Access Control to Information in Pervasive Computing Environments

HotOS 2003

Urs Hengartner &
Peter Steenkiste

Carnegie Mellon

Privacy in Pervasive Computing

- Pervasive computing:
  - Many computers for everyone
  - Embedded, networked sensors
- New types of information about people (location, activity, health,…)
- Privacy is a big concern in a ubicomp world.
  - Unlimited coverage
  - Loss of awareness
  - Access control
  - …

Outline

- Unique challenges
- People locator service
- Three design principles
- Design of access control mechanism
- Related work
- Conclusions

Ubicomp Scenario – Location Information

Meeting in Room 8220

Calendar Parser

Room 8220

People Locator

Room 8220

Room 8220

IP address

Laptop Locator

Room 8220

Filter

Pittsburgh

Face Recognizer

Picture

Face Detector

Face Parameters

No Single Point of Access

Meeting in Room 8220

Calendar Parser

Room 8220

People Locator

Room 8220

Room 8220

IP address

Laptop Locator

Room 8220

Filter

Face Recognizer

Pittsburgh

Picture

Face Detector

Face Parameters

Change in Nature/Granularity

Meeting in Room 8220

Calendar Parser

Room 8220

People Locator

Room 8220

Room 8220

IP address

Laptop Locator

Room 8220

Filter

Face Recognizer

Pittsburgh

Picture

Face Detector

Face Parameters

Multiple Administrative Entities

Meeting in Room 8220

Calendar Parser

Room 8220

People Locator

Room 8220

Room 8220

IP address

Laptop Locator

Room 8220

Filter

Face Recognizer

Pittsburgh

Picture

Face Detector

Face Parameters

Challenges for Access Control

	"Pervasive" Information (Location, activity,..)	"Conventional" Information (Files, database objects,..)
Points of Access	Multiple	Single
Type/Granularity	Variable	Constant
Administrative Entity	Multiple	Single

Flexibility of Access Rights

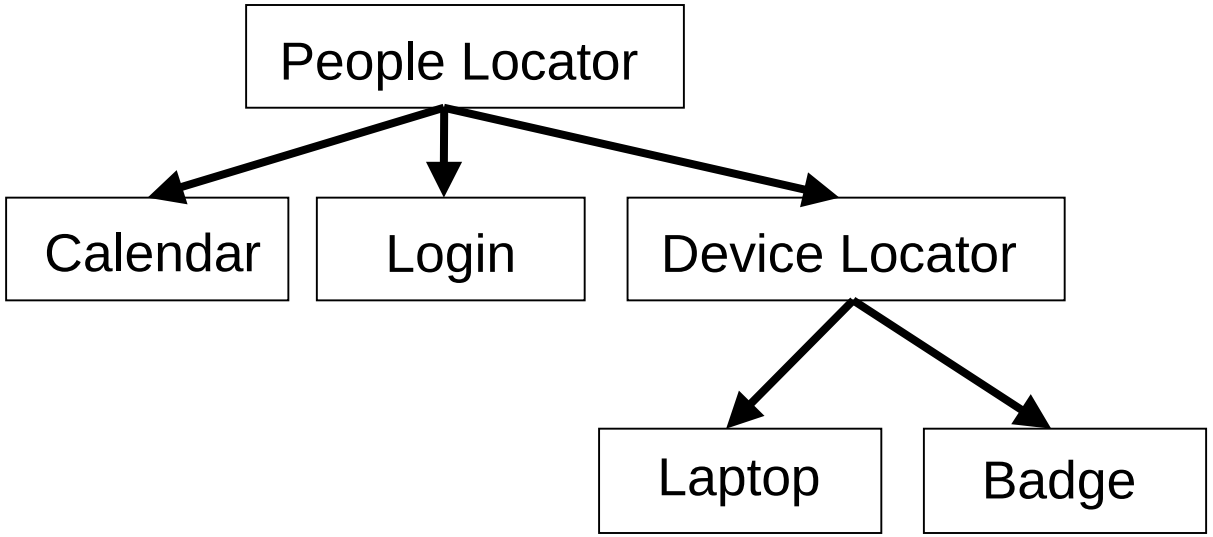
- Support of constraints based on individual's context
  - Current time, activity, or location
- Entities granting access rights
  - Central authority vs. individuals
- Delegation of decision about access rights
  - Have other entity grant access rights.

