

Pseudonymity is the best that you can do

David Evans

Computer Laboratory
University of Cambridge
david.evans@cl.cam.ac.uk

Devices have persistent or transient identities

- Bluetooth devices: MAC address
- RFID tag: serial number, etc.
- mobile phone: IMEI
- sensor node: ad-hoc network address

Device identities are essential

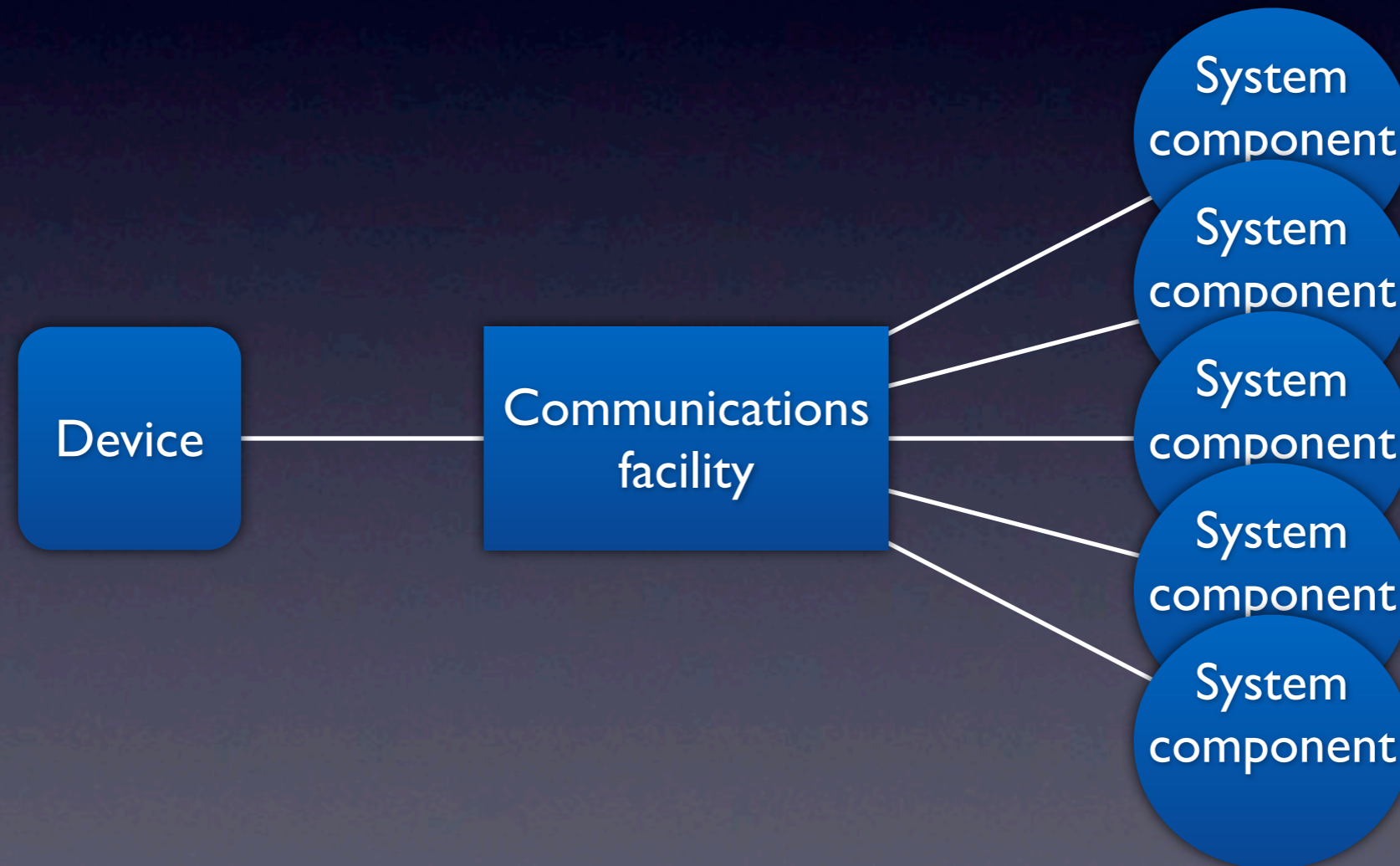
- packet addresses
- differentiate recipients and senders
- handles for state

Anonymity = unlinkability

- no multi-packet communications protocols
- no replies without broadcast
- stateless protocols

