

## Computer security meets ubiquitous computing: Security for, and by, converged mobile devices

Michael Reiter

*Professor of ECE & CS  
Technical Director, CyLab  
Carnegie Mellon University*

20 May 2005

## Converged Mobile Devices (“Smartphones”)

### ■ Converged mobile devices (“smartphones”)

- ▼ Match wireless telephony to evolved OS or application environments
- ▼ Include the ability to download data to local storage, run applications, and store user data beyond PIM capabilities
- ▼ Leaders: Nokia, Motorola, Sony Ericsson, RIM, Samsung



### ■ Smartphones on a trajectory to “win” in the market

- ▼ IDC: Smartphones show “significant growth and future promise”, with compound annual growth rate of ~86% projected through 2007
- ▼ Gartner: 20 million will ship in 2006 (versus only 13 million PDAs)
- ▼ Stand to inherit mobile phone market that shipped over 648 million units in 2004—or **more than one phone per ten people in the world**

20 May 2005

Security for, and by, Converged Mobile Devices

2

## Progress Through Cellphone Deployment

### The Real Digital Divide

Encourage the spread of mobile phones is the most sensible and effective response to the digital divide

The Economist, March 10, 2005

... The digital divide that really matters, then, is between those with access to a mobile network and those without. The good news is that the gap is closing fast. The UN has set a goal of 50% access by 2015, but a new report from the World Bank notes that 77% of the world's population already lives within range of a mobile network.

## New Applications on the Horizon

### DoCoMo trials Sony Felica smart chip mobile phones

i4u, December 16, 2003

... One service being tested ... allows residents of a new apartment complex to use the FeliCa-equipped phones as keys to both the main entrance and their homes.

The phone can also pay utility bills when swiped against a reader at the building's entrance.

### Smart phones work like train tickets

AP, February 22, 2005

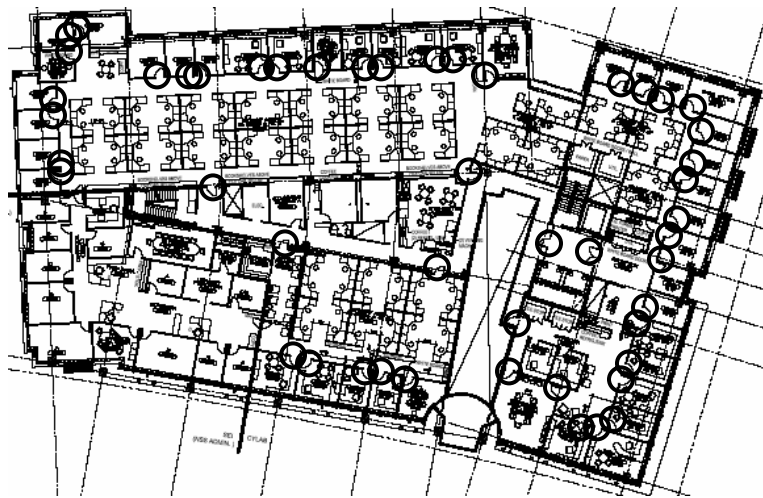
... With a service planned for launch in January next year, they'll be able to use their mobile phones in place of the cards to pay for their train fares ... Users will also be able to use their Suica-compatible cell phones to pay at some restaurants, convenience stores and shops. ... The service will later be expanded to include online shopping and reserved ticket purchases.

## Our Take on This Vision: The Grey System

[w/ Bauer, Garriss, McCune, Rouse]

- Existing efforts utilize these devices as a replacement for existing mechanisms (charge card, physical keys, ...)
  
