Vanquishing Voyeurs: Secure Ways to Authenticate Insecurely

Andrea Bianchi & Zoz
Overview

- Password/PIN Features & Observation Attacks
- Observation from Without
  - Physical Key Entry at Insecure Terminal
  - Mechanical Observation-Resistant Solutions
- Observation from Within
  - Key Protection between Insecure Input Device and Network
  - Recorder/Logger Subversion
- Rethinking Password Entry Mechanics
  - Remote Entry with Secure Transmission to Terminal
  - Utilization of Common Mobile Digital Devices
AUTHENTICATION METHODS

**Password**
- alphanumerical
- graphical
- haptic

**Token**
- keys
- RFID security cards

**Biometric**
- fingerprints
- retina scanner
- voice
- vein scanners
## NEED FOR PASSWORDS

<table>
<thead>
<tr>
<th></th>
<th>PASSWORDS</th>
<th>TOKENS</th>
<th>BIOMETRICS</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>-</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>-</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Common Delegation</th>
<th>Observation</th>
<th>Common Delegation</th>
<th>Physical Property</th>
<th>No cognitive load</th>
<th>Physical Property: can be observed, copied, deteriorated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Passwords</td>
<td>Cheap</td>
<td>Memory (scaling, cognitive load)</td>
<td>Cheap</td>
<td>Can be stolen, lost, copied, deteriorated</td>
<td>Can be easily accepted by people [Coventry 2003]</td>
<td>Technology not ready yet</td>
</tr>
<tr>
<td>Tokens</td>
<td>Invisible information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Biometrics</td>
<td></td>
<td></td>
<td></td>
<td>No delegation</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Philosophical issues concerning identification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>


NEED FOR PASSWORDS

INVISIBLE INFORMATION + DELEGATION

HIGH COGNITIVE LOAD
Passwords are still valuable compared to other options, and this is why they are the most common in security systems. However their cognitive load is ultimately caused by their weakness against observation.

**Passwords are subjected to observation**

- need to have many passwords and change them frequently
- high cognitive load
## Observation Attacks

### Human Interface
- **External**
  - Shoulder Surfing
  - Mirrors/Cameras
  - Keypad Dusting

- **Internal**
  - ATM Skimmers
  - Keyloggers

### Network
- Sniffing
- MITM

### Secure Private Interface

**What about when we have to use public terminals?**
PUBLIC TERMINALS

ATMs
Airport kiosks
Door locks
Public computers
Access control
PIN ENTRY TERMINALS

What about bank ATM (Automatic Teller Machine) terminals?

Once upon a time...

... there was only the human bank teller
PIN ENTRY TERMINALS

What about bank ATM terminals?

The human bank teller

1967: The 'Barclaycash' cash dispenser (1st cash dispenser, Barclays Bank)
PIN ENTRY TERMINALS

The terminal was public to grant access 24 hours a day.

1973 - The future tellers.

TOTAL TELLER
Handles all of your standard Ready-Reserve checking and instant interest savings transactions including deposits, withdrawals, transfers and installment loan and mortgage payments. You need your instant cash card to operate.

TV INFORMATION CONSOLE
Watch and listen to find out how to get an instant cash card -- or about other bank services.

AUTOMATIC POSTAL CENTER
Weigh packages, get stamps, envelopes, postcards and zip code information day and night.

TELEVISION TELLERS
Do your banking by television. 7:00 AM - 6:30 PM: Mondays. 7:00 AM - 6:00 PM: Tues. - Fri.

PICTUREPHONE INFORMATION SERVICE
Information on all bank services and directions to various bank departments. 8:30 AM - 4:00 PM - Mon. - Fri.

Wells Fargo Archives
PIN ENTRY TERMINALS

The terminal was public to grant access 24 hours a day and even remotely!

Key features of the bank of the future are the Total Teller, remote television tellers, a Picturephone and a self-service postal unit.

The future tellers (1973) and PAT (2010)
Interaction history
In the past 40 years, the ATM terminals substantially **did not change**. The interaction with the terminals did not change as well.

