MIT PROJECT OXYGEN
PERVASIVE, HUMAN-CENTERED COMPUTING

The Untrusted Computer Problem and Camera-Based Authentication

Dwaine Clarke, Blaise Gassend, Thomas Kotwal,
Matt Burnside, Marten van Dijk, Srinivas Devadas, Ronald Rivest

LCS

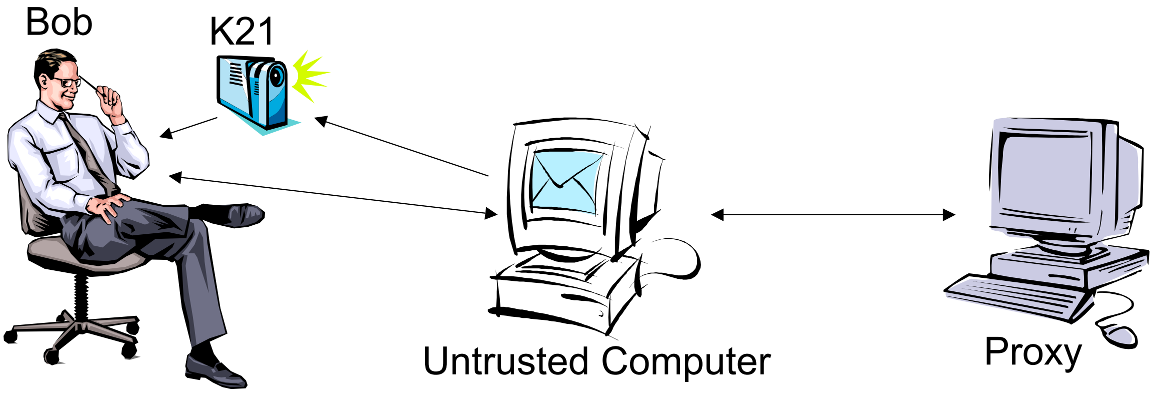
lab
@ MIT

MIT PROJECT OXYGEN
PERVASIVE, HUMAN-CENTERED COMPUTING

Overview

1. Problem
2. Camera Augmented K21
3. Reducing the problem …
4. Pixel Mapping
5. Optical Character Recognition

Problem: Bi-directional Authentication



- Bob is using an untrustworthy computer.
- He wishes to communicate with his proxy.
- He can trust what he sees on the screen, because his camera augmented K21 is monitoring the screen content.
- Why not use SSL?

The Camera Augmented K21

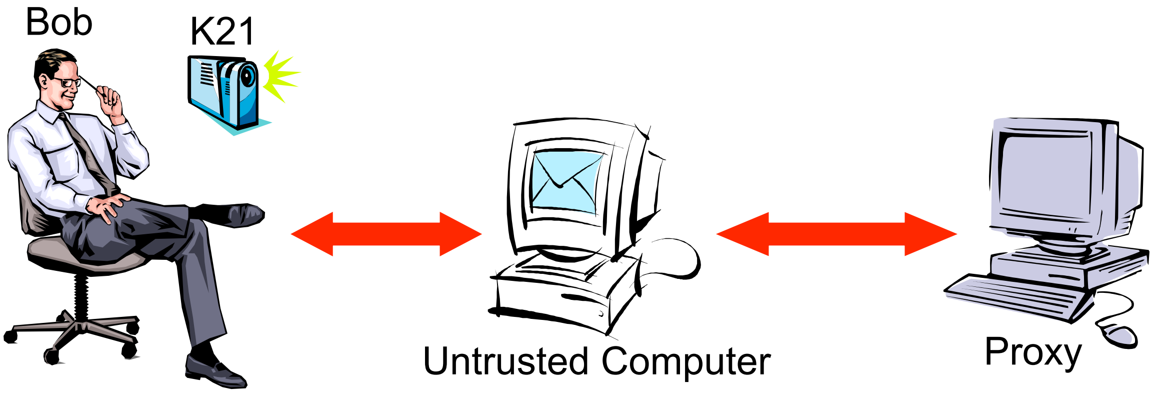
Pixel Mapping Approach

- A digital camera.
- Status indicator lights. (red, green)
- A small numerical LCD display.
- Symmetric keys shared with the proxy.

