Secure Real World Interaction Using Mobile Devices

William Claycomb and Dongwan Shin

New Mexico Institute of Mining and Technology

May 7, 2006

Agenda

- Motivation and Background
- Security Service Model
- Security Service Scenarios
- Analysis
- Summary
- Questions

Motivation

- The use of mobile devices in pervasive computing environments is growing
  - The types of interactions available are also increasing
- The security of these interactions needs to be addressed
  - Particularly in one-to-one situations
  - Between a mobile device and a service point

Motivation

- Secure interaction needs to be intuitive and easy to use
  - Simple enough for the basic user to understand
  - Applicable to a wide variety of applications and service points
  - Lightweight. This needs to be available for the smart phone as well as the laptop.

Background

- Authentication and Key Exchange
  - Devices need to authenticate for key exchange to occur
  - “Resurrecting Duckling”
  - Location limited channels

Background

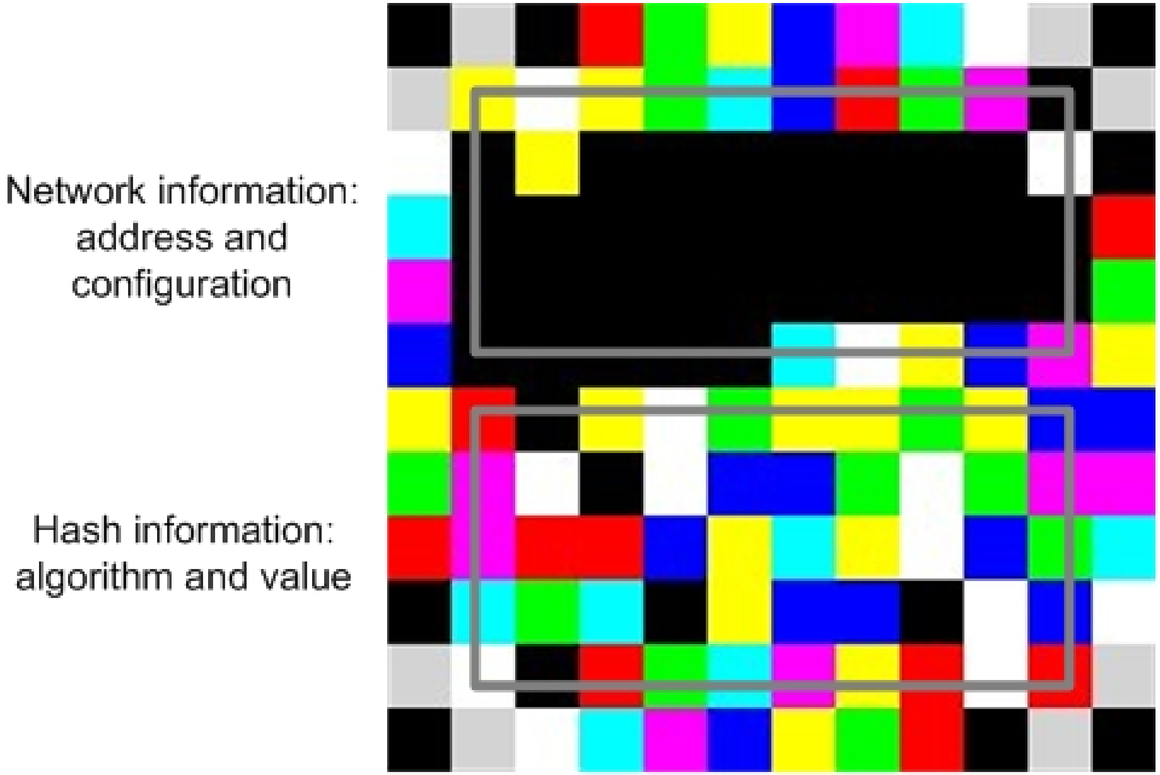
- Using Digital Cameras
  - Visual tags
    - Capture an image of a tag and decode information contained within
  - Establishing a communication channel
    - Demonstrative identification

Background

- Using Visual Tags for Authentication and Key Exchange
  - UbiCode
  - UbiColor
- Mobile Interaction Framework

