Seeing-Is-Believing: Using Camera Phones for Human-Verifiable Authentication

May 10, 2005

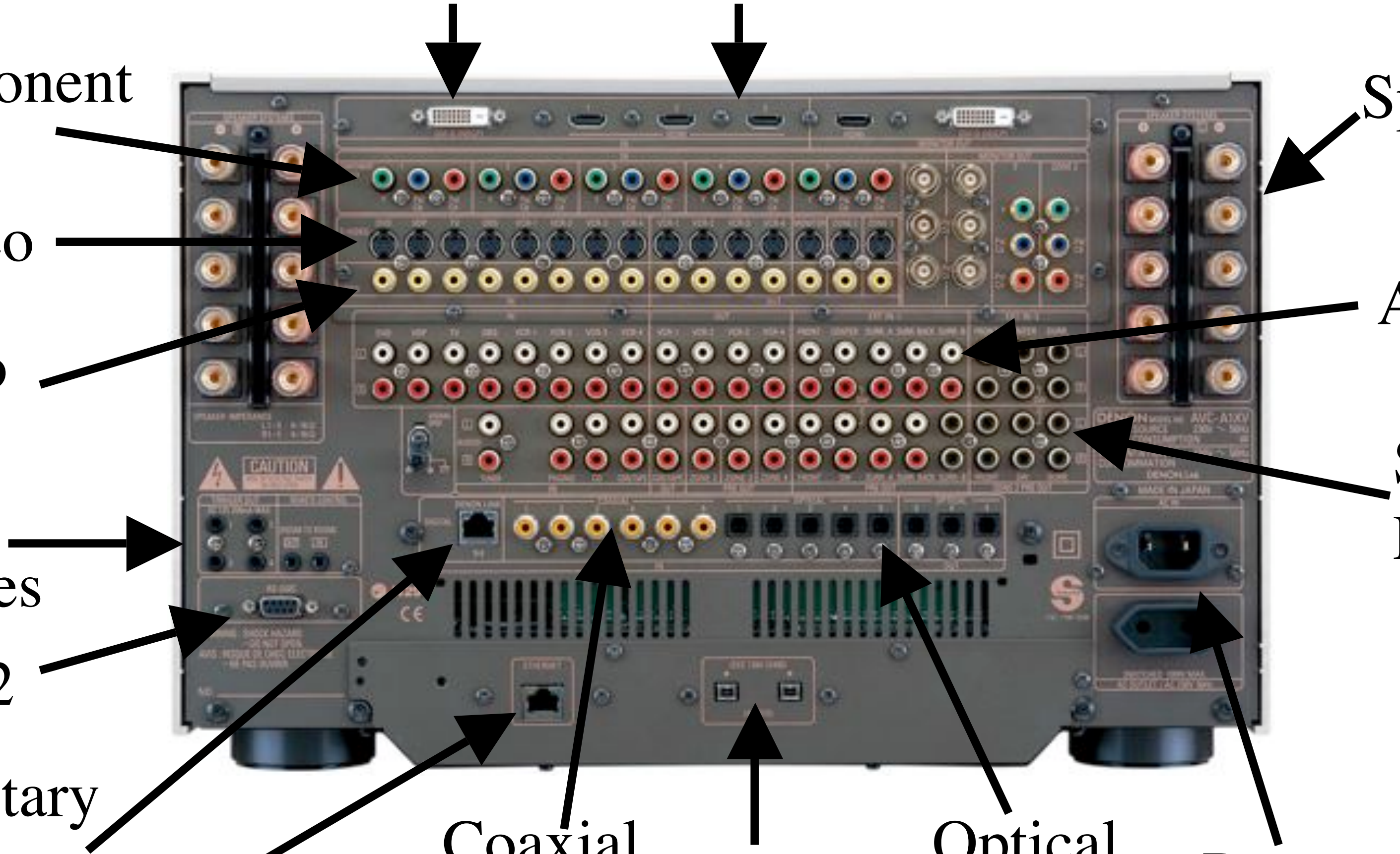
Jonathan McCune,
Adrian Perrig, Mike Reiter

Carnegie Mellon University

Ubiquitous Electronics

- More devices every day
- More device interaction

Too Many Connections!



