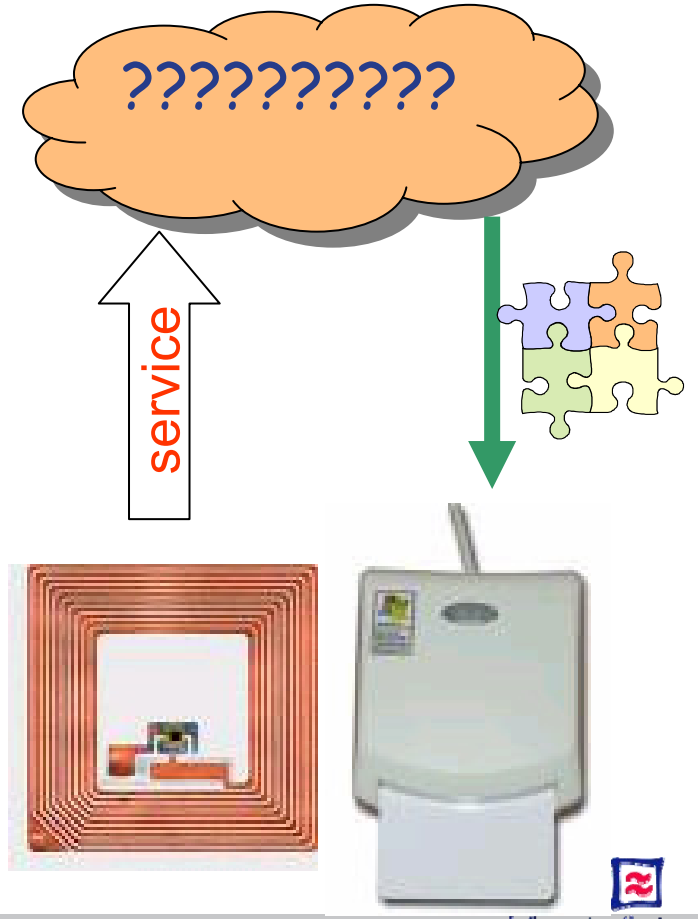
- Encrypting a message makes it “secret”
- Encrypting it *twice* makes it ….
- … more secure (with a lot of encryption methods)
- … completely public if one uses XOR

Computational adversary

Dolev-Yao adversary

Second Highlight: checking customizable sec. policies

- Classical: secrecy, authentication
- Less classical: non-repudiation (2005)
- Customizable security policies (2006)
  - $p(d_1,\ldots,d_n)$, learn(m)
  - $Y\varphi$, $\varphi_1 S \varphi_2$, $O\varphi$ (= true S φ) , $H\varphi$ (= $\neg O \neg \varphi$)
  - $\neg\varphi$, $\varphi_1 \wedge \varphi_2$, $\varphi_1 \vee \varphi_2$, $\exists v.\varphi$, $\forall v.\varphi$



Challenging