  - However, we believe this device-centric paradigm can support more flexible approaches than previously possible
    - ▼ Loan you my car without giving you my phone
    - ▼ Send money from my phone to my daughter's phone
    - ▼ Give your secretary temporary access to your email without revealing information (e.g., password) that could be used at a later time
    - ▼ Use your phone to open your hotel room door, without ever stopping by the front desk
- ... and do it all from a distance

## A Planned Deployment at CMU



## Capabilities of Smartphones

- **Good data connectivity**
  - ▼ Bluetooth: short range radio link
  - ▼ 2.5G (GPRS, ...) / 3G (UMTS, ...) for wireless access to data networks
  - ▼ Messaging protocols: MMS and SMS
- **Growing computation power: public-key crypto is within range**
  - ▼ For example,  $x^y \bmod z$  in
    - ▼ ~455ms for  $|x| = |z| = 1024$  and  $|y| = 160$
    - ▼ ~2.5s for  $|x| = |y| = |z| = 1024$on the (already dated) Nokia 6600
- **Rich graphical input and output**
  - ▼ Graphical display and camera

## Some Challenges

- **A sufficiently flexible authorization infrastructure**
  - ▼ Must support usual modes of access and delegation for each protection mechanism it is to replace, and more
- **Device theft**
  - ▼ Should ensure that stolen devices cannot be misused
- **Usability**
  - ▼ Human-to-device authentication
  - ▼ Device-to-device authentication
  - ▼ Access-control policy creation

## Logic-Based Access Control

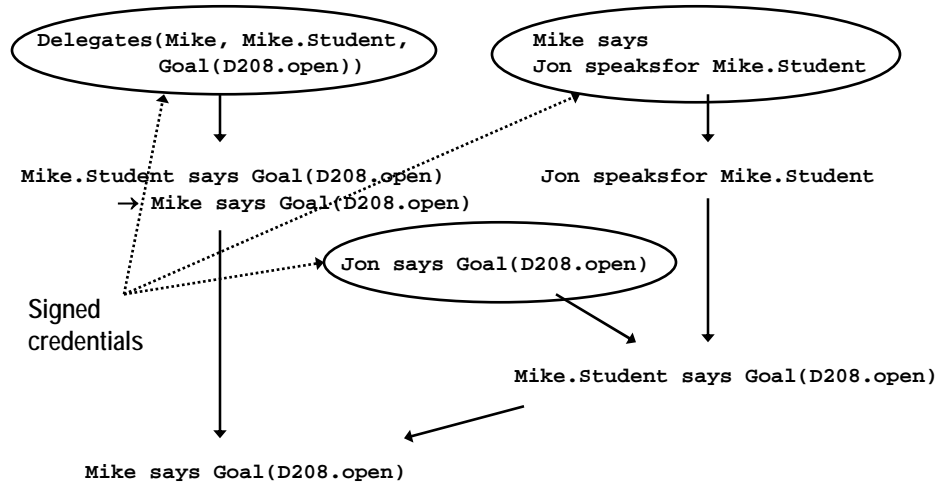
[Lampson, Abadi, Burrows & Wobber 1992; ...]

- Access-control decision procedure can be modeled by a formal logic
- Logic might consist of
  - ▼ Strings `Lujo, Mike, CMU.HH.D208`
  - ▼ Channels `0x4C892BD...` (public key)
  - ▼ Groups `Mike.Students, CMU.Faculty`
  - ▼ Statements `Jon says Goal(CMU.HH.D208.open),  
Jon speaksfor Mike.Students,  
delegates(Lujo, Lujo.Mike, Goal(...))`

