Smart Phones

Edgardo Vega

Smart Phones

- Device-enabled authorization in the Grey system(2005)
  - Lujo Bauer, Scott Garriss, Jonathan M. McCune, Michael K. Reiter, Jason Rouse, Peter Rutenbar
- Lessons learned from the deployment of a smartphone-based access-control system(2007)
  - Lujo Bauer, Lorrie Faith Cranor, Michael K. Reiter, Kami Vaniea

Introduction

- Grey is a **flexible** platform that provides **ubiquitous** access control to both **physical** and **virtual** resources, via smartphones.
- At the core is a **flexible** and **provably** sound **authorization framework** based on **proof-carrying authorization(PCA)**, extended with a new **distributed proving** technique that offers significant **efficiency** and **usability** advances

Introduction (continued)

- Delegates authority in a convenient fashion.
- Relies on cryptographic key management.
- Also incorporates capture resilience
- Takes advantage of Bluetooth, cellular data (GPRS), and messaging protocols (SMS and MMS)

Graphical Identifiers

Capture-Resilient Cryptography

Proof-Carrying Authorization

COMPONENTS

Graphical Identifiers

- Person
  - Photograph – less failure-prone
- Public Key
  - Two-dimensional barcode of the hash
- Network Address
  - Two-dimensional barcode of the address
  - Circumvent the high-latency of device discovery in Bluetooth