DVI

HDMI

Component Video

S-video

Video

Add'l Remotes

RS-232

Proprietary Digital

Ethernet

Coaxial Digital

Firewire

Optical Digital

Power

Speakers

Audio

Surround Processor

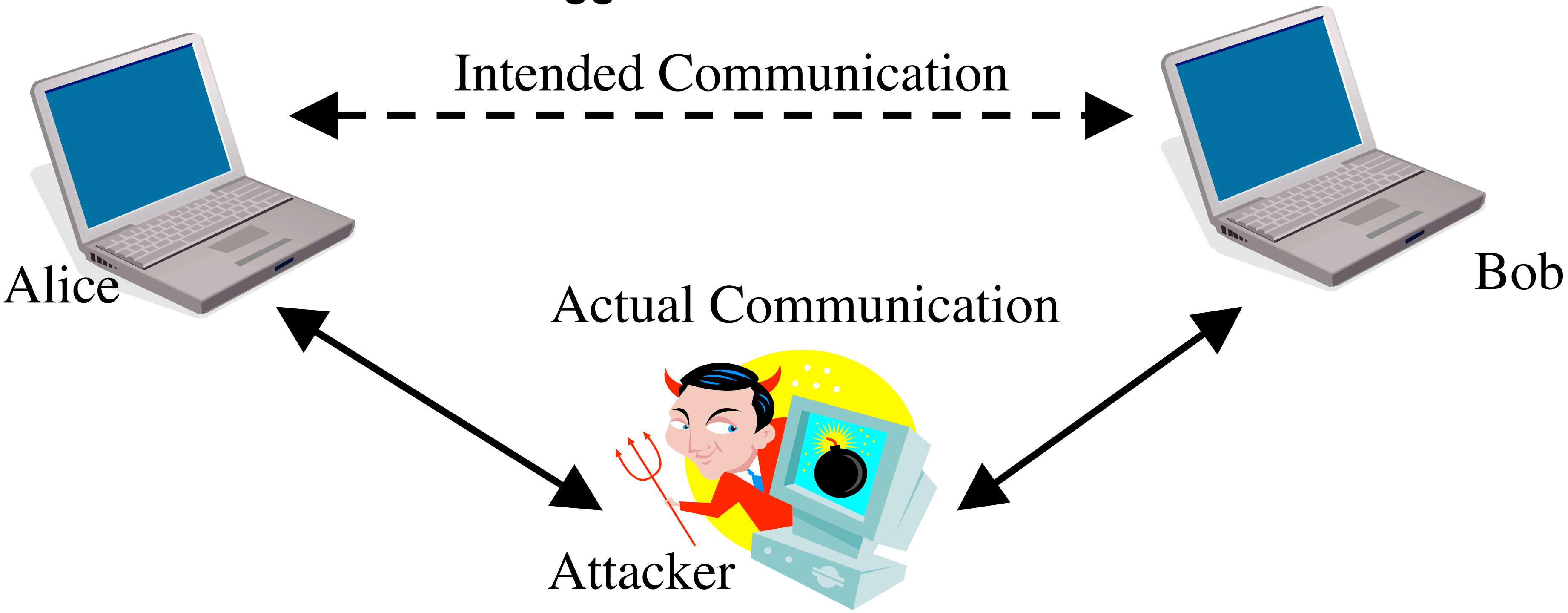
Go Wireless!

- **802.11, Bluetooth, Ultra Wide Band, Zigbee, GPRS, …**
- **Cable replacement!**
  - Computer to printer
  - MP3 player to computer
  - Cell phone to laptop
  - Cable box to TV
  - … and many others

- **Introduces a problem…**

Man in the Middle!

- Attacker can easily control communication between wireless devices
- More devices == bigger threat



Solution?

- **Communication must be authenticated**
  - Rules out man-in-the-middle
  - Bootstraps secret and private communication
  - Reduced problem: key setup
- **Challenges**
  - No prior context between devices
  - No centralized authority to do configuration
  - No expertise in user
  - Transient network topology (mobility, power-saving, …)
  - Different device vendors

Prior Work

- **Resurrecting Duckling [Stajano & Anderson 1999]**
  - Two state device (duckling)
  - Can be “imprinted” multiple times (device ownership)
  - Mother gives “life” via **physical contact**
    - Establishes shared secret
    - Rules out man-in-the-middle
    - Very convenient for user
- **Disadvantages**
  - Interface unavailable in commodity devices

Prior Work

- **Talking to Strangers [Balfanz et al., NDSS 2002]**
  - Extends ideas in Resurrecting Duckling
    - No communication through physical contact today
  - Demonstrative identification (***that*** device)
  - Location-limited side channel
    - MitM hard if channel severely limits proximity
- **Infrared**
  - Restricts location of attacker
- **Disadvantages**
  - Infrared invisible to humans
  - Infrared not available in all devices

Seeing-Is-Believing

- **Modern mobile phones**
  - Camera (read 2D barcodes)
  - Display (display 2D barcodes)
  - Powerful CPU (perform asymmetric cryptographic operations)
- **Used in concert, we have a new, *visual*, location-limited channel**
- **This visual channel *can* provide *demonstrative identification* of communicating parties to the user**
- **Available in commodity devices**
- **This enables very strong authentication**