## Our Starting Point

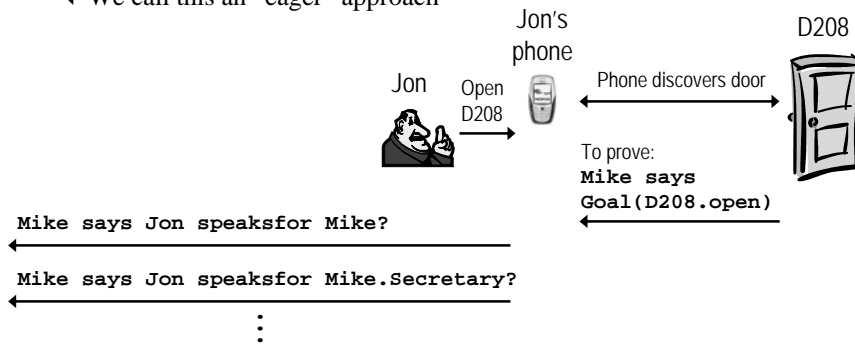
- Logic-based techniques such as “Proof-Carrying Authorization”  
[Appel & Felten 2000; Bauer et al. 2002]
  - ▼ Server implements checker for higher-order logic
  - ▼ Client makes proofs in an application-specific logic for which proof generation is efficient
- Permits expression of arbitrarily complex policies in framework
- Numerous potential limitations in practice, however
  - ▼ No implementations have been deployed, much less evaluated in realistic conditions

## An Example Proof (Sketch)



## Traditional Approach to Proof Generation

- Client runs tactical theorem prover, working backward from goal
- Tactics guide client to achieve as much as possible of the proof
  - ▼ Client queries for credentials to realize proof assumptions
  - ▼ We call this an “eager” approach



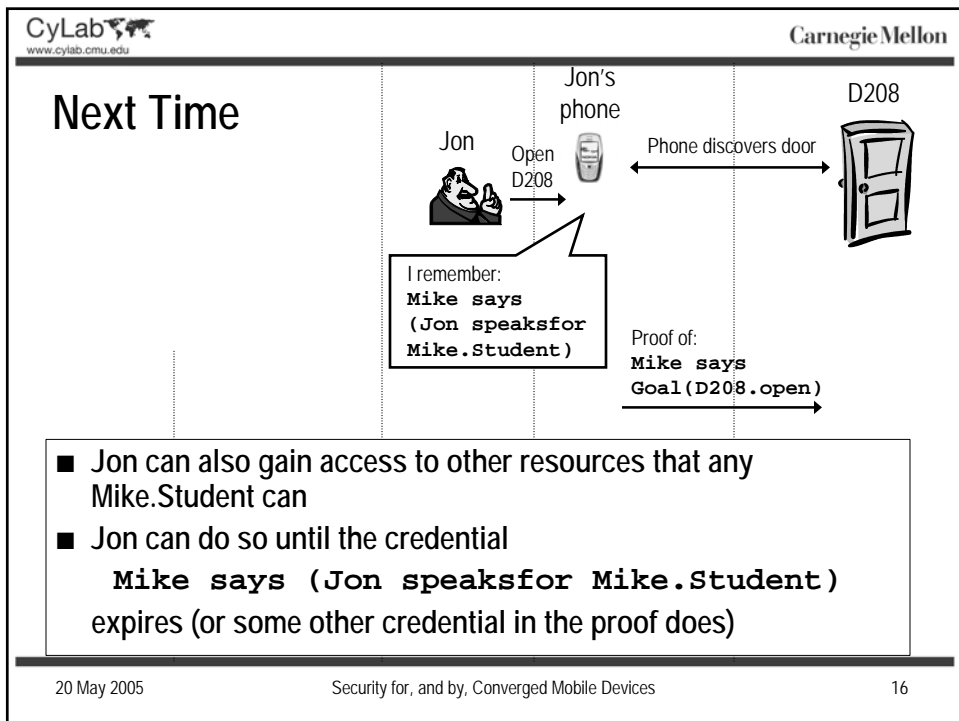
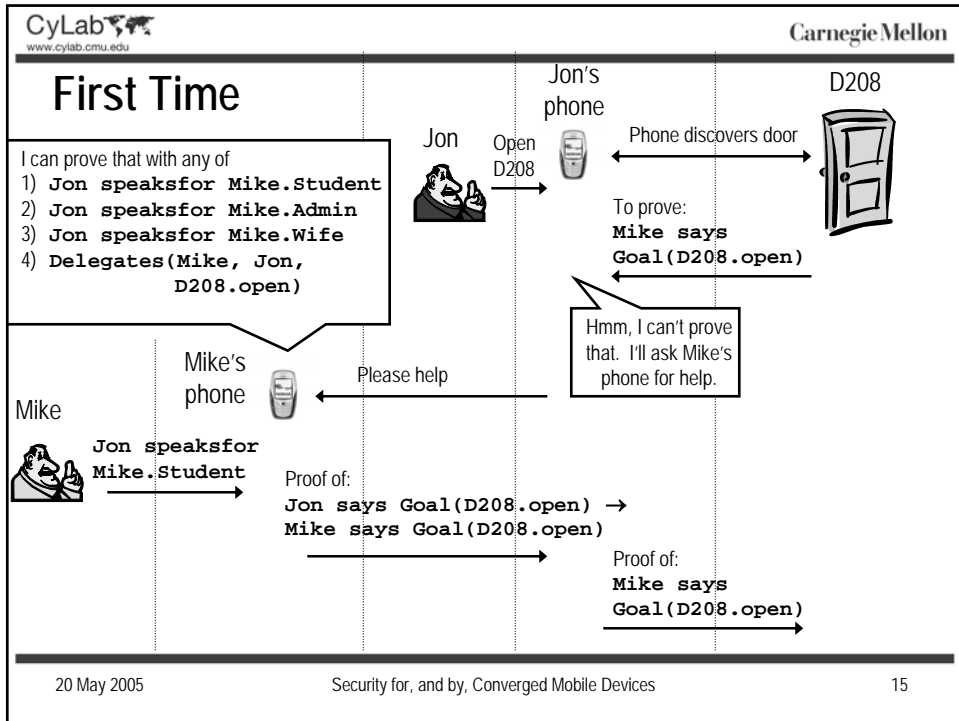
## A “Lazy” Approach