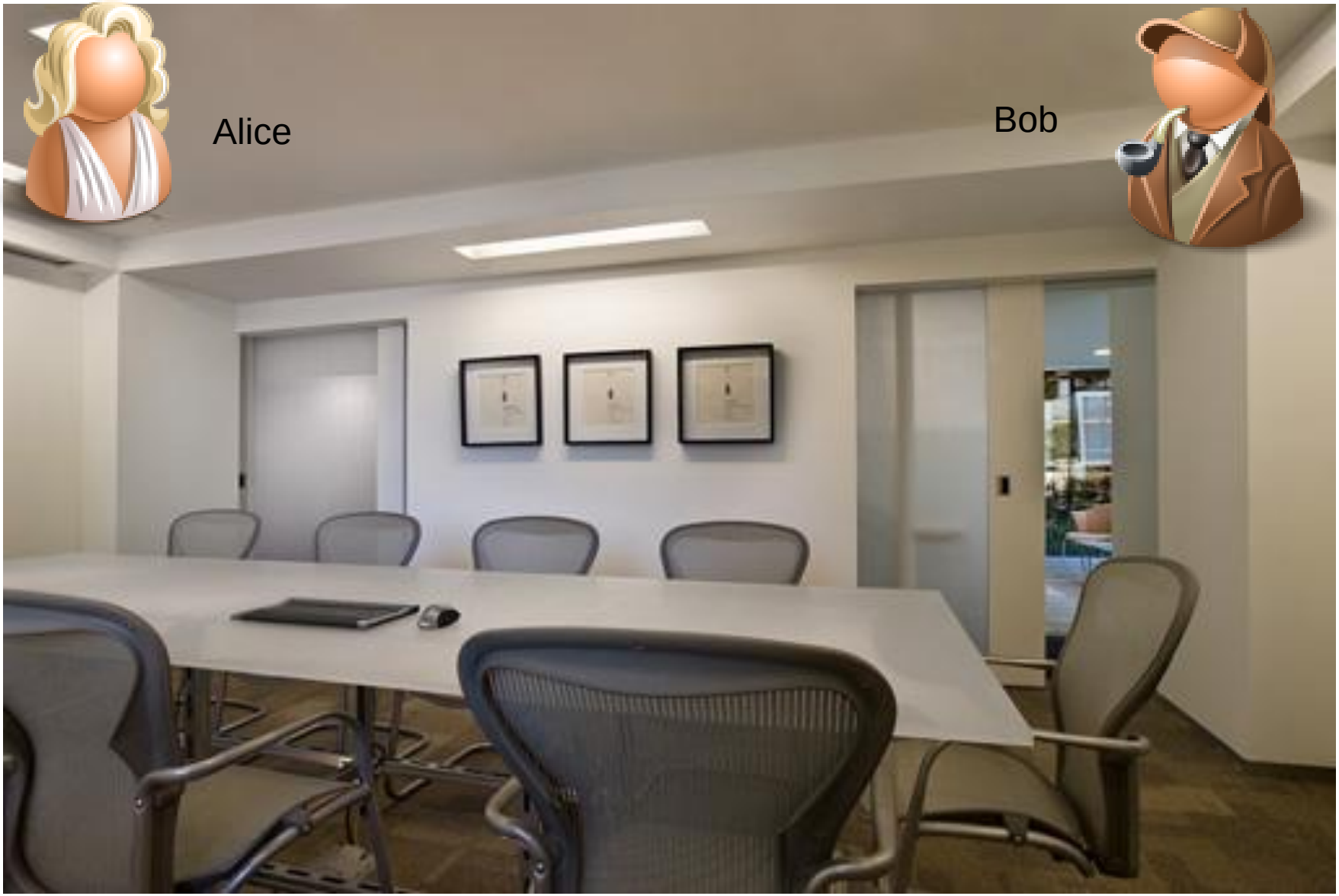
Capture-Resilient Cryptography

- Protects the phones private key by using a **remote capture-protect server**
- User can **disable** the key if the phone has been lost or can temporarily disable to protect from dictionary attacks
- Server is an untrusted space → user's key information is not passed back and forth
- Decentralized system → each user can use their own server (i.e., desktop computer)

Proof-Carrying Authorization

- Utilizes formal logic directly in the implementation of the system.
- Directly manipulates fragments of the logic and represents credentials/proofs of access as constructed in formal logic.
- Contains an automated theorem prover and checker
- Client is responsible to prove that access should be granted

USAGE SCENARIOS


Alice
Bob


4500
4500


4500
4500

Graphical User Interfaces

Prover

Verifier

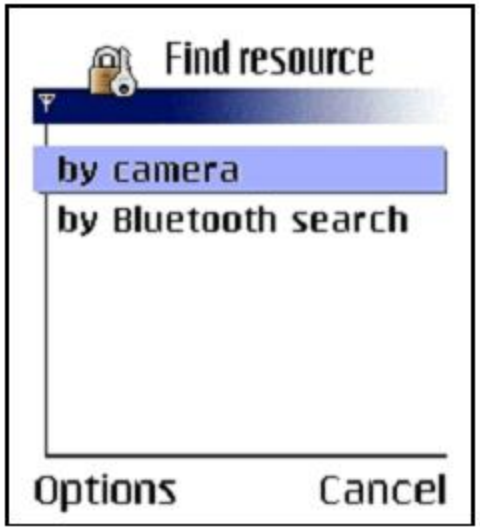
Communication Framework

Performance

SOFTWARE ARCHITECTURE

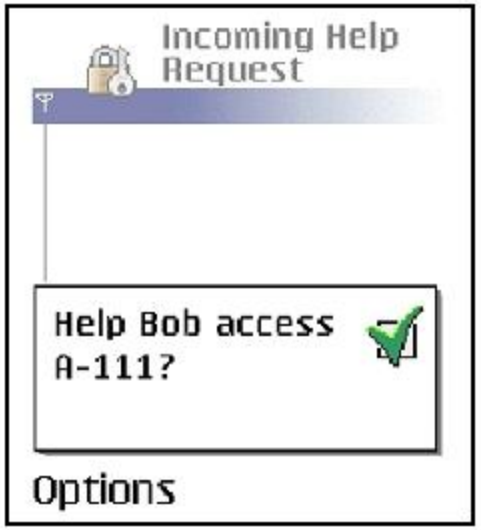
Graphical User Interfaces

- Phone
  - Address Book
  - Access requests to a resource
  - Reactive policy creation
- Computer
  - Groups
  - Roles
  - Policy Creation

