Stacking Identity

HIIT Retreat
June 1, 2004

Pekka Nikander, Ph.D.

Outline

- A problem to solve
- Three layers or steps
  - Identify hosts
  - Manage trust and authority
  - Create trust and reputation
- Our position

A problem to solve

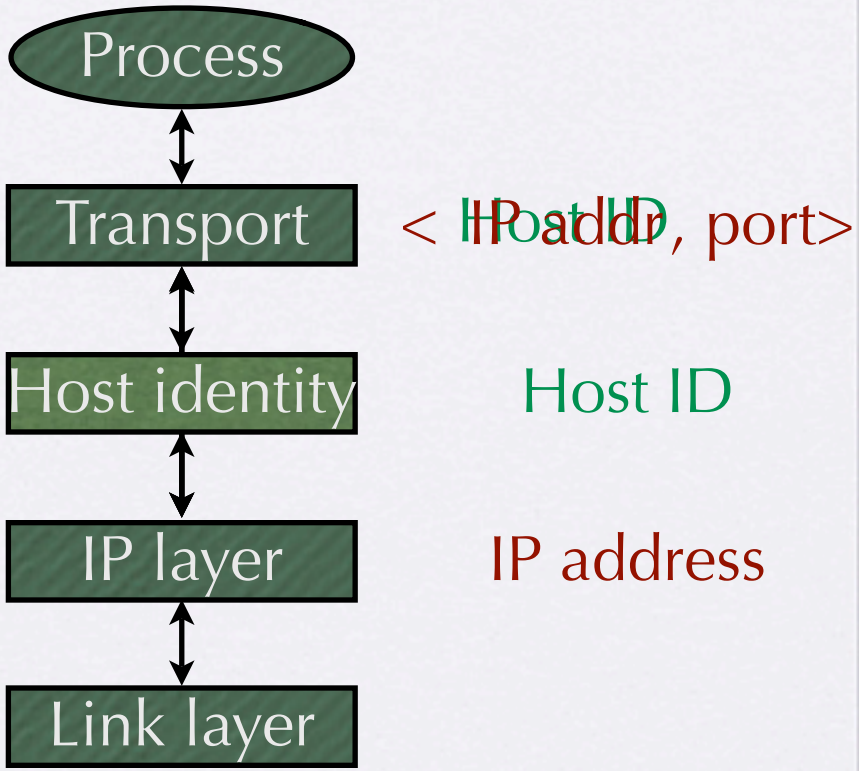
- How to make systems simultaneously secure and usable?
- Basic approach: *Minimise need for user intervention*
- Conversely: *Make computers more security "conscious"*
  - Establish strong identity
  - Assign authority to the strongly identified entities
  - Enable trust and reputation based on experiences

Step 1: Identity

- Goal: *Cryptographically strong identity to devices*
- Means: Host Identity Protocol (HIP)
  - Identify each communicating device with a cryptographic public key
  - Insert the key into the TCP/IP stack