[w/ Bauer and Garriss. *IEEE Symposium on Security and Privacy*, 2005.]

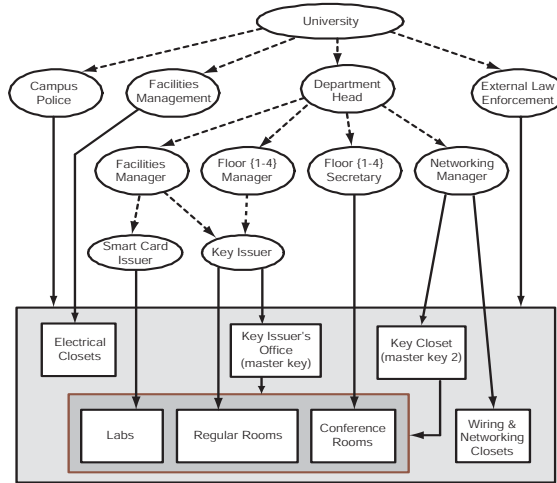
- Problems with the eager approach
  - ▼ Prover must request certificates without knowledge of what certificates are available or will be signed
    - ▼ Prover may request certificates for too much authority, or too little
  - ▼ Eager approach offers no opportunities for infrastructure to “learn” from computed proofs
  
- As a result, we employ a “lazy” approach in this work
  - ▼ Prover outsources proofs of subgoals to others
  - ▼ Far more efficient and usable proof construction
  - ▼ Permits infrastructure to adapt through caching and *automatic tactic generation*

## An Example Scenario

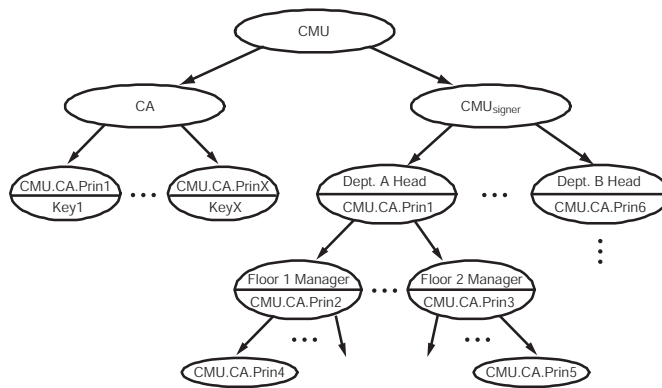
- Jon and I have smart phones running Grey
  - ▼ In particular, proof generators
- The door is running Grey, too
  - ▼ In particular, a proof verifier that controls an electric strike
  