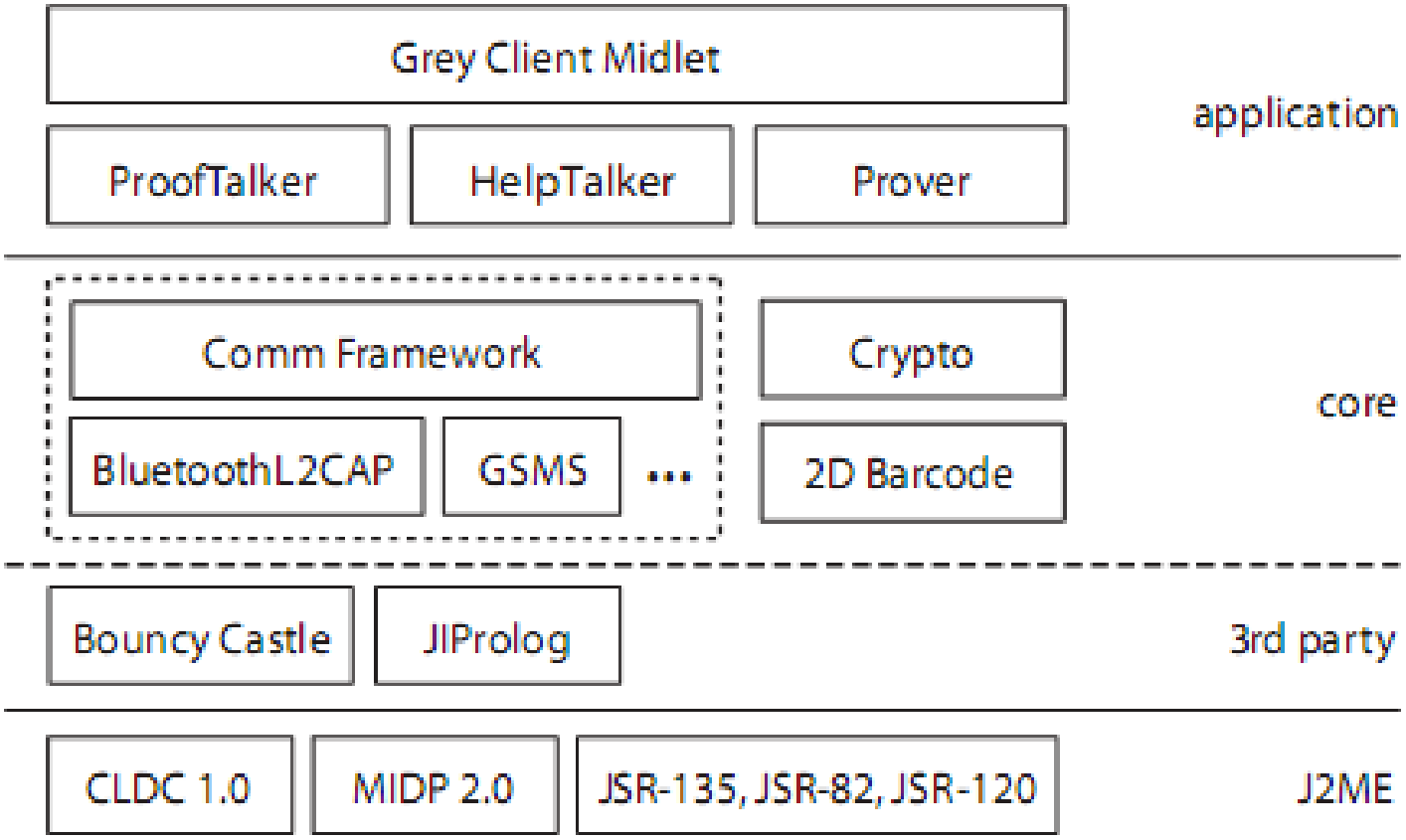


Prover

- Distributed proving
  - Eager – completely unable to make progress
  - Lazy - ask for help as soon as he isolates a theorem that someone else might help with