Outline

- Unique challenges
- People locator service
- Three design principles
- Design of access control mechanism
- Related work
- Conclusions

People Locator Service

- Addressed challenges in context of people locator service.
- Built and deployed at Carnegie Mellon.
- Multiple sources



People Locator Service

- Digital certificates for defining location policies and specifying trusted nodes.
- Experience gained contributes to three design principles.

Outline

- Unique challenges
- People locator service
- Three design principles
- Design of access control mechanism
- Related work
- Conclusions

Extract Information Early

- Strictly limit access to raw information.
  - E.g., camera picture
- Grant access to raw information only to entities doing extraction.
  - E.g., camera picture → face recognizer
- Grant more entities access to extracted information.
  - E.g., Alice's location → Alice

Define Policies Controlling Access at Information Level

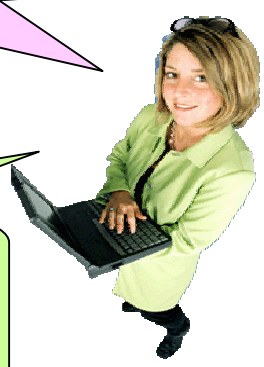
- Many nodes in ubicomp environment.
  - M. Weiser, 1988: "Provide hundreds of wireless computing devices per person per office."
- Requires many policies that control access between pairs of nodes.
- Heavy burden on individuals defining policies.
- Insight:
  - Let individuals make statements about information, not nodes.

Examples

Bob can access my location information as provided by the people locator, which is derived from the location of my laptop as provided by the laptop locator.

The people locator has access to the location of my laptop as provided by the laptop locator.

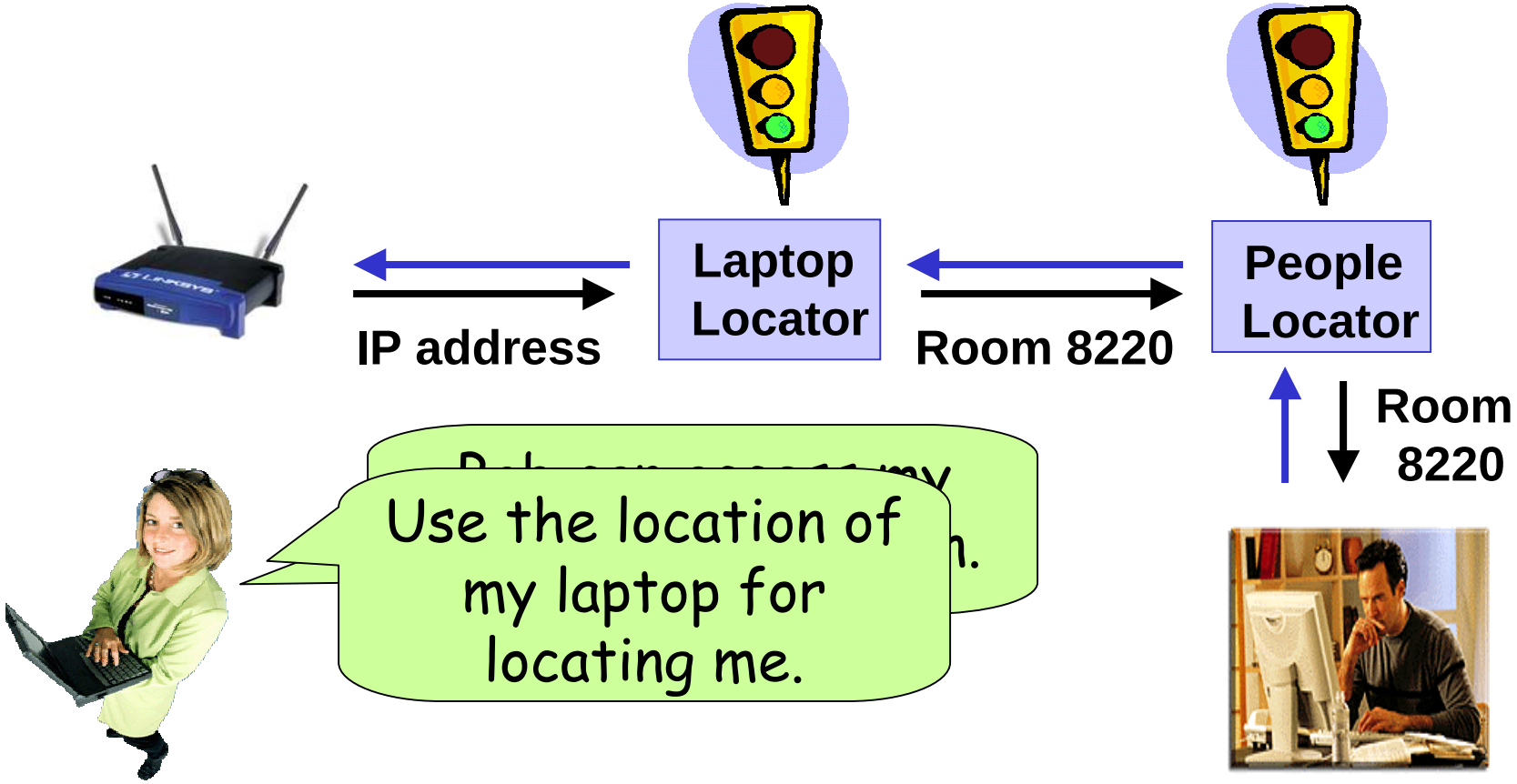
Instead:



Bob can access my location information.

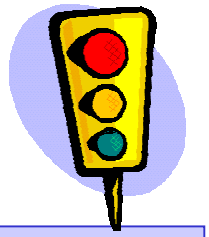
Use the location of my laptop for locating me.

Exploit information relationships for access control



Exploit information relationships for access control

Use relationships to make access control more robust !



Laptop Locator

People Locator

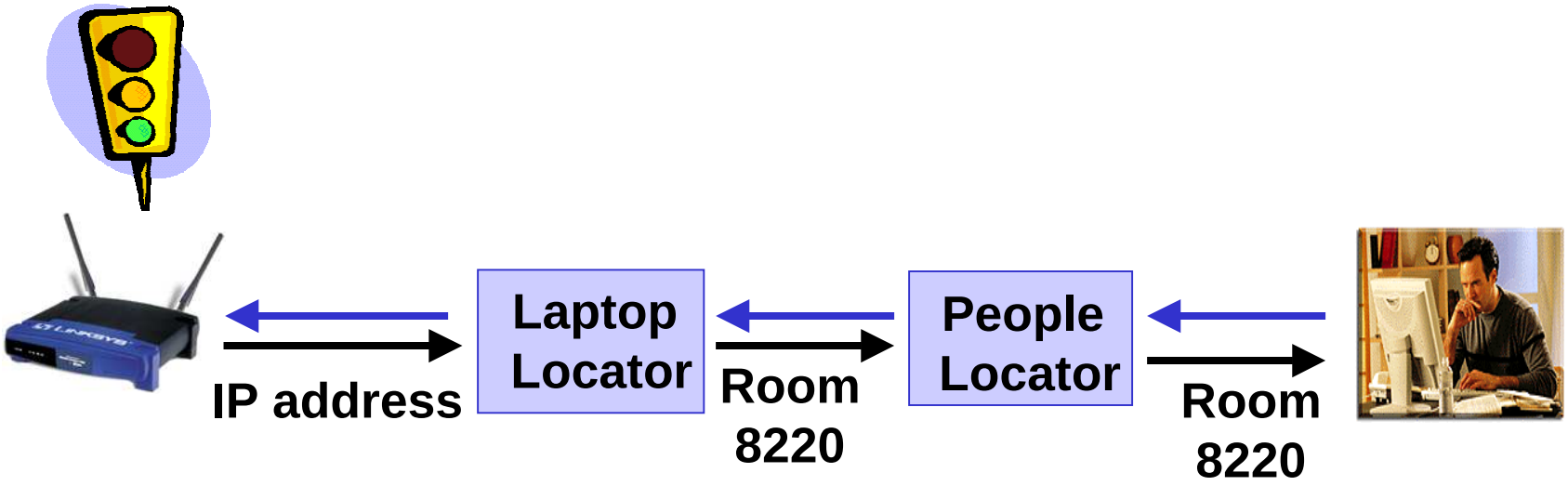
Use the location of my laptop for locating me.