OCR Approach also has

- control buttons
  1. capture image
  2. send image to proxy
- IR link to untrusted computer

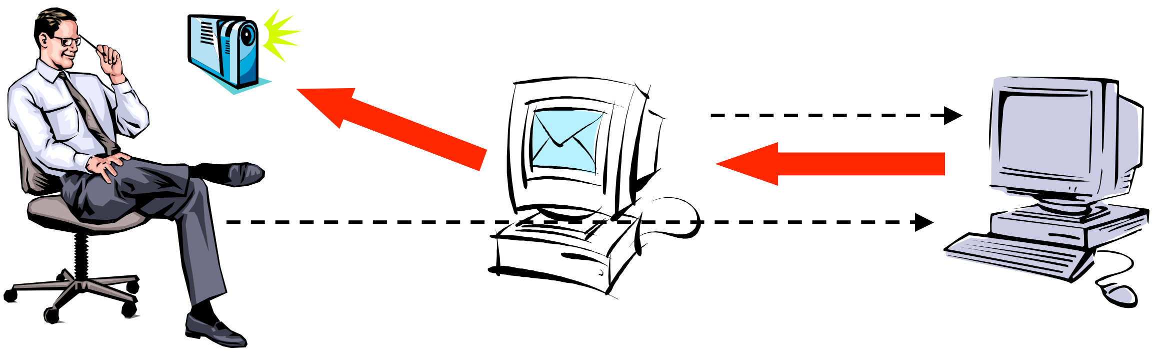
Reducing the Problem …



We would like:

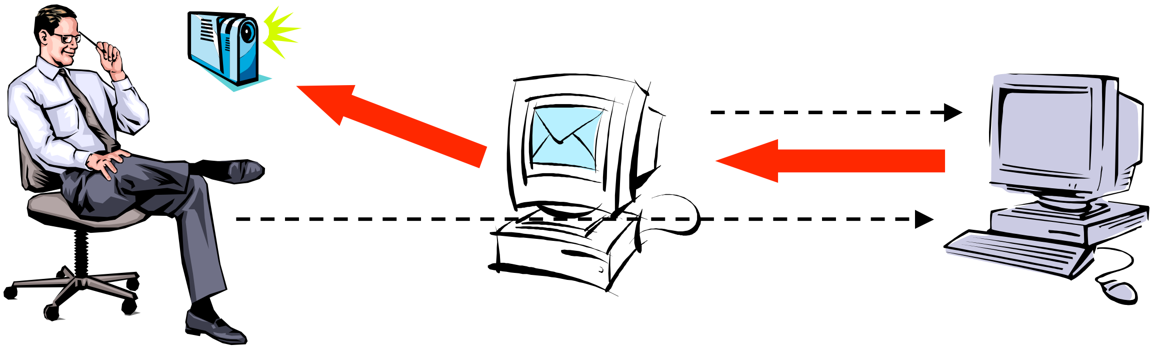
- **Downwards Authentication: Bob to receive authentic messages from his proxy**
- **Upwards Authentication: Bob’s proxy to receive authentic messages from him**

But if we have:



- **Upwards Transmission: Bob sends a message to proxy from untrusted computer**
- **Downwards Authentication**
- **Secure Approval: Bob can securely inform proxy that he approves a specific authenticated message from proxy**

Upwards Authentication

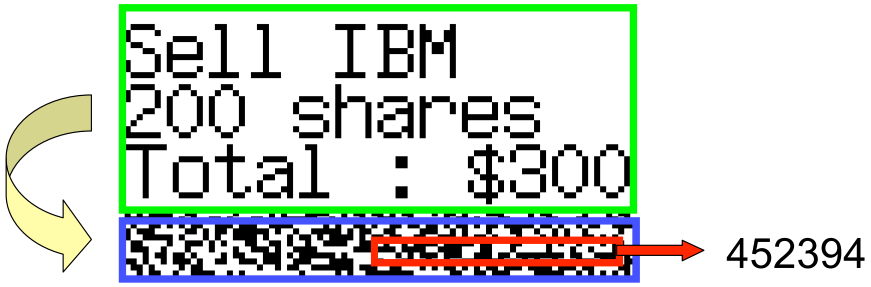


- Bob sends a message to proxy using untrusted computer (Upwards Transmission)
- Proxy receives message’, message’ might be different from message if untrusted computer/network was unfaithful.
- Proxy does authentic transmission of message’ to Bob (Downwards Authentication)
- Bob securely approves message’ if message’ == message, and if Bob did send message to proxy. (Secure Approval)