Authenticating a Public Key with SiB

Alice

Bob

$h_a \leftarrow \mathrm{SHA1}(PK_A)$

$\xrightarrow{h_a}$

$(visual)$

$\xrightarrow{PK_a}$

$(wireless)$

$h' \leftarrow \mathrm{SHA1}(PK_A)$

$if\,(h' \neq h_a) : abort$

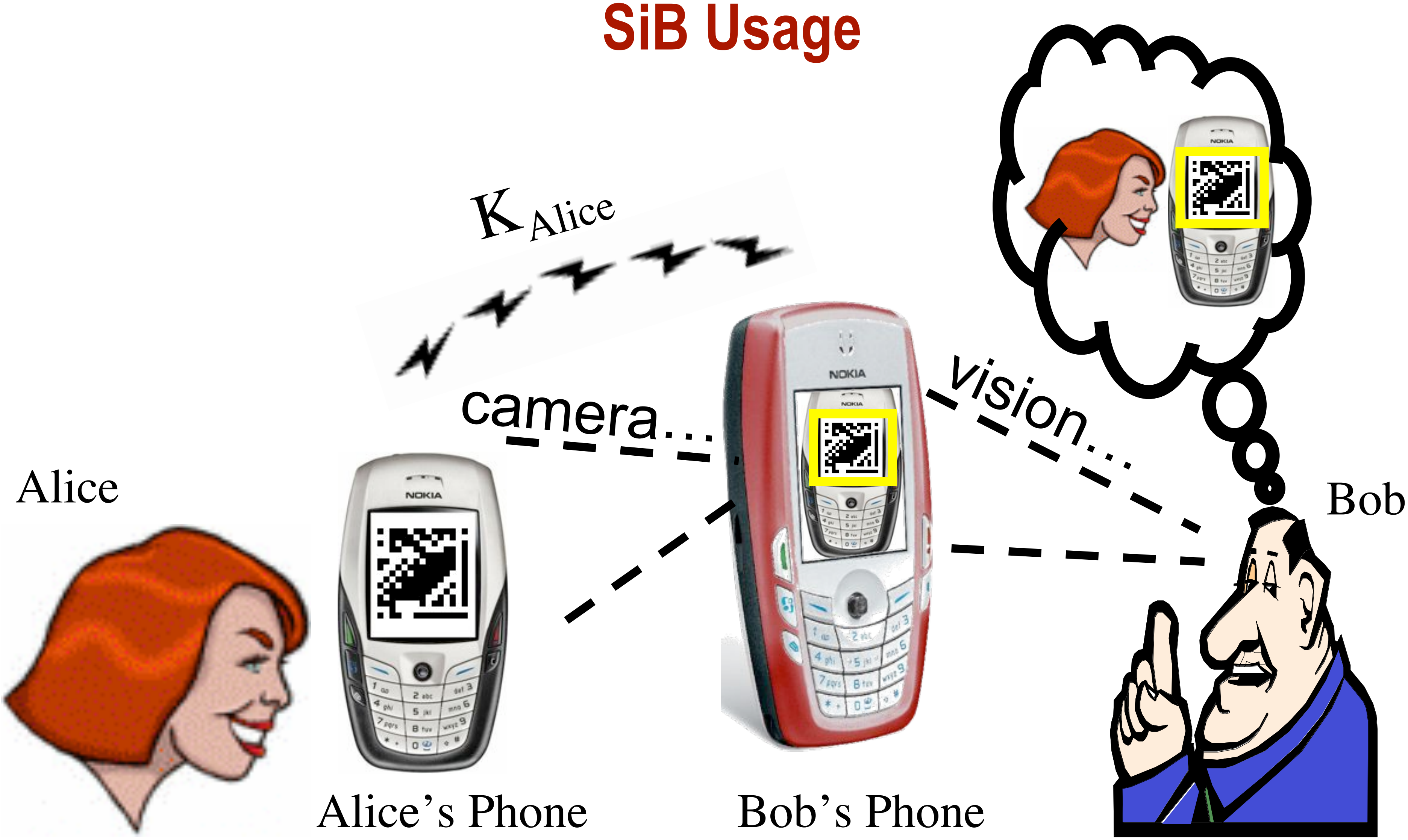
Motivations for SiB

- **Ubiquitous computing in the home**
- **Bootstrapping secure communications**
  - Email (well known from, e.g., PGP)
  - Text messaging (end-to-end encryption & authentication)
  - Voice calls (end-to-end encryption & authentication)
- **Aid in the establishment of *trusted paths* from a user to applications on her computer**
  - Interacting with a Trusted Platform Module (TPM)
  - Entering passwords
  - Assuring that a particular application receives user input

Outline

- **SiB phone-to-phone usage example**
- **Properties of different device configurations**
  - Devices may not have cameras
  - Devices may not have displays
- **Examples with limited devices**
  - Public printer
  - Setting up connection between TV and DVD Player
- **Examples with Trusted Computing Group (TCG)**
  - Taking ownership of a TPM
  - Verifying display ownership
- **Implementation details**

SiB Usage



Mutual Authentication

- Both parties perform basic SiB protocol to get authenticated public key of other party
- SiB authenticates origin of public key
- Can use freshly generated keys
  - Different public keys for different people
  - Achieve unlinkability between sessions

Device Configurations

- Both devices have cameras and displays (most powerful configuration)
- SiB can be useful even if some devices are missing a camera, a display, or both
  - Display but no camera
    - Laptop, PDA, television, …
  - No display and no camera
    - 802.11 access point, printer, …