**Observation** is still one of the most common **attacks**!
SIMILAR INTERFACES

IDEO for BBVA
THE INTERACTION

Ideo for BBVA

=

ATM in 1973
The interaction is **physically situated**

**hence easily attackable** (i.e. shoulder surfing and camera attack)
PUBLIC THREAT

1. Public terminals **dangerous** (DeLuca 2010 and Gizmodo)

---

**card ‘skim’ scheme**

ATM cardholders have been warned for years about the dangers of card skimmers. The technology is now so compact that many consumers might not notice it. Here are some elements of a typical skimming operation.

1. Keypad overlays capture PIN numbers on a magnetic chip.
2. Hidden cameras can also copy customers’ PIN numbers.

**Skimming a terminal**
1. Public terminals **dangerous**

*Camera, Observation, Tamper*
Different people want different password schemes or input methods.

- PIN Entry by trapdoor game (Roth et al.)
- Spy-resistant Keyboard (Tan et al.)
- Gaze-Based Password (Kumar et al.)
- Haptic Passwords by Malek and Sasamoto
PINS IN THE REAL WORLD

Despite all these new methods we still rely on keypads!
BASIC CONSIDERATIONS

We need to access public terminals, **but** it does not mean that

- the interaction **must be the same for all of us**
- the interaction **must be limited to the default interface**
- and the interaction **must be done at the terminal**

- **DIFFERENT PASSWORDS FOR DIFFERENT PEOPLE AND DIFFERENT SITUATIONS**
- **ONLINE INTERFACE SECURITY IS ONLY A MINIMUM STANDARD**
- **INTERACTING AT THE TERMINAL IS DANGEROUS**
STRATEGY SHIFT

Before

After

PIN

CHOICE

MEDIATED INPUT

Private Device or Software
An alternative strategy is to **decouple** interaction in two parts:

- we separate the **input** method for a PIN from the **communication** of the password to a terminal.
PART I
THE ENEMY WITHOUT:
PROTECTED PHYSICAL KEY ENTRY METHODS
FOR UNTRUSTED ENVIRONMENTS

CHOICE

CHOICE
The Secure Haptic Keypad
A Tactile Password System

The Problem: Observation Attack

Authentication in public spaces is common
ATMs, entry door systems, quick flight check-in kiosks, etc...

Stolen PINs pose a significant risk to many systems
U.S. estimated yearly bank fraud amount s $60M

Observation attack: “Shoulder-surfing” or “Camera-attack”
Related Work

1. Visual Obfuscation
2. Eye Tracking
3. Personal Interfaces
Multimodal systems: password information (i.e. textual and graphical passwords) can be obfuscated using haptics, as an invisible channel.

Relies on a cognitive transformation/mapping.

Haptic-based Graphical Password (*Malek et al.*)

Undercover (*Sasamoto et al.*)
The idea: Haptic Password

A sequence of **tactile cues** (tactons), inherently **invisible** to everyone.
Password Model

Passwords in the system take the form of a sequence of tactile feedback in the forms of vibrations (from a set of 3 possibilities)

Our 3 Tactons

Continuous

1 Hz

2 Hz

Example of Haptic Password made of 3 tactons
Keypad constructed of three physically independent buttons each capable of (1) sensing finger input and (2) rendering vibrotactile cues in the form of tactons and (3) accepting input selection.
Haptic Keys

Three *identical* hardware:

1. *force sensing resistor* (FSR) adjust the strength of the vibrotactile output
2. *linear coil vibrotactile actuators* within the casing
3. *physical switches* for key selection
The Password Software

1. AVR micro-controller handles sensing, rendering and input.
2. The Haptic Keypad is connected to a computer via serial port.
3. Minimal GUI represents only completion progress
Interaction Model

Rules:
3 tactons are **assigned** to 3 keys (1<->1 correspondence)
Tactons are **randomized** on keys after each entry.