- I have previously created signed credentials (**Mike says ...**)
  - `Delegates(Mike, Mike.Student, Goal(CMU.HH.D208.open))`
  - `VF: Delegates(Mike, Mike.Admin, Goal(CMU.F))`
  - `Mike.Wife speaksfor Mike`
  - `Key(0xA84C32...) speaksfor Mike.Wife`
  - `Key(0x75DD1B...) speaksfor Mike.Admin`
  - `Key(0x316A6B...) speaksfor Jon`



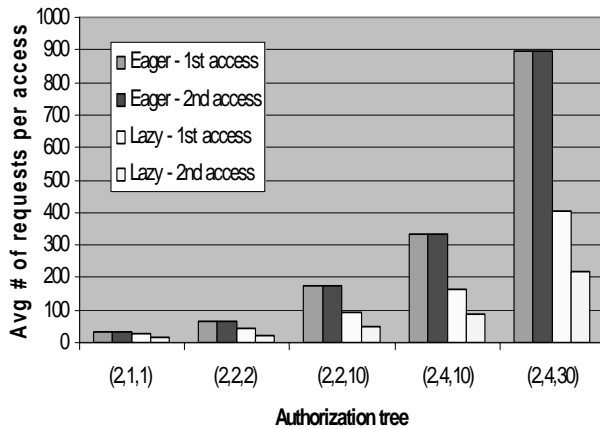
## A Real (Subset of a) Policy



## An Abstract Policy

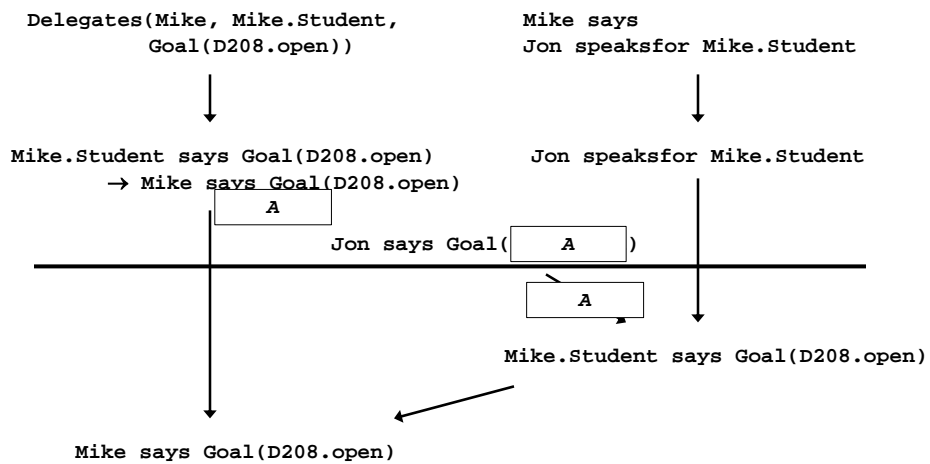


## Lazy's Cache Is More Useful

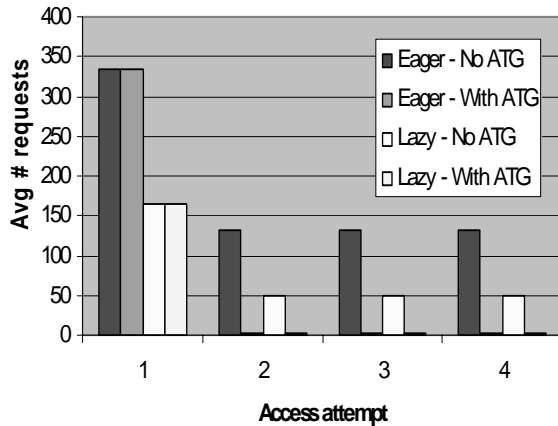


- Shows subsequent access by different principal to different resource
- Provers on "interior" nodes can cache results
- Caching benefits others in lazy proving, but not in eager