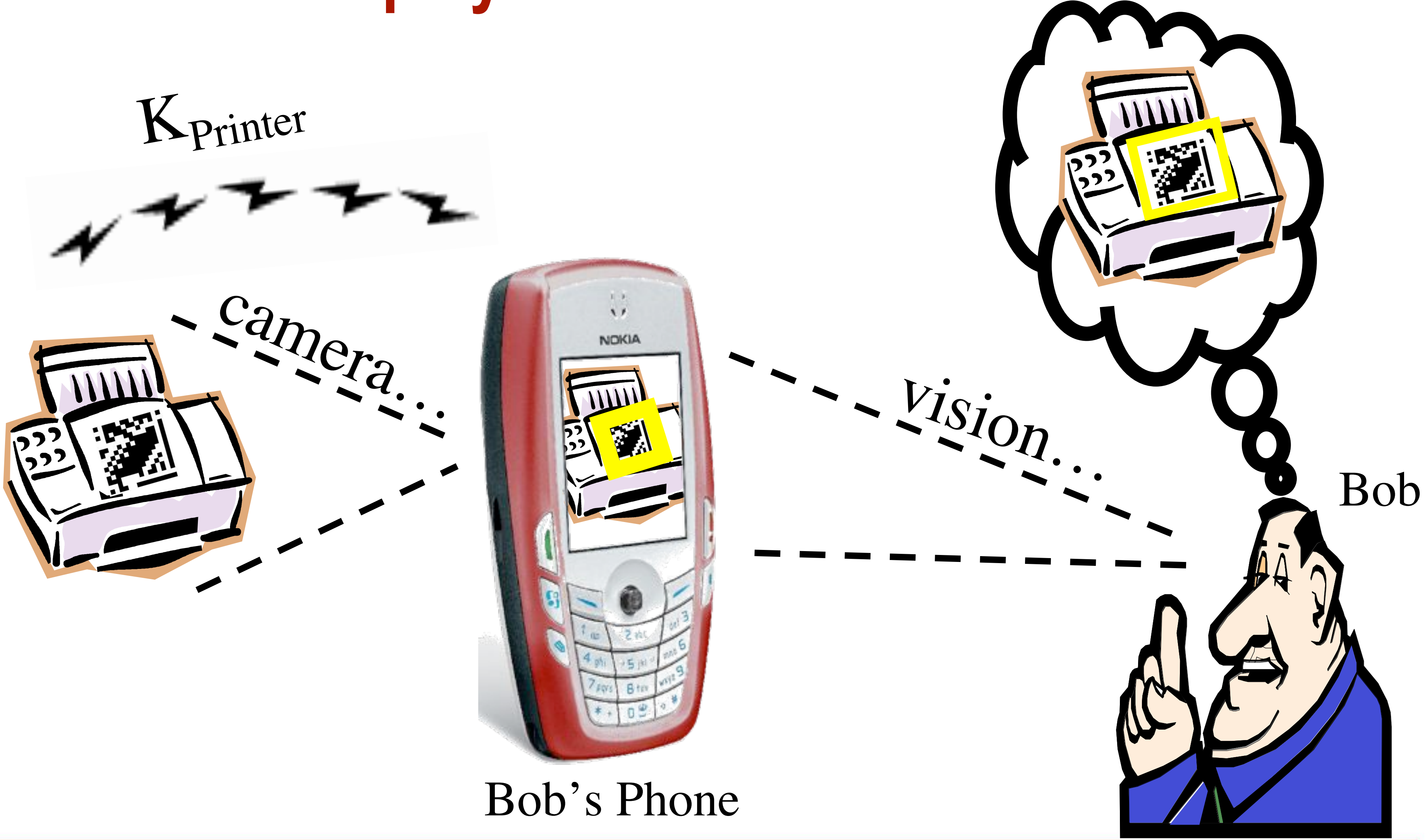
No Display and No Camera Devices

- Equipped with a long-term public key and a barcode sticker on housing
  - Cannot use freshly generated public keys
- The resulting communication channel (following SiB) remains secure against active adversaries

Bob’s Phone

Bob

No Display and No Camera Devices



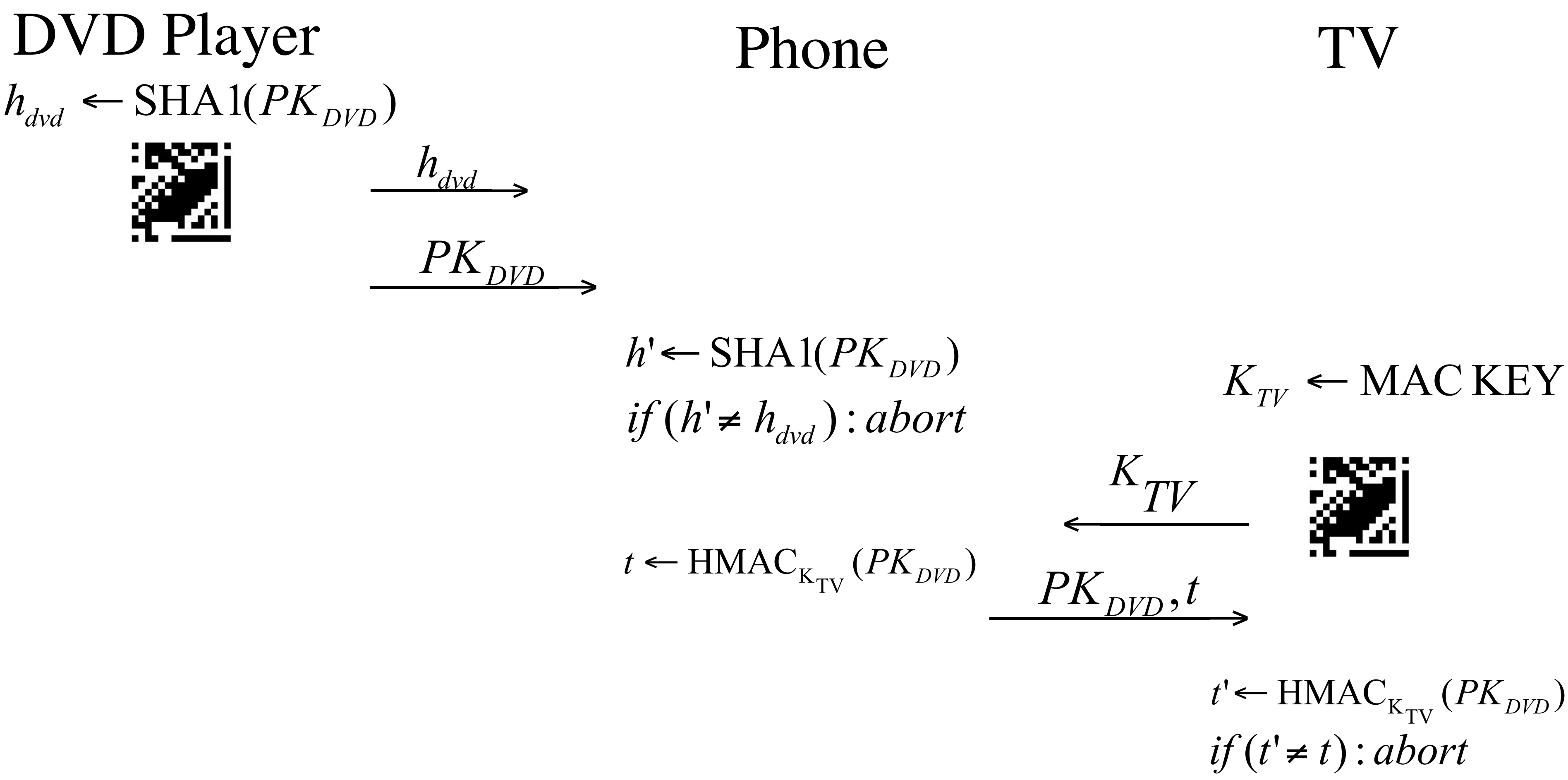
Display but No Camera Devices

- ***Camera-less*** **devices cannot authenticate other devices with SiB**
- **If display-equipped, they can still generate barcodes so they can be authenticated**
- **Can obtain a** *presence* **property**
  - The device knows something is in line-of-sight with the display
  - Can display a challenge during a short time