UbiColor

- A Visual Tag



Network information: address and configuration

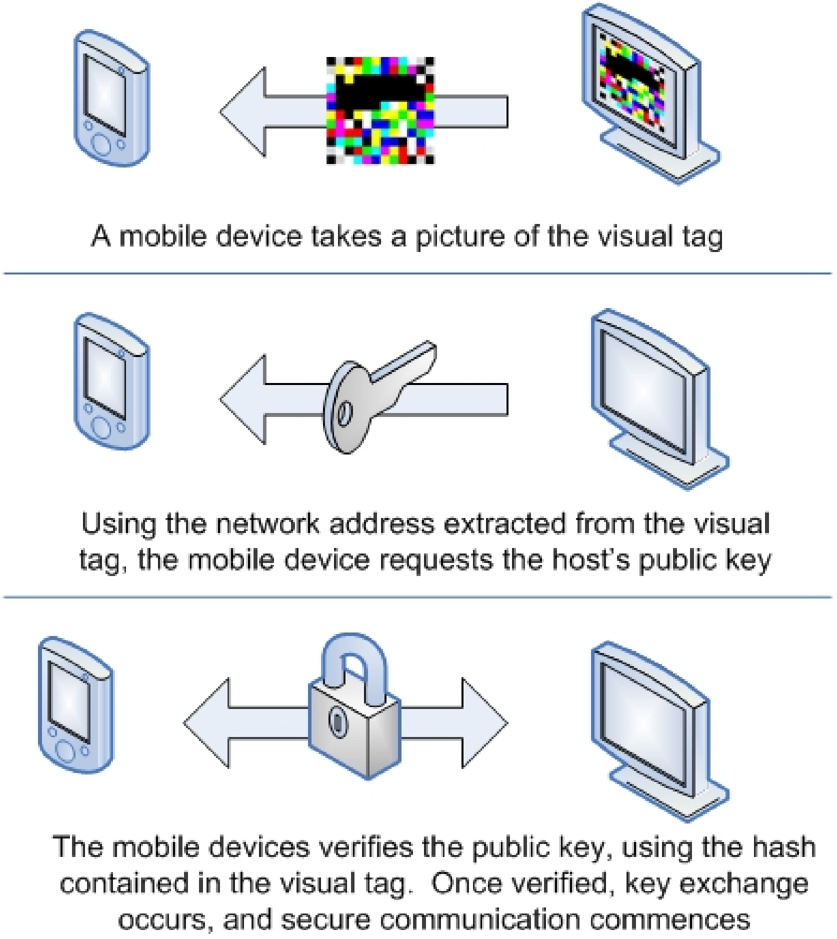
Hash information: algorithm and value

Security Service Model

- Establishing the secure connection
- Using the secure connection

Establishing a Secure Connection

- UbiColor



A mobile device takes a picture of the visual tag

Using the network address extracted from the visual tag, the mobile device requests the host's public key

The mobile devices verifies the public key, using the hash contained in the visual tag. Once verified, key exchange occurs, and secure communication commences

Using the Secure Connection

- Interacting with a service-providing device
  - Not human-to-human communication
  - Must be somewhat automated
  - Require a secure connection

Security Service Scenario

- ATM
  - Capture visual tag image from ATM
  - Establish secure connection
  - Authenticate user
    - Several storage methods for this
  - Interact with ATM via mobile device
  - ATM responds when appropriate

Security Service Scenario

- ATM (cont)
  - – Advantages
    - Less physical use of service device
    - More options for physically locating the device
    - Personalization is possible
    - Additional physical security
    - No need for ATM card
    - Protection from “skimming”
    - Additional interface capabilities (account information, funds transfer, etc.)
    - Standardized interaction
    - Privacy and protection from onlookers

Security Service Scenario

- Vending Machine
  - Capture image of visual tag from vending machine
  - Establish secure connection
  - Interact with vending machine
    - Receive product information
    - Make purchases using digital cash, credit card, store credit, etc.

Security Service Scenario

- Vending Machine
  - – Advantages
    - Detailed product information may be obtained
    - Product selection can be externally controlled
    - Payment information can be stored on the device, but that is not required
    - Electronic receipts

Analysis

- This model provides a secure communication channel
  - Particularly useful for sensitive transactions
- Easily adaptable to various networking environments
- Adaptable to various computing platforms
- Does not require presence of CA
- External connection not required, unless further user authentication is necessary
- This model does not require the use of device discovery protocols

Analysis

- Security
  - – Man-in-the-middle attack prevented
  - – Misidentification of tag information is not a threat
    - The incorrectly identified host will not have the correct public key
  - – Keys change with every instance of communication
  - – The of pre-printed, superimposed visual tags for and attack is possible, but not likely

Summary

- Security Service Model
  - Establish secure connection
    - Use a method that requires demonstrative identification to eliminate the need for external connections
  - Using the secure connection
    - Examples: ATM and Vending Machine
  - Analysis
    - Several security issues are addressed by this model

Questions