Pixel Mapping Approach (Blaise Gassend)

- Each message from Proxy is accompanied with raw data that is used to authenticate the message
- K21 monitors screen and uses camera to reconstruct the contents of the untrusted computer’s screen; K21 verifies the authenticity of the displayed information.

Message



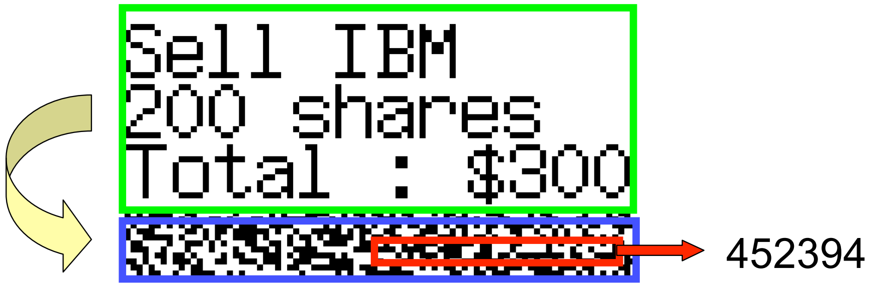
Each transmission from the proxy has:

- A nonce
- A MAC on the message and nonce

When the user must confirm a decision (in Secure Approval), the transmission from the proxy also contains:

- An encrypted one-time password

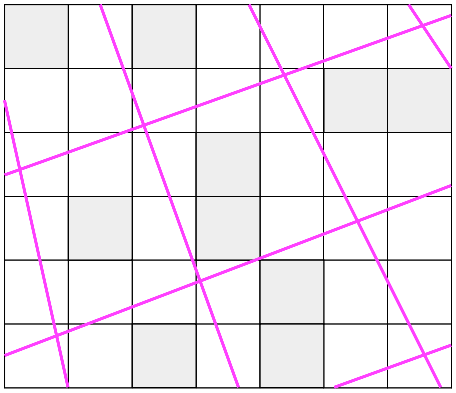
Message contd.



- The K21 monitors screen and reconstructs the contents of the screen
- Only the K21 with the correct key can:
  - Verify the MAC on the message
  - Decrypt the one-time password
- The K21 provides the decrypted one-time password to Bob to use for Secure Approval

The Pixel Mapping Idea

- Screen content is displayed in black and white.
- Each screen pixel is seen by at least one significant camera pixel.
- Screen pixels must be large compared to camera pixels.