**System Randomize key-tacton assignment**

**User feels the keys and finds the only right tacton**

**User selects the tacton clicking the key**

Match **input** with **password**
Example of Interaction

System Randomize

User feels the keys

User selects

Password To match

With no interaction, keys are silent
Example of Interaction

System Randomize

User feels the keys

User selects

Password To match

Press the FSRs to “feel” the tactons
Example of Interaction

The "strength" of the tacton depends on the pressure applied.
Example of Interaction

System Randomize

User feels the keys

User selects

Password To match

Click the button to apply selection
Example of Interaction

System Randomize

User feels the keys

User selects

Password To match

The tactons are randomly re-assigned to the keys
Example of Interaction

System Randomize

User feels the keys

User selects

System

Password To match

Next Input

Keep going on until done.
Example of Interaction

Password to Match

Case 1: User Input

Case 2: User Input

AUTHENTICATION SUCCESSFUL

AUTHENTICATION NOT SUCCESSFUL
Security Objective

\[ p(\text{brute-force attack}) = p(\text{observation attack}) \]

resilience to observation and brute-force attacks.

\[ p(\text{attack}) = \binom{\text{pin}}{1 \atop 3} \]

Security Standard:
4 digit numerical password
\[ p(\text{attack}) = 1/10000 \]
Evaluation: 2 studies

To gauge our interface we conducted 2 experiments

Pilot Study
Test tactons recognition rate
Evaluate if tactons are perceptually distinct

User Study
Evaluation of 3 software interfaces with the same hardware (Haptic Keypad)
Compare extreme authentication schemes to obtain some insight.
Experiments Design

Pilot Study

- Tacton recognition rates and times
- 4 participants
- Simplified version of the hardware
- 15 practice trial + 60 test trials (20 of each cue)
Experiments Design

Pilot Study
- Tacton recognition rates and times
- 4 participants
- Simplified version of the hardware
- 15 practice trial + 60 test trials (20 of each cue)

  • Result 1: no errors.
  • Result 2: average selection time was 2.5s (SD 0.57s)

User Study
- 3 experimental conditions (3 software prototypes)
- 12 participants volunteered (mean age 29y)

  • Fully balanced repeated measures. Given random passwords.
  • 10 trials x 12 subjects x 3 conditions = 360 PIN entry (2520 selection events)
3 Conditions, 3 Software Prototypes

Evaluation

<table>
<thead>
<tr>
<th>PIN</th>
<th>TACTONS</th>
<th>P(attack)</th>
<th>Safe?</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>3</td>
<td>1 / 729</td>
<td>NO</td>
</tr>
<tr>
<td>9</td>
<td>3</td>
<td>1 / 19863</td>
<td>YES</td>
</tr>
</tbody>
</table>

Trade off

“password length-performance”
3 Conditions, 3 Software Prototypes

Evaluation

Hybrid Mode

<table>
<thead>
<tr>
<th>PIN</th>
<th>TACTONS</th>
<th>P(attack)</th>
<th>Safe?</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>3</td>
<td>1 / 11941</td>
<td>Only to Observation</td>
</tr>
</tbody>
</table>

System Randomize

User feels the keys

User selects

OR

weighted 55% of cases

System Randomize

User feels the keys

User selects

all the **WRONG** tactons (complement)

Trade off

“complexity-performance”
1. Experiment Results: Authentication Time

Median task completion time

Medians were used to minimize the effect of outliers.

**ANOVA** and post-hoc **pair-wise**
t-tests **significants**.
2. Experiment Results: Errors

Mean number of Errors per Authentication Session

An ANOVA not significant (perhaps due to high variance)
2. Experiment Results: NASA TLX

ANOVA on overall workload (Nasa TLX) significant involving the Hybrid condition.
## Results

<table>
<thead>
<tr>
<th>Type</th>
<th>Performance</th>
<th>Security</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>6 PIN</td>
<td>Fast Time / Low Error</td>
<td>Low</td>
<td>User as reference value</td>
</tr>
<tr>
<td></td>
<td>3.7s per selection</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(2.5s in Pilot study: 3.7 &lt; 2.5*3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9 PIN</td>
<td>Fast Time / Low Error</td>
<td>Safe</td>
<td>Users didn’t find more challenging entering additional PINs</td>
</tr>
<tr>
<td></td>
<td>3.7s per selection</td>
<td></td>
<td>(linear proportion with 6 pin: 1.5 ratio between password length and time)</td>
</tr>
<tr>
<td>HYBRID</td>
<td>Slow Time / High Error</td>
<td>Observation Safe</td>
<td>High cognitive load (overhead)</td>
</tr>
<tr>
<td></td>
<td>6.5s per selection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Comparison with Previous Systems