Bob can access my location information.

Outline

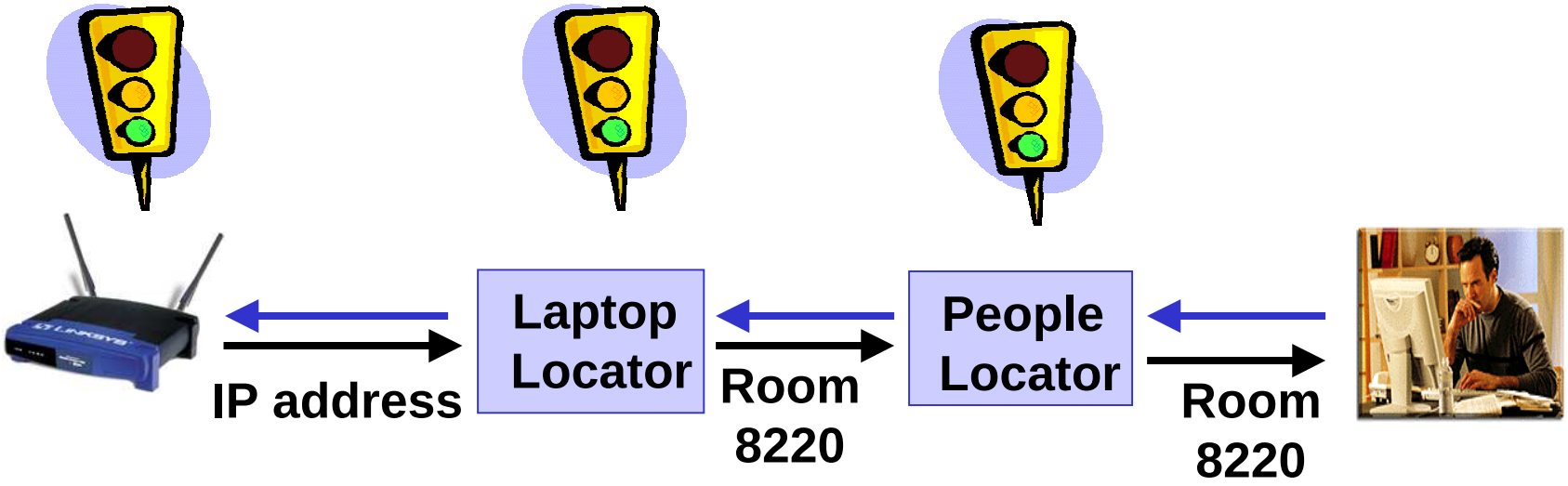
- Unique challenges
- People locator service
- Three design principles
- Design of access control mechanism
- Related work
- Conclusions

End-to-end Access Control



+ Single point for access control
- Heavy load on node running access control
- What about multiple source nodes?
- Vulnerable to DoS attacks

Step-by-Step Access Control



+ Access control load distributed
+ Less prone to DoS attacks
- Multiple points for access control
- What about "dumb" nodes?