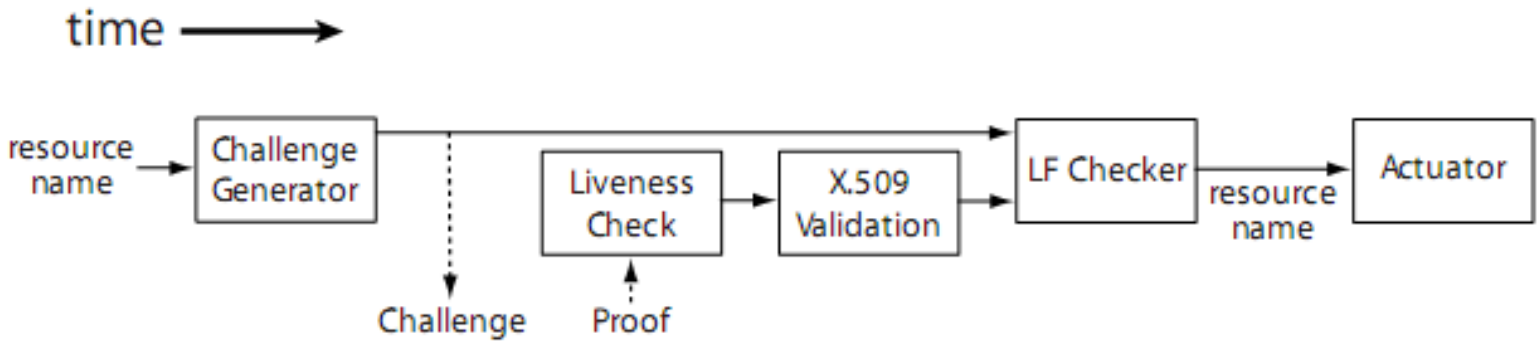


Prover


Grey Client Midlet
ProofTalker
HelpTalker
Prover
application
Comm Framework
BluetoothL2CAP
GSMS
...
Crypto
2D Barcode
core
Bouncy Castle
JIProlog
3rd party
CLDC 1.0
MIDP 2.0
JSR-135, JSR-82, JSR-120
J2ME