Example of Presence Property

- We have a TV and a DVD player
- Assume they communicate wirelessly
- Want to set up secure communication
  - Authenticated
  - Encrypted
- Want to give DVD player’s public key to the TV in a secure way

Presence Protocol Example



DVD Player

Phone

TV

$h_{dvd} \leftarrow \mathrm{SHA1}(PK_{DVD})$

$\xrightarrow{h_{dvd}}$

$\xrightarrow{PK_{DVD}}$

$h' \leftarrow \mathrm{SHA1}(PK_{DVD})$

$if\,(h' \neq h_{dvd}) : abort$

$K_{TV} \leftarrow \mathrm{MAC\ KEY}$

$\xleftarrow{K_{TV}}$

$t \leftarrow \mathrm{HMAC}_{\mathrm{K}_{\mathrm{TV}}}(PK_{DVD})$

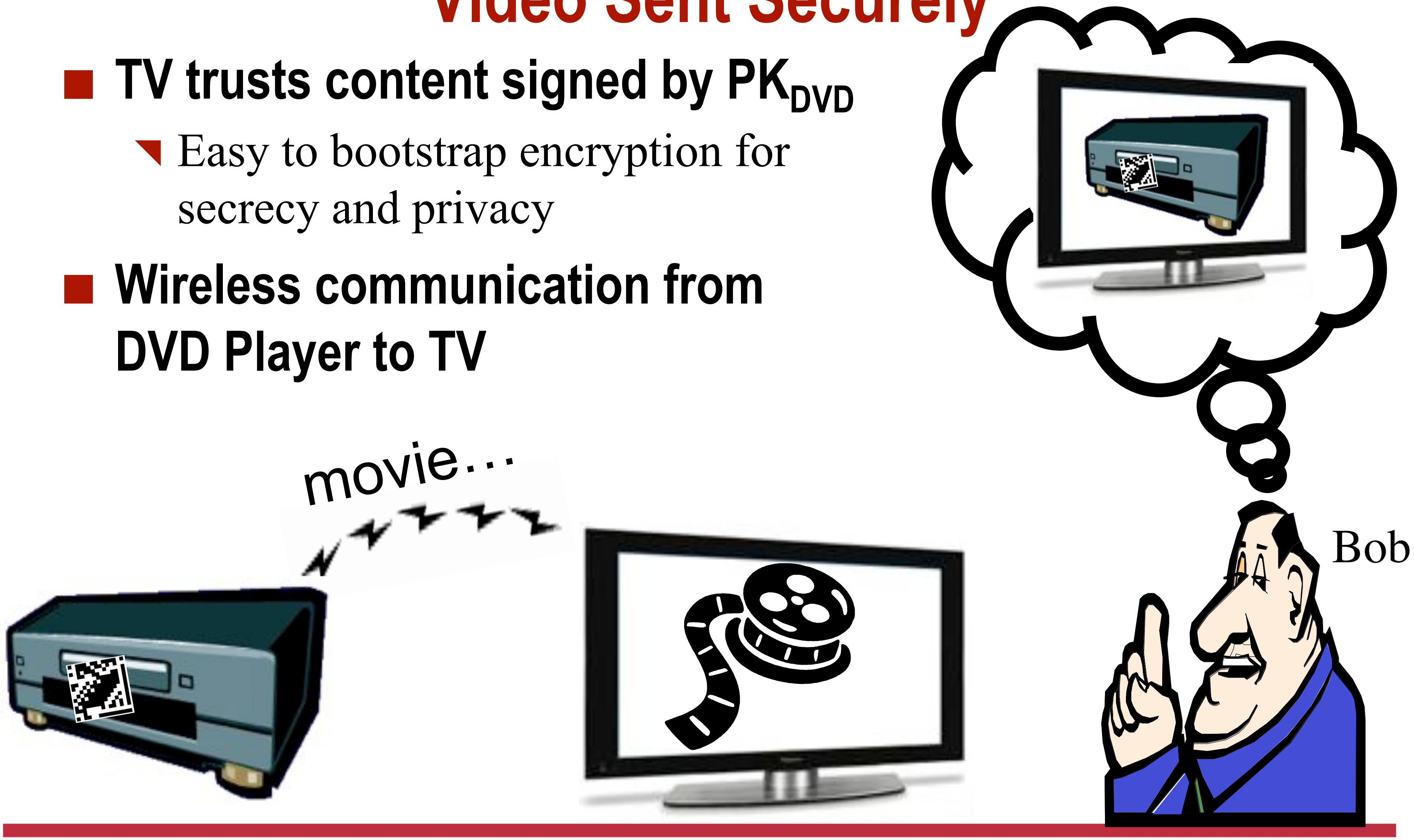
$\xrightarrow{PK_{DVD}, t}$

$t' \leftarrow \mathrm{HMAC}_{\mathrm{K}_{\mathrm{TV}}}(PK_{DVD})$

$if\,(t' \neq t) : abort$

Video Sent Securely

- **TV trusts content signed by PK$_{DVD}$**
  - Easy to bootstrap encryption for secrecy and privacy
- **Wireless communication from DVD Player to TV**