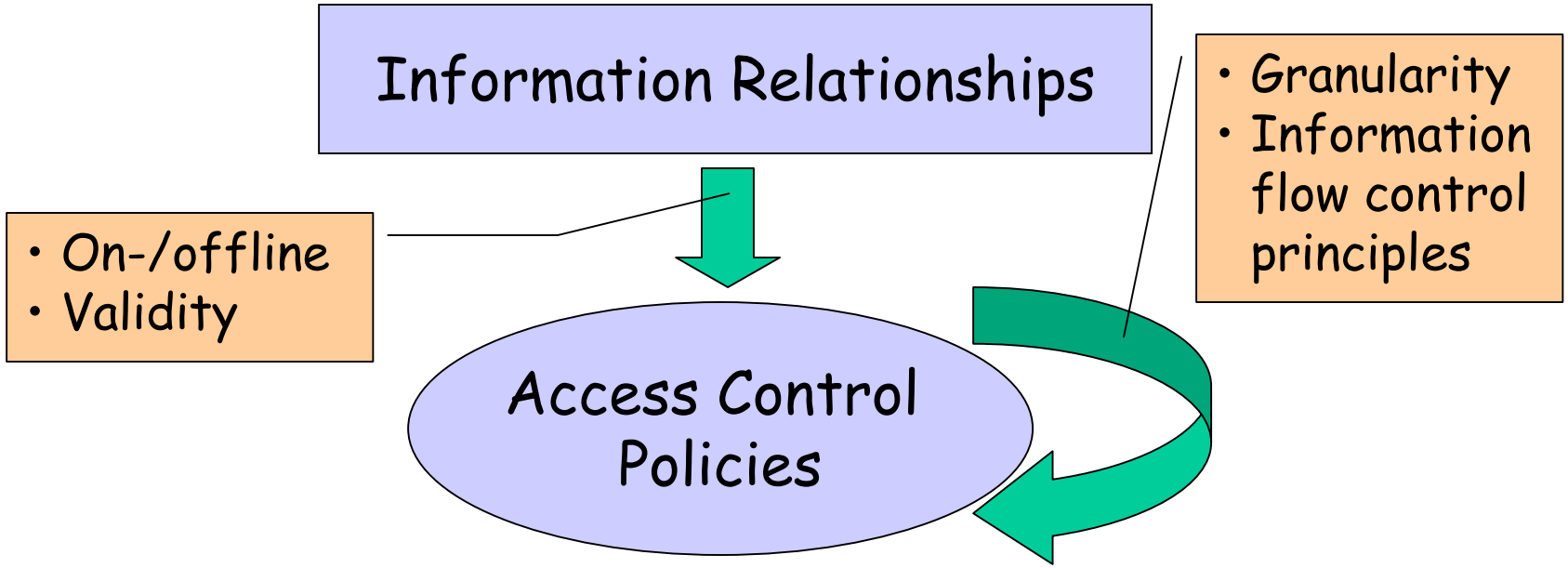
Our Approach

- Step-by-step
  - Delegation for dumb nodes
- Access control mechanism exploits:
  - Policy description language
    - Subject
    - Constraints
    - Type and granularity of information
  - Information description language
    - Type and granularity of information
    - Relationships between information

Access Control Mechanism

Each node:

- Checks existence of access control policy.
- Tries to derive policy if necessary.



Related Work

- Authorizing intermediate nodes
  - [Howell and Kotz 2000],[Neuman 1993]
  - Have intermediate node become part of trusted environment.
  - Dangerous in case of break-in.
- Access control to services in ubicomp
  - [Kagal et al. 2001], [Al-Muhtadi et al. 2003]
  - Concentrate on services (printers, projectors,…), not information.
  - Common issues like flexible policies.

Related Work

- Access control to information in ubicomp
  - [Jiang and Landay 2002],[Minami and Kotz 2002]
  - Assume trusted environment.
  - Automatic derivation of access control policies based on principles from information flow control.
  - What if nature/granularity of information changes?
  - How do individuals specify policies?

Conclusions

- Unique challenges for access control to pervasive information.
- Three design principles:
  - Extract information early.
  - Define policies at information level.
  - Exploit information relationships.
- Access control mechanism for pervasive information.