Verifier

- Simple, lightweight, and device independent

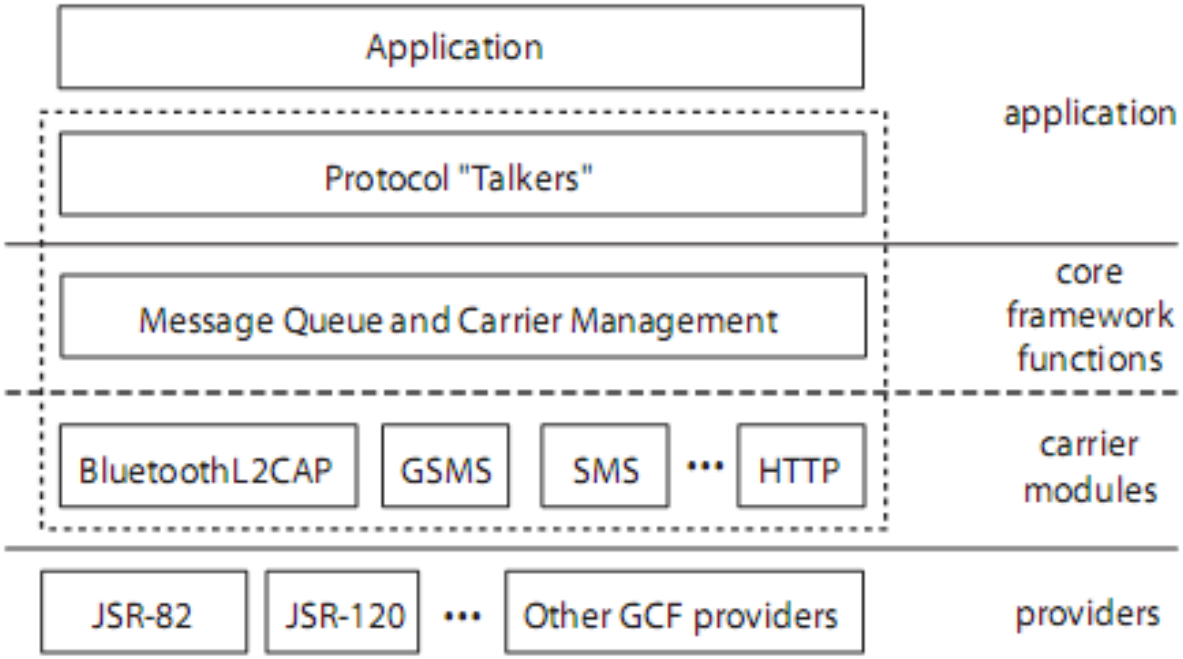


Communication Framework

- Support for multiple transport layers
- Reliable, flexible message routing
- Light user burden

Communication Framework

- Application Layer
- Management Layer
- Carriers



Performance

Access	Time (s)	Variance
Door Access	5.36	0.33
Windows XP Login	9.31	2.20

Action	Nokia 6620		Audiovox SMT 5600	
	Time (ms)	Variance	Time (ms)	Variance
RSA PSS	1780	480	1260	30
RMS Read (1.5KB)	697	100	60	4
RMS Write (1.5KB)	480	88	170	3
RMS Read (30KB)	900	115	90	20
RMS Write (30KB)	1109	78	200	28