## Automatic Tactic Generation



## Automatic Tactic Generation



- ATG remembers the “shape” of proofs, but abstracted so as to be applicable to other goals
- Graph shows sequential access of four resources by same principal in a (2,4,10) tree

## Capture and Misuse



### Thieves get away with Israeli spy chief's phone

Reuters, March 3, 2004

... Meir Dagan, the retired general who heads Israel's shadowy foreign intelligence agency, lost the phone when his car was broken into in Tel Aviv last month. ....

“There were quite a few numbers of agents and secret service heads stored there.”

### Hackers post Paris Hilton's address book online

IDG, February 21, 2005

... The address book contains information on over 500 of Hilton's acquaintances, including super celebrities such as Eminem and Christina Aguilera. ... Hilton was ... reportedly compromised in an attack on T-Mobile's network that netted information on 400 of the company's customers, including sensitive information from the account of a U.S. Secret Service agent.

## Capture-Resilient Cryptographic Devices

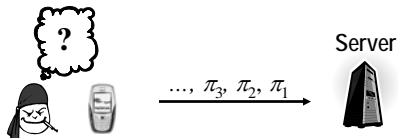
[w/ MacKenzie. *International Journal of Information Security*, 2003.]

- A device that cannot be used by other than its rightful owner
  - ▼ No amount of reverse engineering exposes its cryptographic secrets
  - ▼ Does not rely on tamper-resistant hardware; a software-only solution

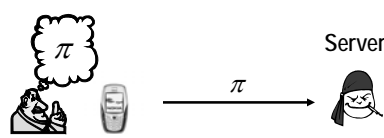


- Approach leverages networked nature of device
  - ▼ Most interesting uses of a key require network anyway
- Idea: The environment confirms that the device remains in its owner's possession before permitting its key to be used
  - ▼ Component in environment is called a "capture-protection server"

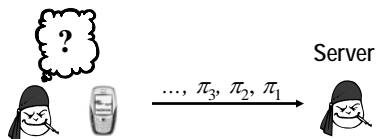
## Capture-Resilience Properties



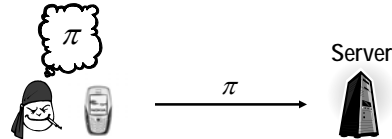
Attacker must succeed in online dictionary attack