### Results

<table>
<thead>
<tr>
<th></th>
<th>6 PIN</th>
<th>9 PIN</th>
<th>HYBRID</th>
<th>UNDERCOVER (CHI 08)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Time (s)</strong></td>
<td>22.2</td>
<td>33.8</td>
<td>39.5</td>
<td>39 - 49 (avg)</td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>9.2%</td>
<td>6.7%</td>
<td>15%</td>
<td>26%</td>
</tr>
</tbody>
</table>

*Data From Undercover*

- Go for unimodal!
- Simplicity of a pure recognition process: feel -> recognize -> select
Contributions

• Introducing the *Haptic Password model*

• Introducing one possible *interface and method* (Haptic Keypad) to use a Haptic Password

• Preliminary user tests suggests that *Haptic Password is a better alternative to Haptic Obfuscation*

  • *Unimodal*
  
  • *Simple cognitive task such as recognition*
The Phone Lock

Audio and Haptic Shoulder-Surfing Resistant PIN Entry Methods for Mobile Devices


Shift in computing, shift in interaction

From **private** user to **collaborative**

From **fixed** to **mobile**
Observation: The New Old threat

Large screens + public spaces =

Observation remains one of the most simple and common way to steal a PIN.
Two Objectives

1
Introducing a new PIN entry system for mobile devices resistant against observation.

Non-visual PIN and its role in tangible and ubiquitous interfaces

2
Comparing authentication performance of audio and haptic stimuli as PIN.

What is the best non-visual PIN?
How can we make an invisible PIN?

Make a PIN invisible using **invisible cues** and a **new interaction method**

**Audio PIN**
- computer speech

- A sequence of **audio cues** (sound) or **tactile cues** (tactons) inherently **invisible** to everyone.
Our Alphabet Cues: example sets

Haptics

Audio

0 1 2 3 4
Our Alphabet Cues: example sets

Haptics

Audio

0 1 2 3 4 5 6 7 8 9
Our Cues

Use these sets to make a PIN

- Orange: 5
- Yellow: 4
- Blue: 8
- White: 7
Our Cues

Haptic vibration patterns

Ordered set of possible cues

Audio computer speech
Mapping to Interface

Generalizing: cues with order

The Wheel GUI

1 to 1 assignment of cues to slots
Mapping to Interface

Generalizing: cues with order

Map every cue to a slot
- randomly
- preserving order

The Wheel GUI
Interaction

Let’s make a password using the cues

System Randomize slice-cue assignment preserving order

User move the finger over the slices and search the right cue

User selects the cue clicking the center of the wheel
Interaction

Let’s make a password using the cues

System Randomize slice-cue assignment preserving order

User move the finger over the slices and search the right cue

User selects the cue clicking the center of the wheel
Interaction

Let’s make a password using the cues

System

1. System Randomize slice-cue assignment preserving order
2. User move the finger over the slices and search the right cue
3. User selects the cue clicking the center of the wheel
Interaction

Let’s make a password using the cues

System Randomize slice-cue assignment preserving order

User move the finger over the slices and search the right cue

User selects the cue clicking the center of the wheel
Let's make a password using the cues

System Randomize slice-cue assignment preserving order

User moves the finger over the slices and searches the right cue

User selects the cue clicking the center of the wheel
Interaction map

Cue Assignment

Search Navigation

Selection

Ordered Randomization

Authentication Denied

Authentication Granted
In practice: demo

Inserting the PIN 1 2 4 3
To gauge our interface we conducted 2 experiments.

**Pilot Study**
- Test cue recognition rate
- Evaluate if cues are perceptually distinct (recognition time and error)

**User Study**
- Evaluation of interface to explore 2 trade-offs.
  - Audio VS Haptics
  - Large alphabet VS Small alphabet
Pilot Study - Highlights

- Simple recognition task. Simplified system.
- Mean cue recognition **time: 2.25s**
- Mean **error: 14%** (for the large haptic alphabet)

Mid-length 80ms element were the most challenging
User Study: analyze the trade-offs

We analyze 2 trade offs, maintaining a security level of 1/10000 (the security of a standard numerical 4 digit PIN).