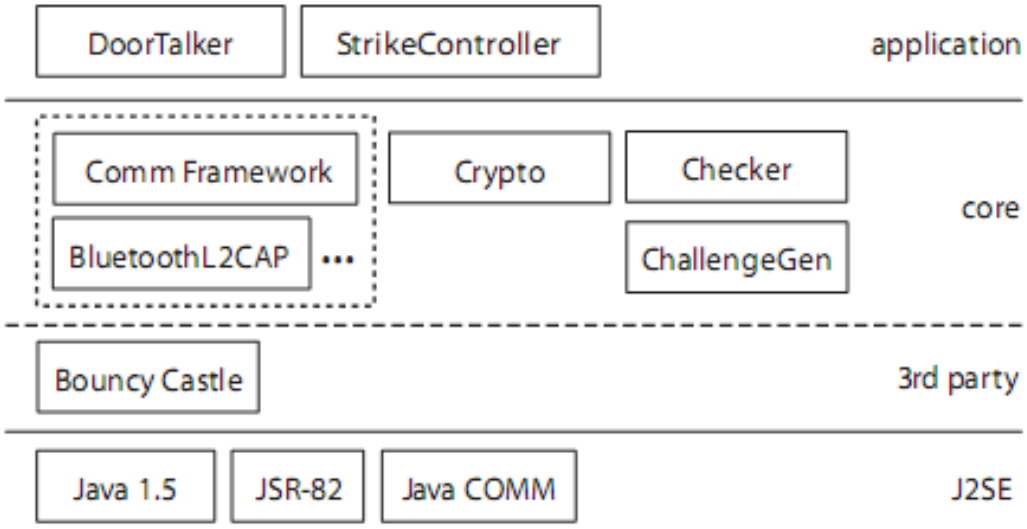
Office Access

Windows XP Login

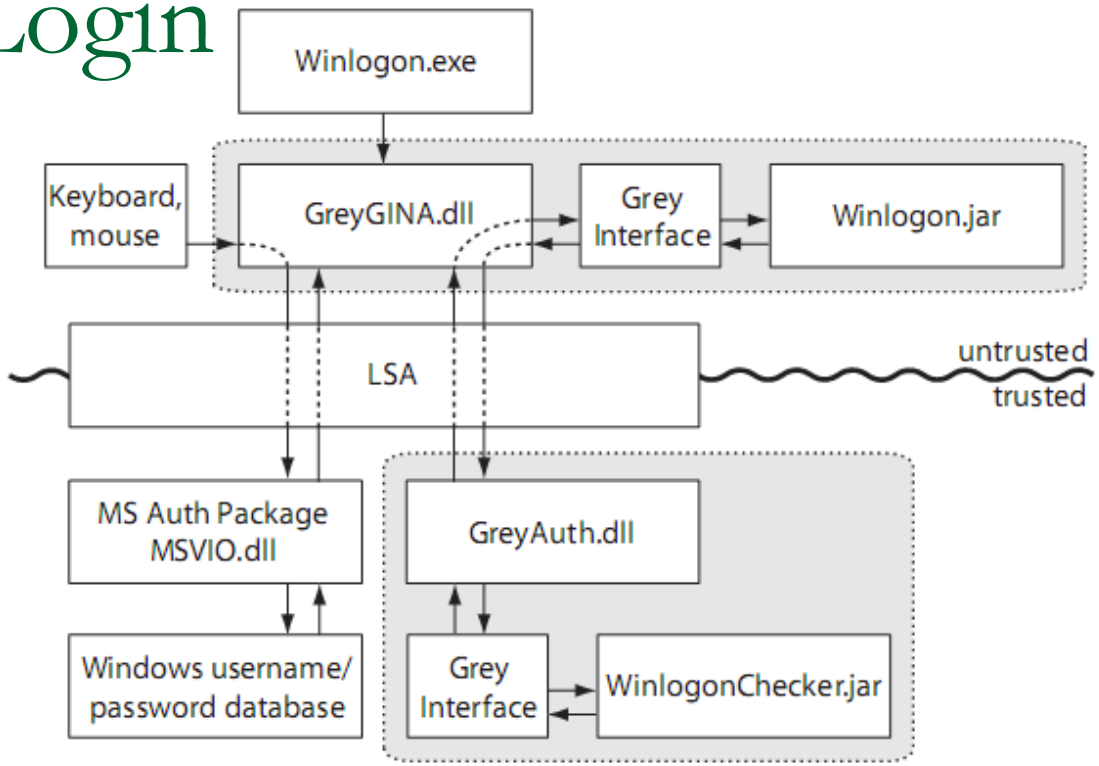
PILOT APPLICATIONS

Office Access

- Enables access to office doors
- Standard electrical door strike and embedded PC (4.55×3.75×1.70 inches).
  - Bluetooth and RS-485 relay controller