Attacker gains no advantage

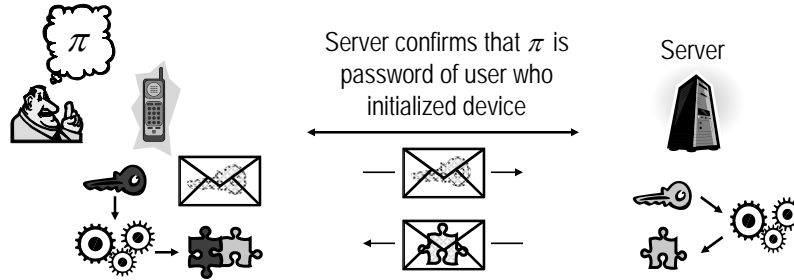


Attacker must succeed in offline dictionary attack



Attacker can forge only until server is *disabled* for device

## Solution Overview



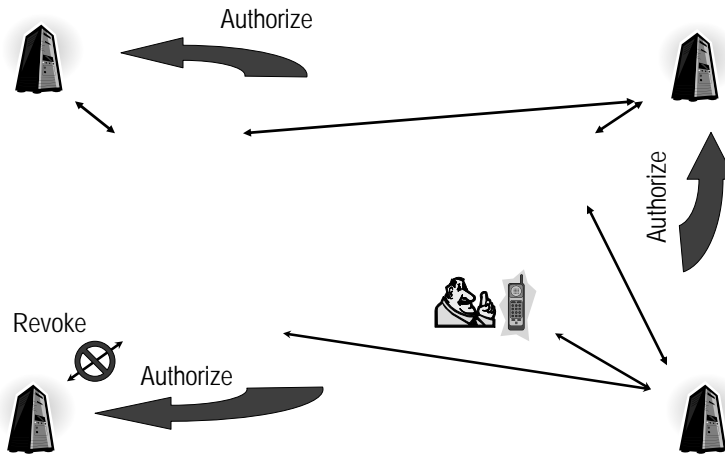
- Known techniques depend on particular form of private key
  - ▼ All use two-party function sharing

## The Cost of Disabling

	Public key operation	Private key operation	Messages	Device exps	Server exps
<b>RSA signatures</b>	verify $s^e \bmod n = h(m)$	$s \leftarrow h(m)^d \bmod n$ return $s$	2	2	3
<b>ElGamal encryption</b>	$r \leftarrow_R \mathbf{Z}_q$ $c_1 \leftarrow g^r \bmod p$ $c_2 \leftarrow my^r \bmod p$ return $\langle c_1, c_2 \rangle$	return $c_2 / (c_1)^x \bmod p$	2	5	5
<b>DSA signatures</b>	$z \leftarrow (s_2)^{-1} \bmod q$ verify $s_1 \equiv_q g^{h(m)z_1 y s_2 z} \bmod p$	$r \leftarrow_R \mathbf{Z}_q$ $s_1 \leftarrow g^r \bmod p$ $s_2 \leftarrow (h(m) + xs_1) / r \bmod q$ return $\langle s_1 \bmod q, s_2 \rangle$	4	46	50

## Delegation in Capture Protection

[w/ MacKenzie. *Distributed Computing*, 2003.]



## Usability: Device-to-Device Authentication

- As in any setting employing keys, we need to solve the key authentication problem
- This is determining for whom a key “speaks”
  - ▼ When receiving a message  $M$  for which a signature can be verified by key  $K_A$ , i.e., we determine
 
$$K_A \text{ says } M$$
 we would like to be able to conclude
 
$$A \text{ says } M$$
 where  $A$  is a named principle (e.g., a person)
  - ▼ To do this, we need to know the person  $A$  for whom  $K$  speaks, i.e.,

$$K_A \text{ speaksfor } A$$

## Location-Limited Channels

- When both the recipient and  $A$  are devices in physical proximity, this can be done using a *location limited channel*
  - ▼ Uses physical proximity to defeat man-in-the-middle (MITM) attacks
- Numerous location-limited channels have been proposed
  - ▼ Some are not supported by most phones
    - ▼ Physical touch [Stajano and Anderson 1999]
  - ▼ Some are not secure
    - ▼ Bluetooth or other short-range radio is still susceptible to MITM
  - ▼ Some are not convenient
    - ▼ Audible shared password to secure radio [Bellovin & Merritt 1992]
    - ▼ Infrared connection [Balfanz et al. 2002]
  - ▼ Most are not intuitive

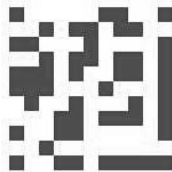
## Seeing is Believing (SiB)

[w/ McCune and Perrig. *IEEE Symposium on Security and Privacy*, 2005.]