We are interested in authentication time and errors.

1. Audio VS Haptics
2. Large alphabet (short PIN) VS Small alphabet (long PIN)

<table>
<thead>
<tr>
<th></th>
<th>Audio</th>
<th>Haptics</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 digits PIN</td>
<td>0,1,2,3,4,5,6,7,8,9</td>
<td><img src="image" alt="Haptics 4 digits" /></td>
</tr>
<tr>
<td>6 digits PIN*</td>
<td>0,1,2,3,4</td>
<td><img src="image" alt="Haptics 6 digits" /></td>
</tr>
</tbody>
</table>

*The 6 digits PIN test is to compare Phone Lock against previous work
1. Experiment Results: Authentication Time

Trade-offs (2-way ANOVA)
- **Modality** significant \((p<0.01)\)
- **PIN length** not significant

Overall
- **ANOVA** and post-hoc pair-wise t-tests **significants** \((p<0.01)\).
2. Experiment Results: Authentication Errors

Mean error 7% (<14% pilot)

Effect of Modality and PIN length and their interaction were not significant.
Discussion - Highlights

- Audio > Haptics.
  
  *Is because it is more familiar?*

- Error rate: 7% study < 14% pilot
  
  *People understood how to navigate the interface*

- Better performing than previous similar systems
Contributions

• Introducing the *Invisible Password* model using audio and tactile cues

• Introducing one possible *interface and method for mobile phones* (Phone Lock) to use with Haptic and Audio PINs

• Preliminary user tests suggests that *Invisible Password thought haptic and audio have a lot of potential*

  • *They are good fit for tangible user interfaces*
  • *Simple cognitive task such as recognition is good*
The SpinLock

Spinlock: a Single-Cue Haptic and Audio PIN Input Technique for Authentication

The problem with haptic passwords

Haptic Password using tactons is based on recognition:
high cognitive load, memorability issues, high error rates and input time
The problem with haptic: example
The problem with haptic: example

Can we create an interface with only 1 tactile cue instead of using many?

Can we build an interface with a different interaction methods that doesn’t require recognition but only counting?
Interaction principle

Using a similar interaction of a safe dial:

directions + numbers (e.g. 2 left, 3 right, 4 left...)
Implementation for a phone

Password are a sequence of direction-number of buzzes or beeps

Implemented for phone devices

Using haptics and audio output
How it works: example

Spin Left or Right until you hear the selection cue (beep)
User Study Planning

User study to compare performance of audio vs haptics, with different password sizes.

**Hypothesis 1:**
counting is faster than recognition

**Hypothesis 2:**
counting is less error prone than recognition

**Hypothesis 3:**
counting comports smaller cognitive load than recognition
The user study

2 modalities $\times$ 2 PIN complexity

- haptic/audio
- numbers 1-5 / numbers 1-10

12 participants (7 male, 5 female with age between 22 and 30 years)

15 trials (first 5 as training) = 480 complete correct PIN entries and 1920 individual data input

PIN randomly generated
User Study Balancing

Repeated measures experiment

<table>
<thead>
<tr>
<th>PIN</th>
<th>Modality</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>Short</td>
</tr>
<tr>
<td>User 2</td>
<td>Long</td>
</tr>
<tr>
<td>User 3</td>
<td>Short</td>
</tr>
<tr>
<td>User 4</td>
<td>Long</td>
</tr>
<tr>
<td>User 5</td>
<td>Short</td>
</tr>
<tr>
<td>User 6</td>
<td>Long</td>
</tr>
<tr>
<td>User 7</td>
<td>Short</td>
</tr>
<tr>
<td>User 8</td>
<td>Long</td>
</tr>
<tr>
<td>User 9</td>
<td>Short</td>
</tr>
<tr>
<td>User 10</td>
<td>Long</td>
</tr>
<tr>
<td>User 11</td>
<td>Short</td>
</tr>
<tr>
<td>User 12</td>
<td>Long</td>
</tr>
</tbody>
</table>