Windows XP Login

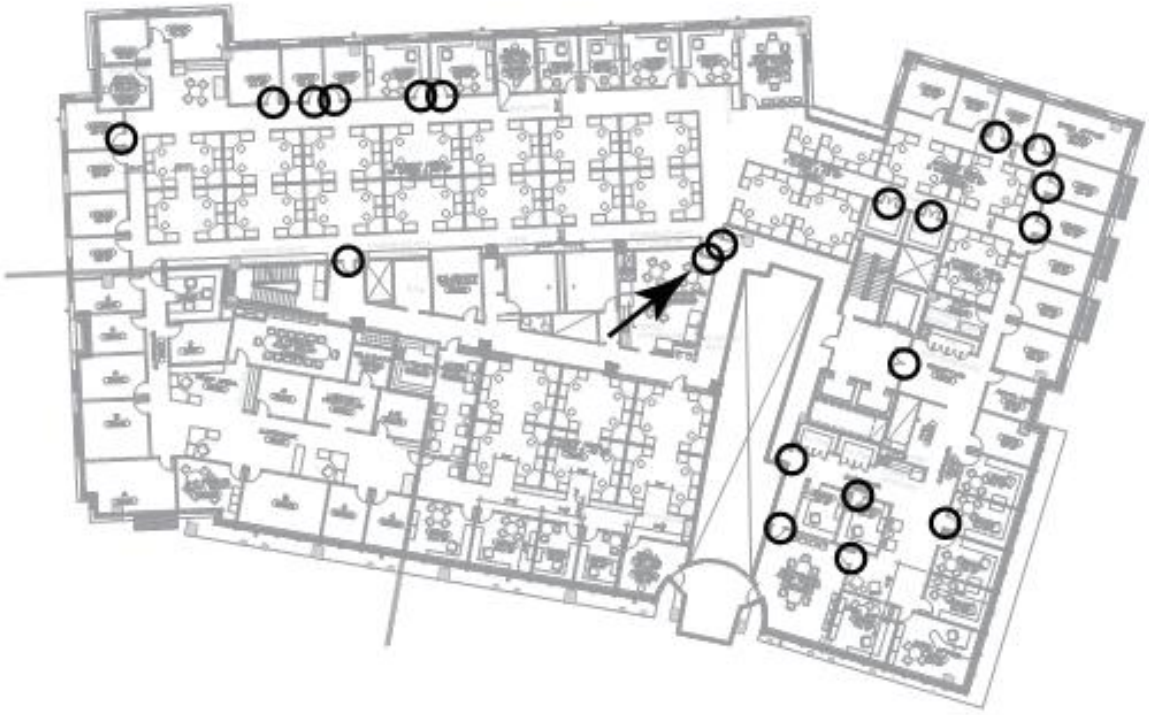


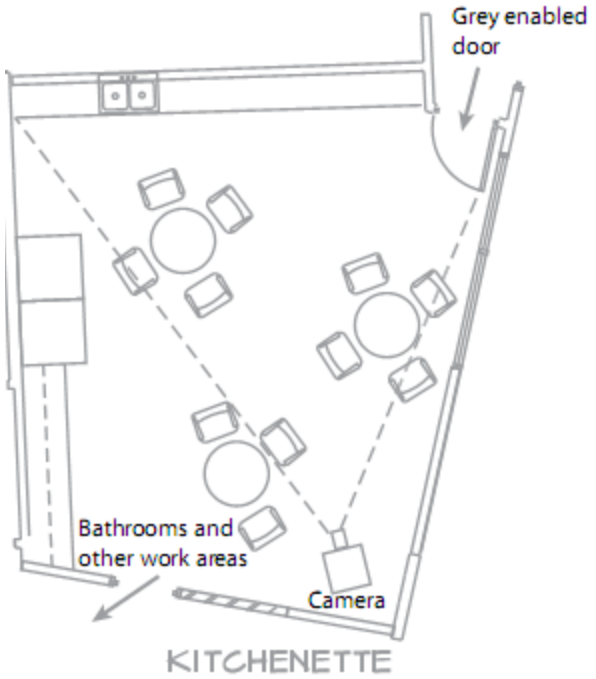
LESSONS LEARNED

Introduction

- 9 months and 19 participants
- Periodic interviews and logs generated by the system
- Principles of concern:
  - Usability downfalls
  - Network effects
  - New flexibility
  - End use behavior

Floor Plan




Grey enabled door
Bathrooms and other work areas
Camera
KITCHENETTE

Users

- Faculty, staff, students in the building
- 19 users
- Demographics:
  - 6 CS and ECE
  - 3 Technical Staff
  - 1 Administrative Staff
  - 16 male and 3 female

Procedure

- Conducted an initial interview
- Given the phone
- Basic Instructions
- Interviewed in a month and then every 4 to 6 weeks
  - All at desk or conference room