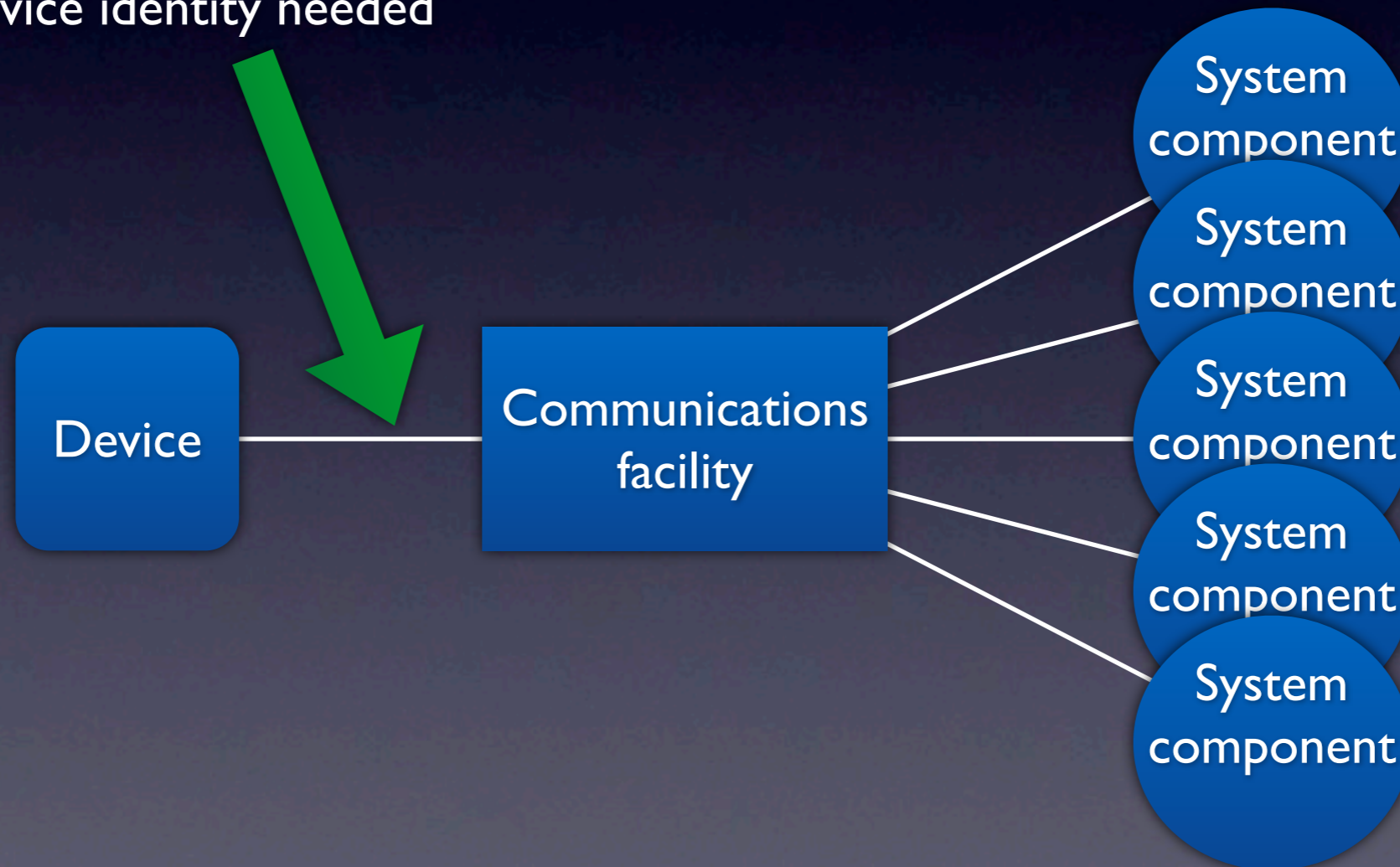
device identities are
involuntarily disclosive

Which needs to know what?



