High Entropy Visual Identification for Touch Screen Devices

Nathaniel Wesley Filardo and Giuseppe Ateniese

April 10, 2012

What are we trying to do?

- Entering(?) an era of ubiquitous computing.
- Computers getting smaller, more powerful, more connected…

What are we trying to do?

- Entering(?) an era of ubiquitous computing.
- Computers getting smaller, more powerful, more connected…
  - Supercomputers in your pocket
  - (Almost) Always on and always at hand

What are we trying to do?

- Entering(?) an era of ubiquitous computing.
- Computers getting smaller, more powerful, more connected. . .
  - Supercomputers in your pocket
  - (Almost) Always on and always at hand
- More *integral to daily life*:
  - Facilitate communication
  - Manage money
  - Play games
  - . . .

What are we trying to do?

- Entering(?) an era of ubiquitous computing.
- Computers getting smaller, more powerful, more connected…
    - Supercomputers in your pocket
    - (Almost) Always on and always at hand
- More *integral to daily life*:
    - Facilitate communication
    - Manage money
    - Play games
    - …
- We want to do these things *securely*.

What are we trying to do? – Security?

- "Secure" might mean many things. Here, a very modest version:

  > *Some requested actions should require that the user give a* not-trivially-forged *indication of explicit consent.*

  For example:

  - Sign a document
  - (Decrypt and) display sensitive information

What are we trying to do? – Security?

- “Secure” might mean many things. Here, a very modest version:

  > *Some requested actions should require that the user give a* not-trivially-forged *indication of explicit consent.*

  For example:

  - Sign a document
  - (Decrypt and) display sensitive information
- This is a really hard problem and we’re not going to solve it fully in this talk. (sorry!)

What are we trying to do? – Security?

- "Secure" might mean many things. Here, a very modest version:

  > *Some requested actions should require that the user give a* not-trivially-forged *indication of explicit consent.*

  For example:

  - Sign a document
  - (Decrypt and) display sensitive information
- This is a really hard problem and we're not going to solve it fully in this talk. (sorry!)
- Traditionally, this means "ask the user for a password"

What are we trying to do? – Passwords

- Entropic yet reproducable.
  - Ideally, many bits of entropy.
  - Usually reproduced exactly.

What are we trying to do? – Passwords

- Entropic yet reproducable.
  - Ideally, many bits of entropy.
  - Usually reproduced exactly.
- Easy way to reproduce: memorize!

What are we trying to do? – Passwords

- Entropic yet reproducable.
  - Ideally, many bits of entropy.
  - Usually reproduced exactly.
- Easy way to reproduce: memorize! Challenge:
  - Too many to easily remember
  - (So use fewer?)
  - Infrequently used and so forgotten
- But also. . .

What are we trying to do?
Passwords and Small Computers

- Small computers do away with traditional, big things.
  - Like big keyboards with large key travel.
- Good passwords *now even more annoying*.
  - Modal keyboards (upper-case, numbers, symbols)

The Password Game

Formal system game is straightforward: Generator, user, verifier
U makes up a slide and images, shares with G
G makes a challenge, shares with U G sends encrypted message to V
U reveals answer to V V verifies that answer decrypts G's message

The Password Game

What did we actually do? Modification of formal game for OISafe

The Password Game – Threat Model

In order for this to be a difficult game, we need to make some assumptions on the adversary:

- Imperfect surveillance.
- No software compromise when secrets are on the device.

Our System

What do we want?

Our System

What do we want?

- More entropy!

Our System

What do we want?

- More entropy!
- Users should not have to memorize more

Our System

What do we want?

- More entropy!
- Users should not have to memorize more
- No specialized hardware.
  - No biometrics, cameras, . . .
  - Just a display with moderate resolution and (ideally) touch-sensitivity.

Our System

How do we get what we want?

- Use *visual secret splitting*

Our System

How do we get what we want?

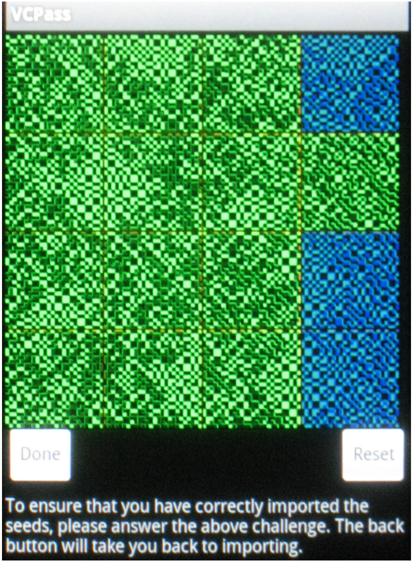
- Use *visual secret splitting*
- *Challenge* the user to prove possession of secret share.
  - amounts to proving the presence of a piece of plastic.
  - (Relatively easy for (able) humans)

Our System
Basic Visual Cryptography Secret Splitting

2x2 information-theoretically secure scheme

What does it look like? Slide, challenge, phone+slide.

What does our system look like? – Answering a Challenge



To ensure that you have correctly imported the seeds, please answer the above challenge. The back button will take you back to importing.

- Encodes the string `NDNDLRUNUNNRNLLR`.

We're not the first to think of this!

Notably, Naor and Pinkas in early work on VC proposed:

Device selects a number of rectangles of the screen, asks the user about the colors of each on a slide.

Works, but 1) more easily copied from afar 2) needs more stuff on the display than we do, making it likely slower to use (?)

Our scheme is cute but hard to actually produce