TCG Introduction

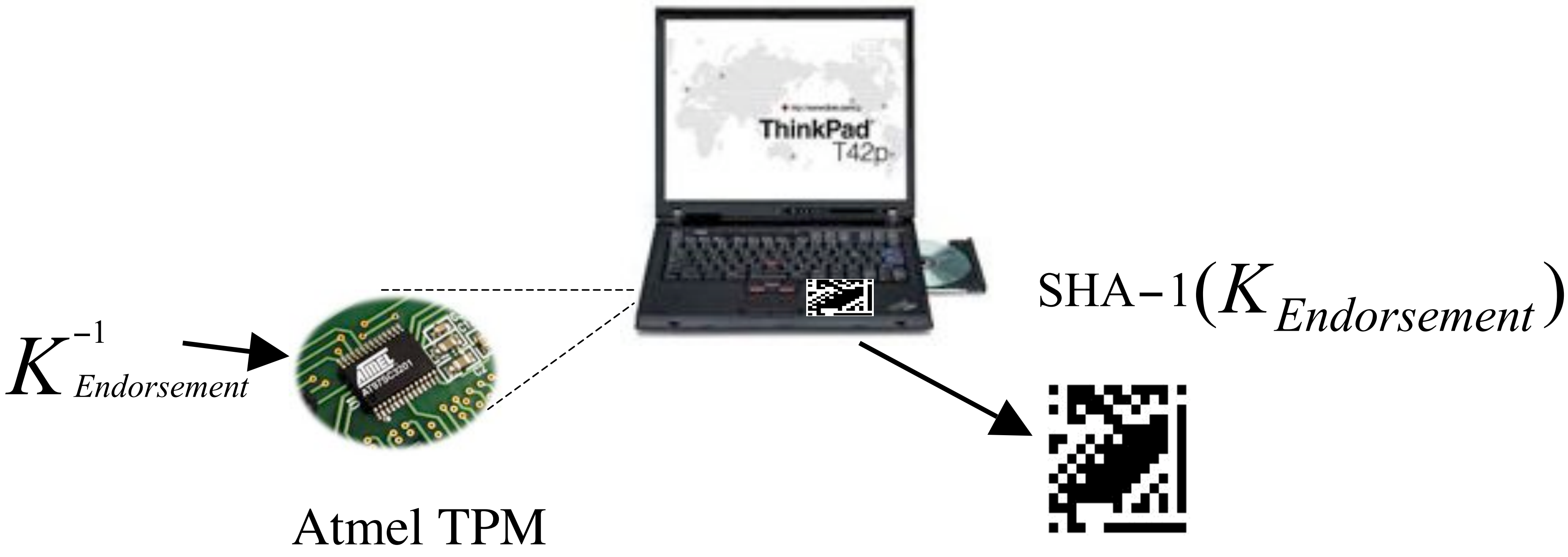
- **Trusted Computing Group (TCG)**
  - Formerly Trusted Computing Platform Alliance (TCPA)
- **Develops and promotes open specifications**
  - Trusted Platform Module (TPM)
  - Passive component with secure storage and ability to perform RSA private-key operations on-chip
  - There’s one in this laptop
  - Lots more… beyond the scope of this presentation

Trusted Path to TPM - Motivation

- **Do not want to trust window manager to deliver password**
  - Cluttered desktops can be confusing
  - Designed for functionality, not security
  - Eavesdropping is easy
- **Taking "ownership" of a TPM is a particularly sensitive operation**
  - User must input Owner Authorization Data (OAD)
- **Endorsement keypair**
  - For encrypting secrets to TPM
  - Private key never leaves TPM