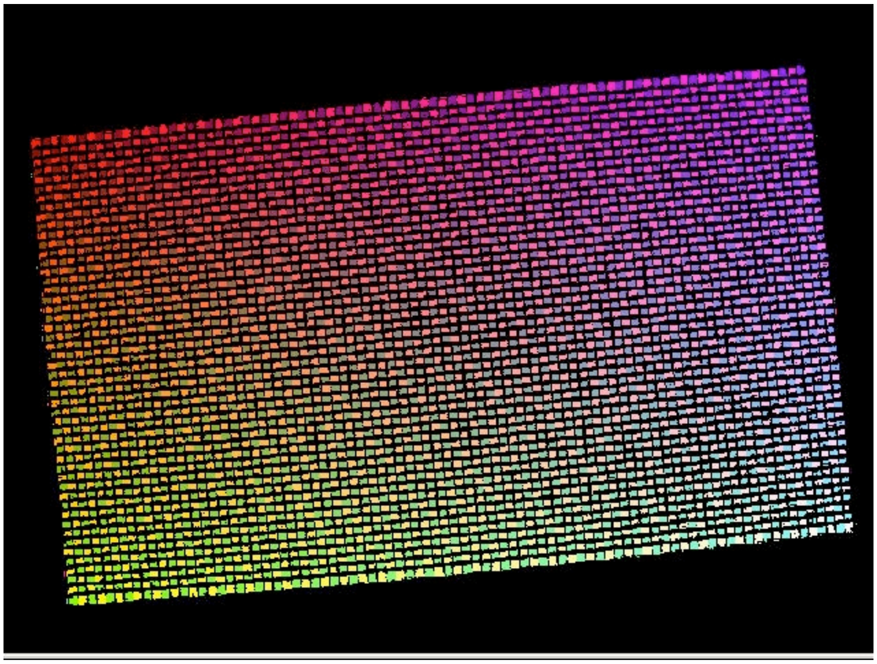


□ Camera pixel

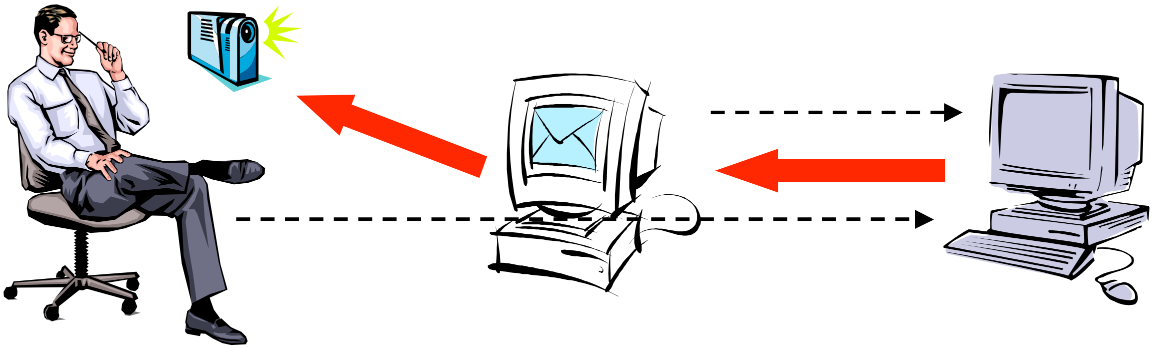
◇ Screen pixel

▨ Significant camera pixel

Successful Calibration



Pixel Mapping: Protocol



- Upwards Transmission: Bob sends message to proxy
- Downwards Authentication:
  - Proxy sends (message, encrypted nonce, encrypted OTP, MAC)
  - K21 exactly reconstructs screen
  - K21 checks nonce and MAC. If checks pass, K21 lights green light, and displays one-time password on a small LCD display.
- Secure Approval: Bob sends one-time password to proxy

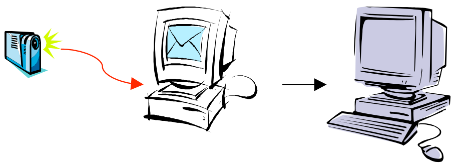
OCR Approach (Thomas Kotwal)

- **K21 has**
  - control buttons (for Secure Approval)
    1. capture image
    2. send approval to proxy
  - IR link to untrusted computer

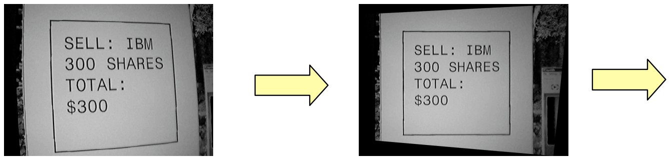
- **The computation of verifying the proxy's message is moved back onto the proxy, instead of doing it on the K21.**

Downwards Authentication

1. Proxy sends message, in form of an image, to untrusted computer.
2. K21 takes a picture; K21 uses its IR link to send ("verify", picture, encrypted nonce, MAC) to the proxy via untrusted computer.



3. Proxy corrects for image distortion and performs OCR. Proxy checks nonce, MAC, and that result of OCR is the same as message in 1.



