HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

A Secure Peer-to-Peer Web Framework

Joakim Koskela, Andrei Gurtov

IETF78, HIPRG, July 27

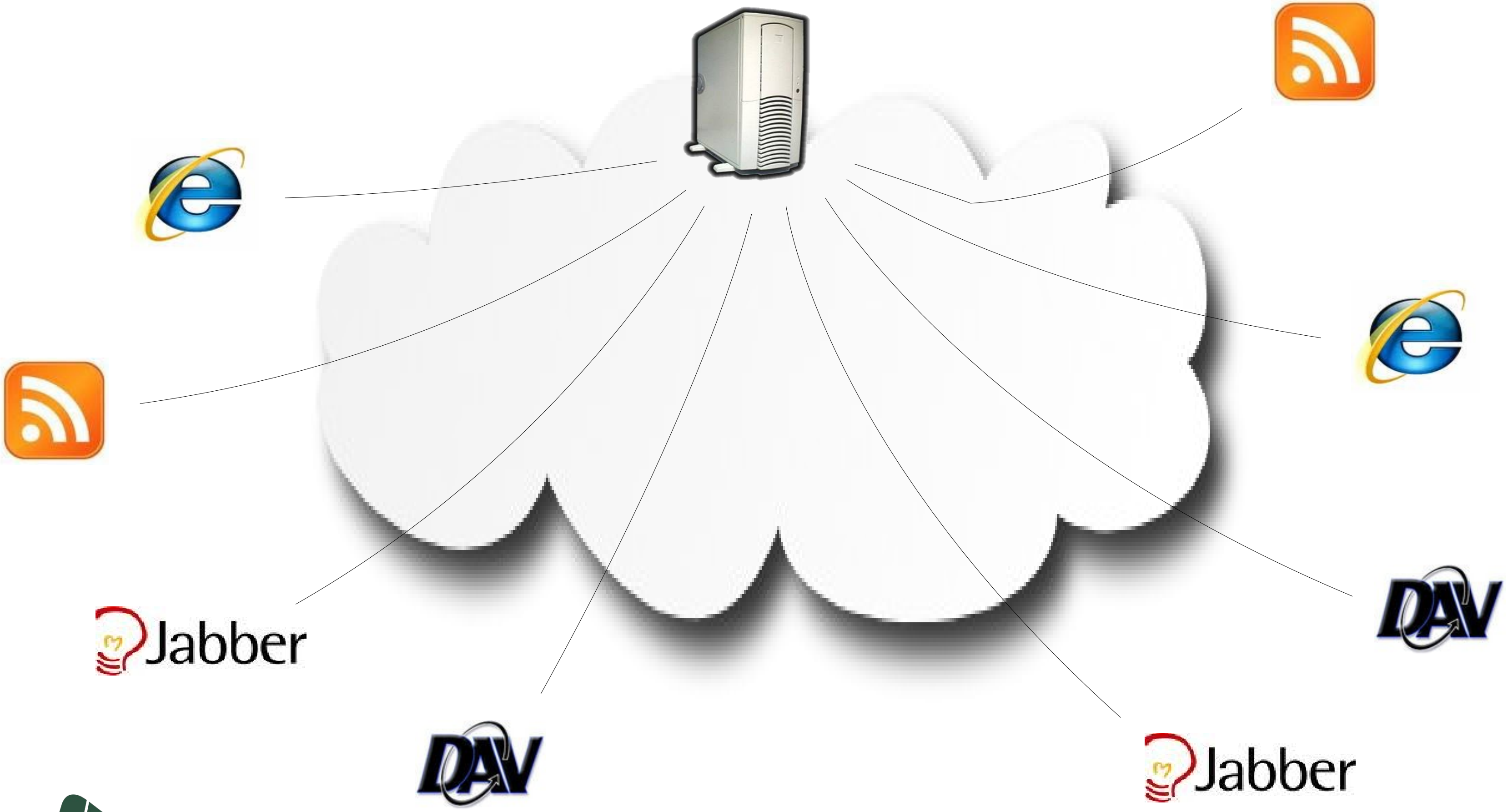
Aalto University

UNIVERSITY OF HELSINKI

HTTP applications

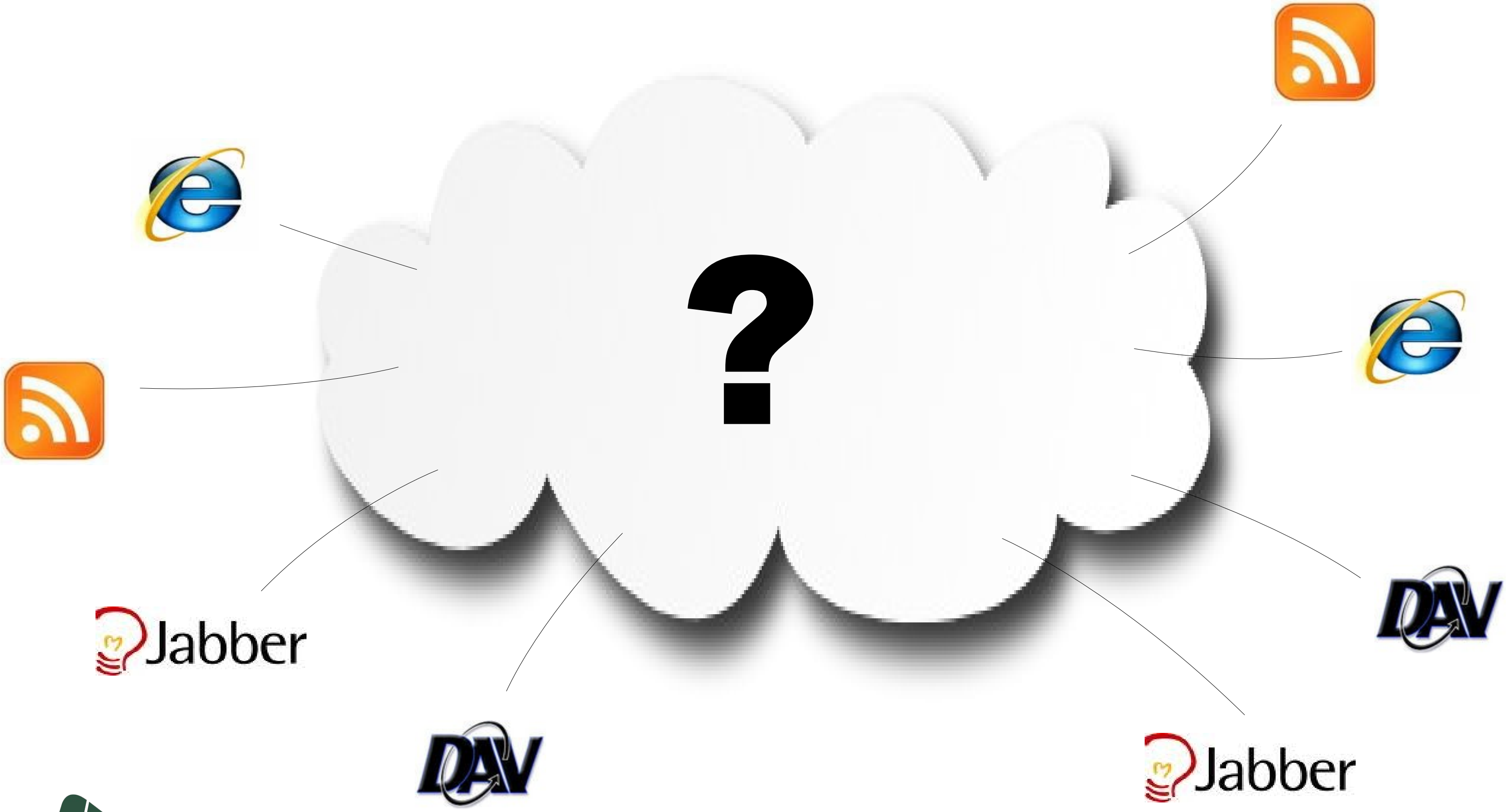
SOAP
DeltaV
e
Jabber
DAV
W3C

Current model



HELSINKI
INSTITUTE FOR
INFORMATION
TECHNOLOGY

Providerless model?



HELSINKI INSTITUTE FOR INFORMATION TECHNOLOGY

Overview

- Introduction
- Design
- Evaluation
- Conclusions

Introduction

- Users produce content
- Privacy issues
- Vendor trustworthyness
- Ad-hoc, mobile devices

Design

- Existing data protocols
- Publicly available resources
- Identities, lookup, connectivity and application interface

Design: Identities

- Strong (public-key) identities
- Name to key mapping
    - Certificates
    - Leap-of-faith

Design: connectivity

- Use existing, deployed, solutions
  - Host Identity Protocol
  - Teredo
- Requires connection parameters
  - HITs, IP addresses, relay information

Design: Lookup

- Signed *registration* packets
- Any key-based storage as backend
- Privacy through obfuscation

Design: application interface

- Client
  - HTTP proxy
  - URL-rewriting

```
http://localhost:9000/alice.at.p2p.hiit.fi/application
```

- Serving applications *register* ports

Evaluation

- Linux prototype
  - Desktops & N810 internet tablet
- HIP added seconds to initial connection
- RTT unaffected
- Throughput -8% of plain TCP

Conclusions

- The resources needed already exist
- Identity management paramount
- Application packaging needed

Thank you

Contact me at joakim.koskela@hiit.fi

Project home: http://www.hiit.fi/trustinet
Code repository: http://code.google.com/p/p2pship