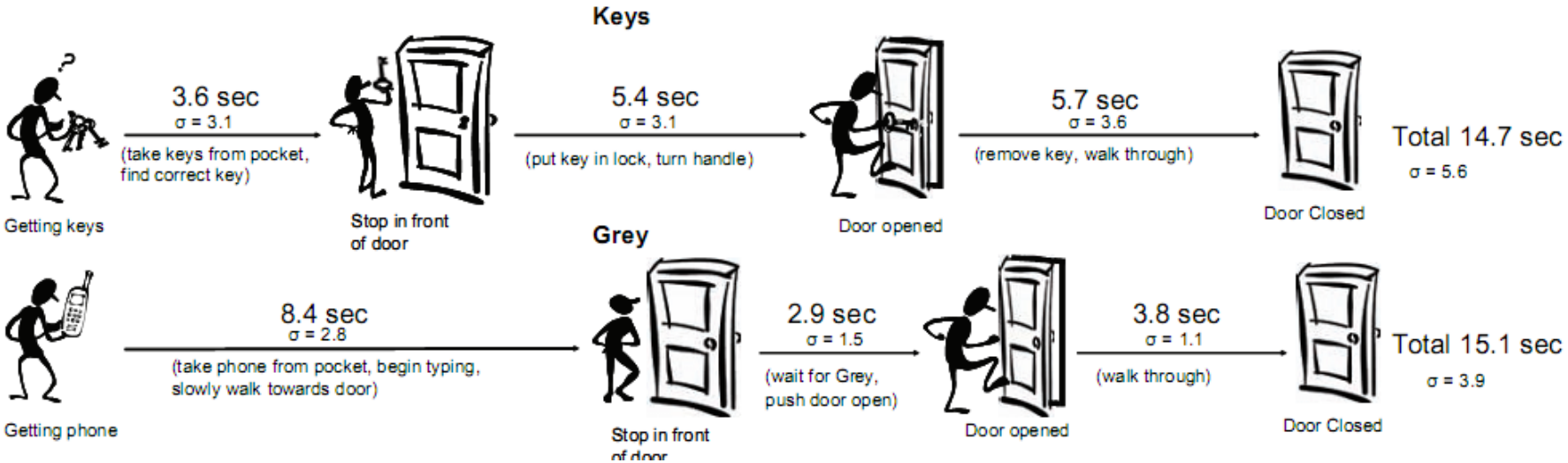
Data

- One year of data
- 19,500 Grey and 236,900 total access attempts
- Video of 70 accesses
- 30 hours of interview data
- Resources: 7.4 average (15 max, 2 min)
- Users: 5.7 average (11 max, 3 min)
- 18 still use the system

Lessons Learned

1. Perceived speed and convenience are critical to a user's satisfaction and acceptance
2. A single failure can strongly discourage adoption
3. Users won't user features they don't understand
4. Systems that benefit from the network effect are often untenable for small user populations
5. Low overhead for creating and changing policies encourages policy change
6. Unanticipated uses can bolster acceptance

Perceived speed and convenience are critical to a user's satisfaction and acceptance



A single failure can strongly discourage adoption

- Getting locked out caused user to go from 28 system requests to 7
- Delegation took so long that users thought it was broken
- Lent someone their phone

Users won't user features they don't understand

- Passed up more effective ways of delegation for simpler to use

Systems that benefit from the network effect are often untenable for small user populations

- To really start to be able to do amazing thing you need large user population and installation base

Low overhead for creating and changing policies encourages policy change

- Role based key policy of students, staff, and faculty
- Spare and hidden keys
- Delegation more casual, 11 received access to resource they did not have before
- Users ideal policy for 95% of access controls

Unanticipated uses can bolster acceptance

- Could open doors from the inside
- Satisfying clicking noises the door made

Discussion

- Why do technical users behave like non technical users?
- What access problems does this technology introduce?
- Is a smart phone the correct device to use?
- Is there a better distributed server system than desktop computers?