The HIP Idea

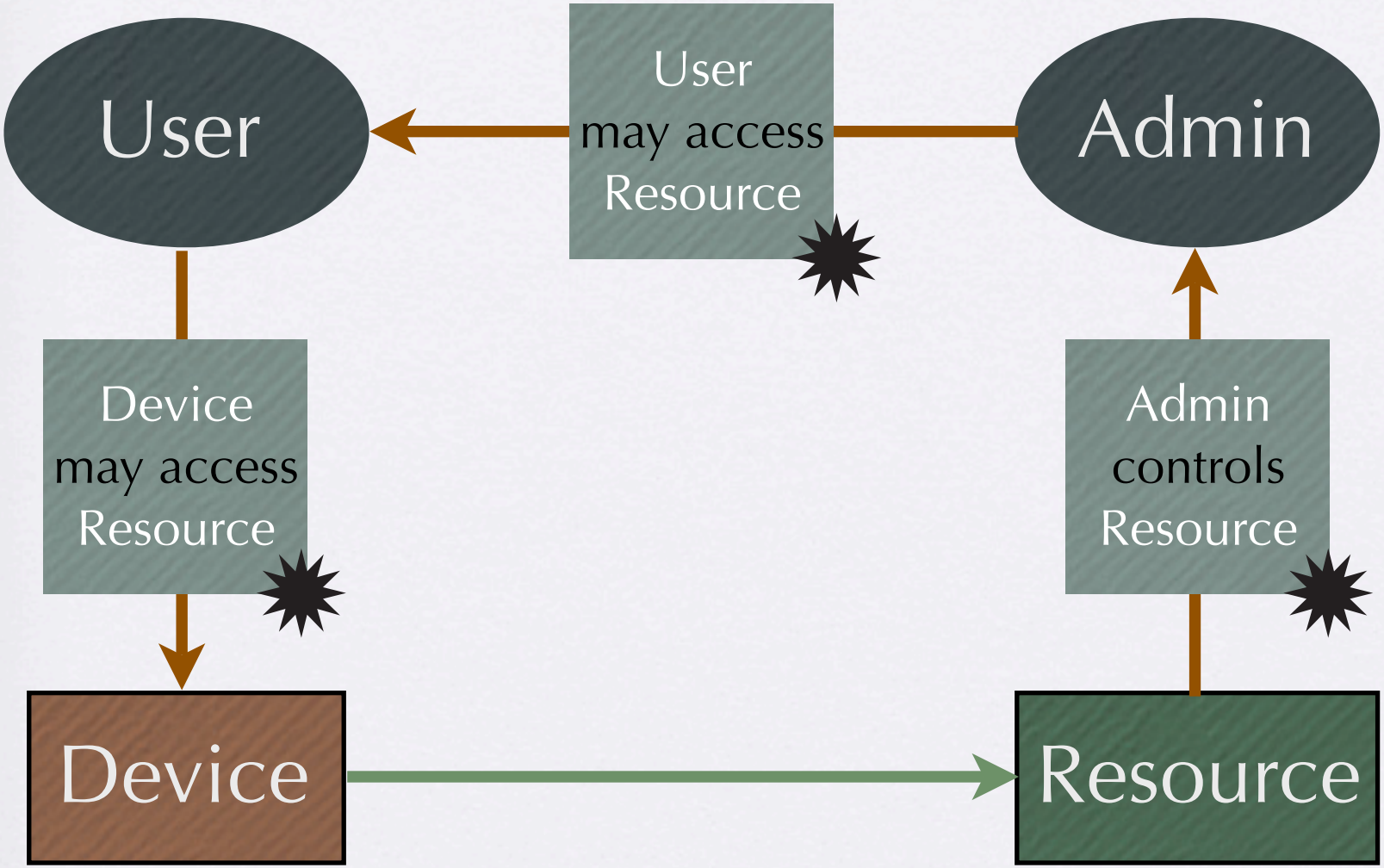
- A new Name Space of Host Identifiers (HI)
  - Presented as 128-bit long hash values, Host ID Tags (HIT)
- Sockets bound to HIs, not to IP addresses
- HIs translated to IP addresses in the kernel



Step 2: Authorisation

- Goal: *Decentralised means for managing authorisation*
- Means: SPKI and KeyNote2 certificates
  - Express delegation with signed statements
  - Eventually integrate to the operating system

The SPoKI Idea



Step 3: Trust

- Goal: *Creation of trustworthy behaviour*
- Means: Micro economic mechanism design
  - Design the rules for the game
  - Make unsocial behaviour uneconomical

The Missing Idea

- Reciprocal resource sharing?
- Decentralised reputation management?
- Incentive to stick to one identity?
- Tokens and other forms of fiat money?

Our position

- Establish identity to all devices by making HIP a component of the future the Internet architecture
- Apply research methods and ideas from micro economics to decentralised systems security
- Eventually bridge the gap between identities and reputation formation with managed authorisation

Your input, please!