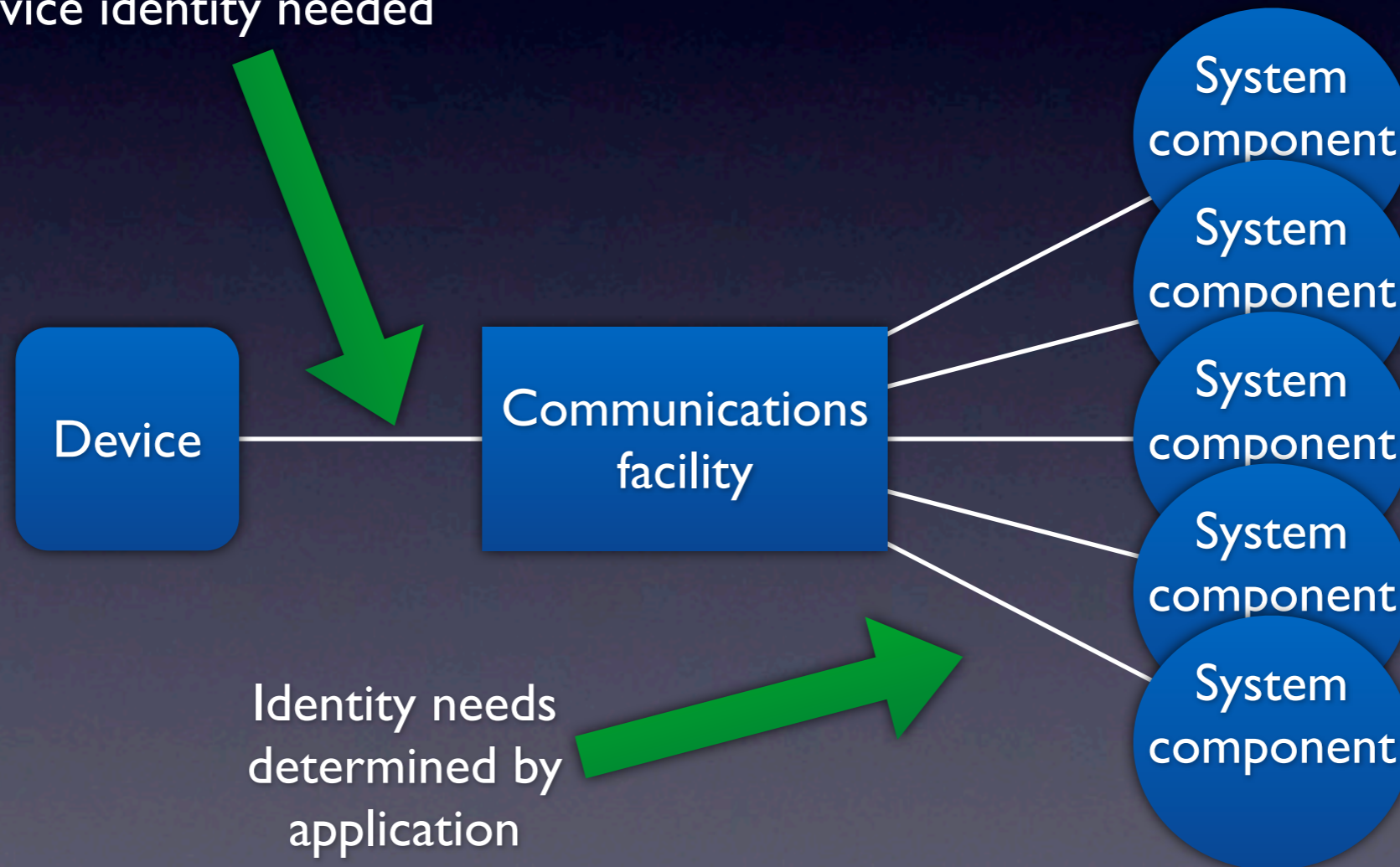
Which needs to know what?

Device identity needed



Which needs to know what?

Device identity needed



Identity needs determined by application

Pseudonymity is inevitable

- lots of system components need
 - complex protocols
 - application state

but have no need to communicate with devices

Sample application requirements

- attribute multiple interactions to the same device
 - session length—a few hours? a week?
- identify pairwise interactions
- link actions to an external entity (a person, a credit card, ...)

Achieving privacy

- responsibility should rest with the application more than with the infrastructure
- devices can label information that is voluntarily disclosive
- application *must* do such labelling!

What labelling accomplishes

- gives privacy context to data
- provides anchors for policy
- labels are hooks for negotiation between administrative domains
- abstracts and hides implementation

Things to think about

- essential application requirements
 - Oyster allows pseudonymous travel
- information sharing needs
- implications of storage, logging, and audit