Encrypt OAD with $K_{Endorsement}$

- Commitment to $K_{Endorsement}$ on computer's housing

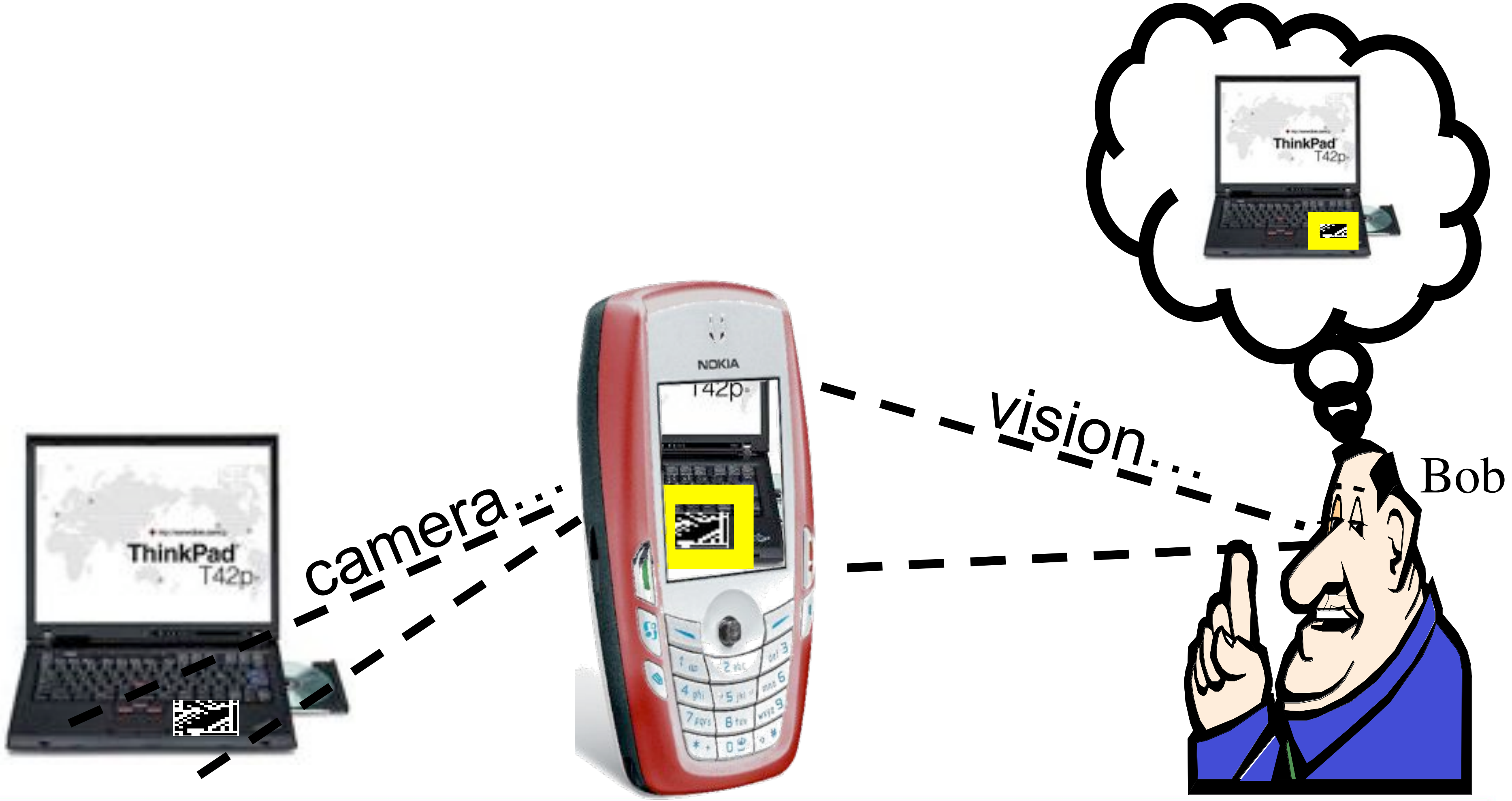


$K^{-1}_{Endorsement}$

Atmel TPM

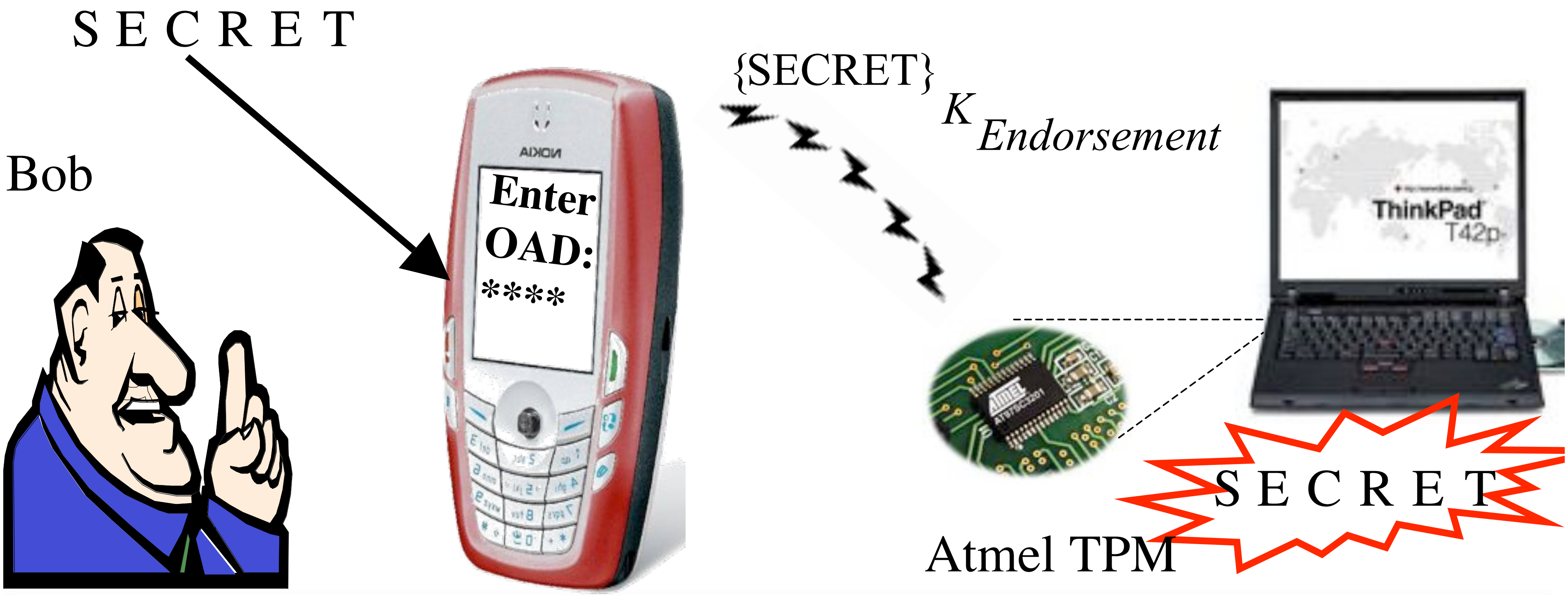
$\text{SHA-1}(K_{Endorsement})$

Authenticating $K_{\text{Endorsement}}$



Entering the OAD

- Bob enters his secret (the OAD) into his phone
- Encrypt with $K_{Endorsement}$ and send to TPM



SECRET

Bob

Enter OAD: ****

$\{SECRET\}_{K_{Endorsement}}$

SECRET

Atmel TPM

Display Ownership Challenge for Applications

- **TPM-equipped computers can perform** *integrity measurements*
- **Mobile phone can challenge application to access a private RSA key which is bound to a particular platform configuration**
  - Encrypt a nonce under the corresponding public key
  - Many additional details involved in real deployment