PIN complexity was balanced among participants

Modality was balanced within each PIN complexity block
User Study Setup

Quiet room

**Procedure:**
Demographic + Instruction + Free test + 4 studies + TLX

Mobile devices + connected to PC and Bluetooth for generating haptics

All data were tested using two-way repeated measures ANOVAs.
Results: time and errors

**Time**: significant effect on modality and PIN complexity \((p<0.05)\) but no interaction

**Error**: significant effect only on modality \((p<0.05)\)
Results: time and errors

**Time**: significant effect on modality and PIN complexity (p<0.05) but no interaction

**Error**: significant effect only on modality (p<0.05)
Results: time and errors

**Time:** significant effect on modality and PIN complexity (p<0.05) but no interaction

**Error:** significant effect only on modality (p<0.05)
The two-way ANOVA on the overall workload of the TLX showed a significant effect of modality (p=0.002) but not PIN complexity.
Haptic modality more challenging but preferred as it was more “private”.

**HAPTIC**

Significant differences were observed in the mean PIN entry times, failed authentication rates and overall workload. One possible explanation for this is system latency.

**PIN COMPLEXITY**

PIN complexity, on the other hand, resulted in increased task completion times, but had no significant effect on other metrics.
82% of error trials involved a mistake in only one PIN item. The majority of errors (78%) involved entering digits one higher or lower than the target item.

That participants were typically aware of such errors (= resets)
Spinlock also performs well compared to previous systems

15.4 seconds and 6%

18.7 seconds and 7% errors
Haptic Spinlock system improves 30% over that reported in PhoneLock
Haptic Comparison

Results

Spinloc

PhoneLock
User study to compare performance of audio vs haptics, with different password sizes.

**Hypothesis 1:** counting is faster than recognition

**Hypothesis 2:** counting is less error prone than recognition

**Hypothesis 3:** counting comports smaller cognitive load than recognition
PART II

THE ENEMY WITHIN:
PROTECTED KEY COMMUNICATION
FOR UNTRUSTED TERMINALS

SOFTWARE MEDIATED INPUT
UNTRUSTED TERMINALS

The password can be kept secret by the user...

...and encryption can keep it secure within the network...

...but it still has to be entered “in the clear” at the terminal!

**keystroke loggers** are a major method of password observation & compromise.

- OS-level loggers on pwned machines
- Malicious logging hardware
Many examples of malware install logging software...

...as do stalkers such as jealous husbands, employers, governments...

Some UI elements that may be logged:

- Keystrokes
- Mouse clicks
- Screenshots
- Mouse movements
PASSWORD MANAGEMENT

Computers & browsers now commonly contain “Keychain” password management software...

...but that's no help on an untrusted public terminal...

...and sometimes you just have no choice but to use that internet café in Uzbekistan.
SOME WEB PROTECTIONS

- Forced password changes
  - Damage control
- Image-based access methods
- Changing security questions
- One-time-password via SMS
  - Phone theft gives bonus account access
- One-time-PIN token
  - Reduces value of stealing password
- Printed list of one-time password modifiers

Few sites offer multiple options, and in many cases not even one!
PROBLEM SUMMARY

Ideal outcome:

Application software for increased resistance to credential loss & replay attack for any website

Public terminal constraints:

- Can’t verify integrity of system
- Usually can’t install or run application software
  
  BUT

- Can access pretty much any web content

Goal: obfuscate data entry via simple, minimally tedious web mechanics
COMMON NAÏVE APPROACHES

- Defense: “Scissor” password copy-paste
- Counterattack: Clipboard logging

- Defense: Character select-drag-drop
- Defense: Onscreen keyboards
- Counterattack: Mouse click screen region capture

- Defense: Chaff logs via tedious extraneous character entry
- Counterattack: Log mining in concert with screen & mouse logging and timestamping (theoretical)
WHAT ABOUT FORM GRABBERS?

