



## Can we avoid Protocol Security meltdown?

Brian Monahan  
Trusted Systems Lab  
HP Labs, Bristol, UK

Tel: +44 (0)117 312-8935  
Email: brian\_monahan@hp.com

Presented at  
**STORK : Towards a Roadmap for Future Research**  
26-27 November 2002

## What is the Internet made from? ☺

- Security not a priority originally, but ...
- When the Internet became global and commercial ...
  - Identity and process integrity becomes a serious distributed issue.
- This means that:
  - Security fixes applied by patch, building upon existing protocols.
  - Known protocols used in ways unintended by original designers.
  - More crypto, communication & distribution ⇒ protocol evolution.



## Protocol Security Engineering

- Protocol security provided by:
  - Subtle compositions of foundational cryptographic primitives.
- System Block level validation & verification
  - Simplified “black box” units characterised by external properties.
  - Security properties are “systemic” and not merely “functional”.
- Need to strengthen:
  - Description and identification of:
    - Security goals for protocols.
    - Systems assumptions that protocols rely on to achieve their goals.
    - How and why a protocol works securely (i.e. explanation and proof).
  - Tool support for protocol security design & engineering



Can we avoid Protocol Security meltdown?

Slide 3/5

STORK: Towards a Roadmap for Future Research 26-27 November 2002

## How to avoid Protocol Security meltdown?

1. **Recognise** there is a problem to be tackled and solved.
  - Innovation & evolution in protocols is *inevitable* because of:
    - PUSH**: Improved cryptographic primitives making interesting things possible
    - PULL**: More applications needing to do more things, more securely.
2. **Encourage** protocol engineering to become more *mainstream*.
  - Education – to broaden *understanding* of protocols issues by developers and engineers.  
Recent security protocols web-site: <http://www.lsv.ens-cachan.fr/~jacquema/splib/>
3. **Encourage** development of improved ways for *describing* protocols with their security goals and assumptions (e.g. spi-calculus, Isabelle, CAPSL [from **SRI**]).
4. **Encourage** development of *effective* applied logic-based tools for protocol security analysis and design, usable by developers and engineers.



Can we avoid Protocol Security meltdown?

Slide 4/5

STORK: Towards a Roadmap for Future Research 26-27 November 2002

## *Protocols at HP Labs*

- Protocol analysis tools : Brian Monahan
  - Automated flaw discovery for simple protocols
  - Proof-of-concept prototype tool
  - New version under development – broader range, more control.
  - Report: <http://www.hpl.hp.com/techreports/2002/HPL-2002-246.html>
  
- CASENET : Wenbo Mao
  - <http://www.casenet-eu.org/>



*Can we avoid Protocol Security meltdown?*

Slide 5/5

*STORK: Towards a Roadmap for Future Research 26-27 November 2002*