Display Ownership

Phone

has K_{Laptop}

gen. $nonce$

$\xrightarrow[wireless]{}$

Laptop

$\{K_{Laptop}, K^{-1}_{Laptop}\}$ **sealed**

$nonce$

Attempt to load K^{-1}_{Laptop}

$s = Sign(K^{-1}_{Laptop}, nonce)$

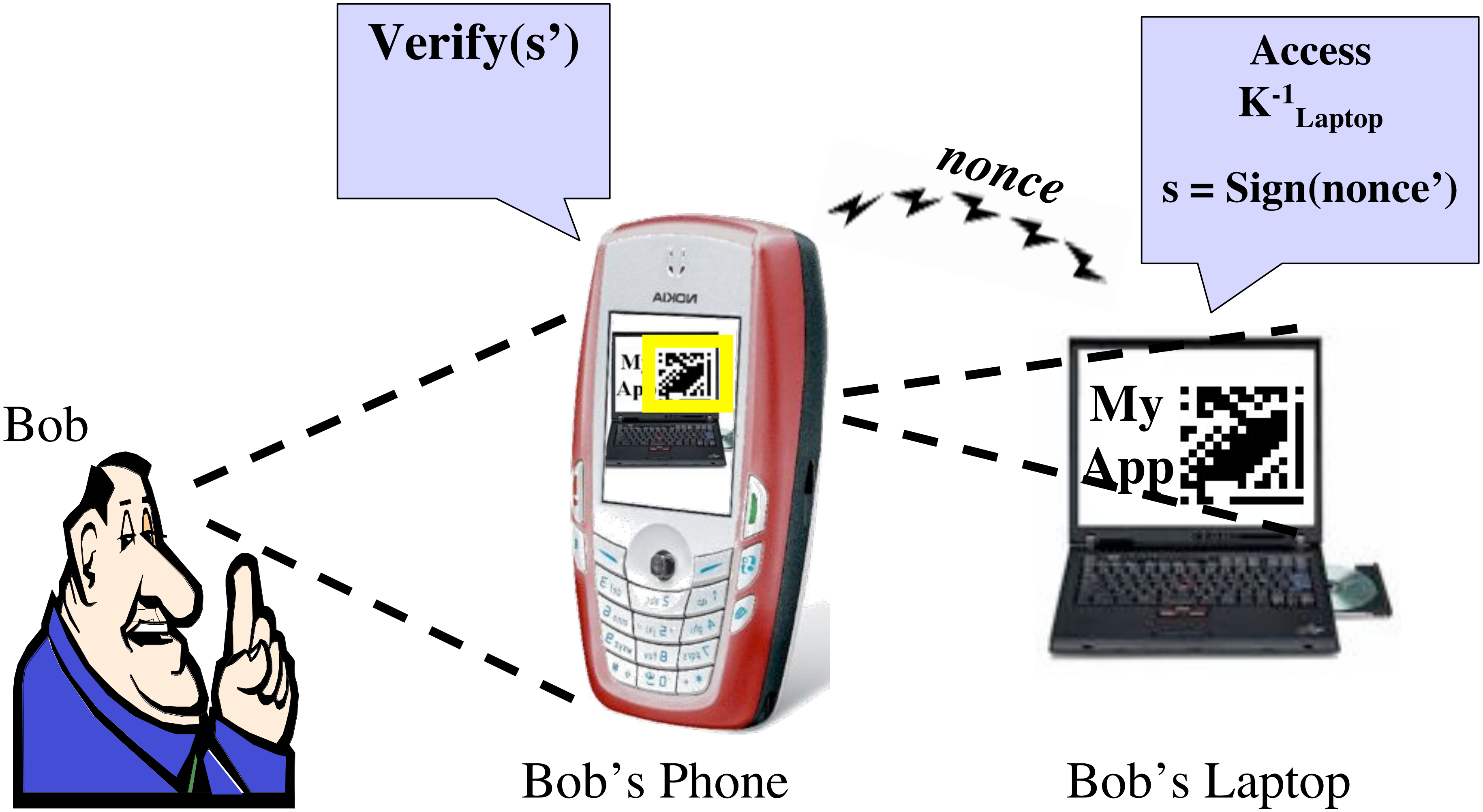
$Encode(s)$

$\xleftarrow[visual]{}$

s'

$\text{Verify}_{K_{Laptop}}(s')$

Display Ownership



Verify(s’)

nonce

Access
K^{-1}_{Laptop}

s = Sign(nonce’)

Bob

Bob’s Phone

Bob’s Laptop

Display Ownership Challenge for Applications

Provides an instantaneous guarantee only

- Imperfect, but raises the bar for attackers
- Valuable first step

Implementation Details

- **Initial prototype written in C++ for Symbian OS**
  - Fast enough to process ~6 barcodes / second
- **Now implemented in J2ME:**
  - Cross platform
    - BouncyCastle for crypto
    - JScience MathFP for floating point ops
    - Barcode format and recognition algorithm derived from Rohs & Gfeller's *VisualCodes*
    - Requires ~2 seconds to process a barcode

Advantages of SiB

- Millions of devices already deployed that can run SiB
- Easy, fast, intuitive authentication of devices is possible
- Enables the security of public key protocols without dependence on a PKI

Prior Work Comparison

- **Desirable properties**
  - Available in commodity devices vs.
  - Provides demonstrative identification

	Resurrecting Duckling	Talking to Strangers	Seeing is Believing
Demonstrative Identification	Strongest	Strong	Stronger
Commodity	No	Some	Yes

- **SiB can achieve both!**

Conclusions

- **Issues for key establishment in ad hoc networks**
  - Security
  - Usability
  - Transparency to the user
- **Totally transparent is undesirable**
- **Involve the user, but in a way that is intuitive**
- **Taking pictures of desired communication endpoints is one way to achieve this property**

Thank You!

- Questions?
- jonmccune@cmu.edu