- Use machine vision as a side channel
- To establish belief in

$K_{Mike}$  **speaksfor** Mike

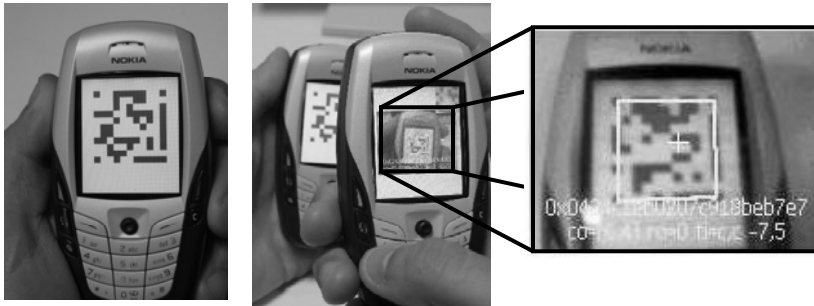
Mike's device displays  $K_{Mike}$  using a 2-dimensional barcode



- Recipient simply photographs the barcode!

## An Implementation

- Bandwidth of current barcodes is too low to encode  $K_{Mike}$
- So, *Mike's* device displays  $h(K_{Mike})$ , instead
  - ▼  $K_{Mike}$  is then conveyed, e.g., over radio, and authenticated using hash sent visually



20 May 2005

Security for, and by, Converged Mobile Devices

31

## Has Numerous Other Applications

- Can authenticate devices without a camera
- And even without a display (e.g., by attaching a sticker)



20 May 2005

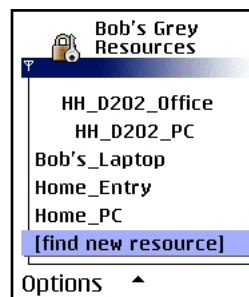
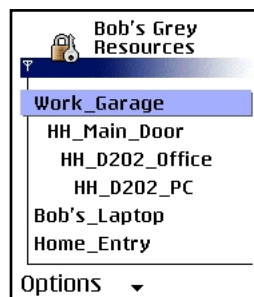
Security for, and by, Converged Mobile Devices

32

## SiB and TCG

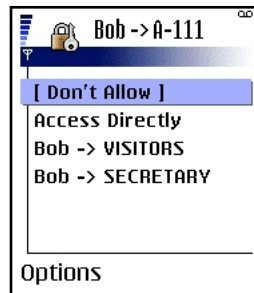
- A TCG-enabled platform contains a hardware component called the Trusted Platform Module (TPM)
  - ▼ TPM “measures” the software that is loaded on the computer
  - ▼ Also offers conditional key release, so a key is made available for use only by the intended software
- SiB provides a means for
  - ▼ Securely configuring the TPM
  - ▼ Confirming that an application running in a particular window is, in fact, the expected application
- See paper for details

## The Grey UI: Requesting Access



- Grey learns “paths” of habitual access
- When a path is selected, phone accesses resources in order
  - ▼ Each step contingent on the previous
- Also permits user to input new resource addresses
  - ▼ By camera (barcodes) or by Bluetooth discovery

## The Grey UI: Granting Access



- Owner can choose to deny access, or from among alternatives for granting access
- This selection produces a credential that is returned to Bob
- At most, this user need only enter her PIN after making a selection

## Conclusion

- Converged mobile devices “everywhere” are a safe bet
  - ▼ We need to figure out how to use them
- We are currently developing a system to deploy on the CMU campus to demonstrate ubiquitous access control using them
- Thus far, the project embodies several advances
  1. New “lazy” distributed proving methods in the context of a flexible authorization system
    - ▼ Can generate any proof that a centralized approach can
    - ▼ Far more efficient than prior work, particularly when paired with automatic tactic generation

## Conclusion (continued)

2. **An approach for defending a key from misuse even if device holding it is captured and reverse-engineered**
  - ▼ Does NOT expose key to server
  - ▼ Server can be used to disable device even if attacker knows password
  - ▼ Delegation enables new servers to be authorized dynamically
3. **New location-limited channels for bootstrapping key authentication**
  - ▼ Utilizes cameras on modern smartphones to provide a convenient location-limited channel