• Form grabbing malware hooks browser form submit pre-encryption
  • e.g. Online banking theft trojans ZeuS, SpyEye
  • Represents majority of password-stealing trojans

• However:
  • Limited platform/browser support (currently Windows-only)
  • There is no UI mechanism that can defend against this tactic anyway
    • We are primarily interested in interface design
  • Still worth defending against UI-device-level loggers
BASIC APPROACH

- Keep any sensitive text entirely out of key log
- Minimize data leakage via other UI logging mechanisms
- Novel interaction methods while trying to minimize tedium
- Support evolutionary ecosystem: force attackers to adapt
- Custom interface element production via JavaScript injection:

```javascript
javascript: void((function() {
  var element = document.createElement('script');
  element.setAttribute('type', 'text/javascript');
  element.setAttribute('language', 'JavaScript');
  element.setAttribute('src', 'https://path/to/logresist.js');
  document.getElementsByTagName('head')[0].appendChild(element);
})(()=>{}))
```
• Key remapper (no mouse)
• User interface metaphor: hunt-and-peck keyboard
• Can be regenerated on per-keystroke basis if required
• Susceptible to screen capture, but only if triggered by keystroke
• Keylog output: encrypted stream equal in length to plaintext
• Time cost: visual search
• Animated key selector
• User interface metaphor: combo lock
• Uses mouse but no clicks
• Susceptible to screen capture, but only if triggered by keystroke and synchronized with mouse pointer location history
• Keylog output: string of identical characters, arbitrary length
• Time cost: visual search plus (variable) animation
• Auditory stimulus to key location
• User interface metaphor: audio phone lock
• Immune to screen capture
• Keylog output: string of identical characters, arbitrary length
• Time cost: fixed animation
SUMMARY

- Give users choice of obfuscation methods independent of support offered by web service
- Seed ecosystem of custom methods easy to implement and select
- Offer modalities not traditionally logged (e.g. audio)
  - Force attackers to expend more effort
- Examples of methods from very large potential space
- User evaluation studies yet to be performed
PART III
DESITUATING THE INTERACTION: PROTECTED KEY TRANSMISSION FOR PRIVATE DEVICE SOLUTIONS

HARDWARE MEDIATED INPUT
Using Light Patterns to Secretly Transmit a PIN
PRIVATE DEVICE MEDIATION

1. Different people want **different password schemes**

and a personal private device is where this is possible.
2. **We want to move away the interaction** from the physical terminal **and a private device can help us in this too!**

We shift the problem **from authentication to secure communication channel**
CURRENT PROBLEMS

Current problems with hardware mediated interaction

1. **Spontaneous interaction** - No pairing needed

2. **No wireless** - Safe against Man In The Middle Attack

3. **Fast** interaction, **easy** to use
1) **Shift the interaction** away from the terminal, on a private device

2) **Avoid wireless** to avoid a Man In The Middle (MITM) attack.

3) Secure authentication with **no pairing requirements**: you cannot pair a phone to any terminal you will ever use. PKI is not always possible.

4) **Authentication, not identification**: RFID can be stolen more easily than passwords. Also passwords are easier to replace.

5) Must be **cheap** to make, to install. **Easy to use.**
WANTED INTERACTION

PHYSICAL PROXIMITY
Encoding a password in light patterns

- User has a password
- Inserts a password on mobile phone
- The password is encoded in a light signal (as with Morse)
- Computer + light scanner get the signal and translate it
- Authentication

Input

Light

0001
0010
0011
0100
- Error rate < 1%
- Plain text transmission time < 1 second
- MD5- 128 bit hashing encryption: 5.5 seconds
Insert the correct PIN
Authentication will be granted

Work In Progress - LuxPass Color
MAGNOPASS

Work In Progress

Solenoid  Patterns of on/off magnetic field  Mag Sensor
Conclusions

- Passwords & PINs are not going away
- We still need to authenticate with public locations/terminals
- Generally simple methods can improve their security in potential observation risk scenarios
  - Diversifying ecosystem of entry methods
  - Mediated obfuscation of entered data
- Presented novel key entry systems for terminals & private devices
- Presented software & hardware mediators for observation resistance
- Attacks will always be developed – you don’t have to run faster than the bear, just faster than everyone else!