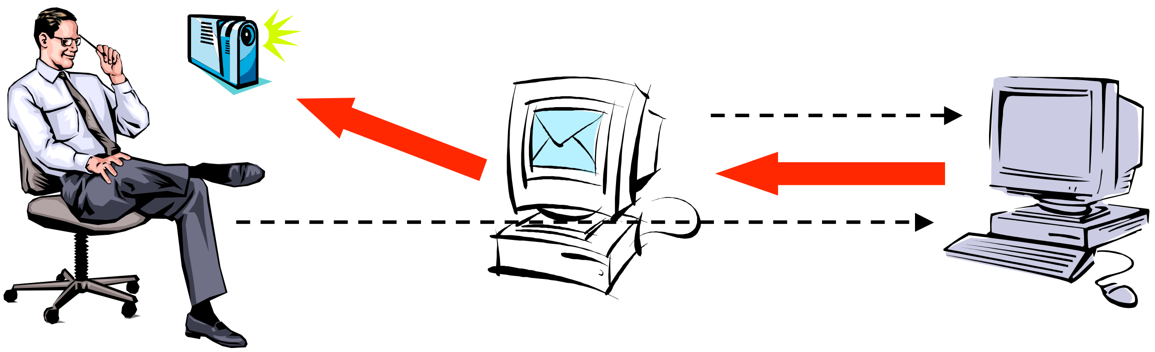
SELL: IBM
300 SHARES
TOTAL:
$300

SELL: IBM
300 SHARES
TOTAL:
$300

```
SELL: IBM
300 SHARES
TOTAL:
$300
```

4. Proxy sends a confirmation ('yes' / 'no', encrypted nonce, MAC) back to the K21. If 'yes' and MAC and nonce verify, K21 lights green light.

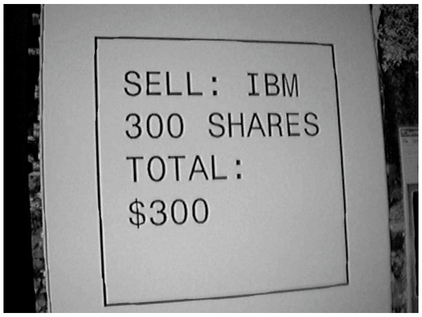
OCR: Protocol



- **Upwards Transmission: Bob sends message to proxy**
- **Downwards Authentication**
- **Secure Approval:**
  - **Bob presses 'capture' button on K21, K21 takes a picture**
  - **Bob presses 'send' button on K21, K21 uses its IR link to send ("accept", picture, encrypted nonce, MAC) to the proxy via untrusted computer.**
  - **Proxy checks nonce, MAC, result of OCR is the same as message in upwards transmission. Only Bob's K21 can create appropriate MAC.**

Image Verification Problem

Is this…



SELL: IBM
300 SHARES
TOTAL:
$300

…the same as this?

```
SELL: IBM
300 SHARES
TOTAL:
$300
```

Obstacles:

- Linear and non-linear distortions
- Decreased resolution
- Noise

Steps to solution:

- Undo distortions
- Compare content

Step 1: Undo Image Distortion

a) Undo lens distortion

- Model as radially symmetric quadratic distortion
- Non-linear transformation

b) Undo linear distortions

- Corrects for affine (scaling, rotation, translation) and perspective distortion (picture at non-perpendicular angle relative to screen)
- Requires four known points in distorted image

c) Undo other non-linear distortions

- Corrects for curvature of screen, etc.
- May not be necessary

Step 2: Compare Content

- **Assume content is text only**
- **Perform OCR on processed image**
  - Advantage: proxy knows what the text should say
  - To save computation time compare each character with what it should be, not every possible character
  - Constrain font to facilitate OCR routine

Comparison of OCR vs. Pixel Mapping

- **OCR Advantages**
  - **Proxy knows what the screen should display so OCR can be optimized**
  - **No image processing on the K21**
  - **No calibration necessary**
  - **Camera does not have to be immobile during session**
  - **User does not have to type a one-time password**
- **Pixel Mapping Advantages**
  - **Does not require IR link between K21 and untrustworthy computer**
  - **Shorter verification time (network latency, computation time)**
  - **Can do graphics**