A Fast Eavesdropping Attack Against Touchscreens

Federico Maggi, Alberto Volpatto, Simone Gasparini, Giacomo Boracchi, Stefano Zanero

Politecnico di Milano
How sensitive data is compromised

- Direct attacks
  - Well-known in both literature and industry
  - Very active research community
- **Other types of attacks**
  - Social engineering attacks
  - Side-channel attacks
  - Difficult to mitigate (if not through awareness)
Side-channel Attacks

- Less known yet very effective
- Digital side-channels
  - Example: decrypting SSL through wifi LAN sniffing
- **Physical-world observation**
  - Direct observation
    - Shoulder surfing
  - Indirect observation
    - Sound emanations
    - Reflections
    - Magnetic radiations
    - Desk surface vibrations
Physical-world Observation
Automated Shoulder Surfing

- First attempt of **automatic** shoulder surfing
- Recovery of long texts
Ubiquitous Touchscreen Mobiles

- **2010** survey on 2,252 US citizens
  - 72% use a mobile phone for **texting**
  - 30% use a mobile phone for **instant messaging**
  - 38% use a mobile phone for Web **browsing**
- (1970) **touchscreen** technology was invented
  - 2010: **5 billion** US dollars market
  - 159% market **grow** rate
  - Q3 2010: 417 million of touchscreen
Automated Shoulder Surfing

- Non-automated
  - not interesting
  - time consuming

- Automated
  - Is it feasible?
  - Mobile context poses several constraints
Mobile Settings Constraints

- Moving target
- Fixed observation point not always feasible
- Very small keyboards
- No visibility of pressed keys
- No visible key occlusions
Touchscreen to the rescue

- Lack of tactile feedback
- Early soft keyboards were hard to use
- UI engineers came up with usable keyboards
Usability vs Security

- Old dilemma
- More secure, less easy to use
- Example: Google’s 2-step authentication
  - Very secure
  - Very unusable
    - Wait for the verification code every time you do email
- Apply also in this context
  - Feedback-less touchscreen keyboards
    - Hard to type on
  - Feedback-rich keyboard keyboards
    - Easy to type on
    - Eyes follow the feedback naturally during typing
To: Rob Tucker

Subject: Re: Jenny's Birthday

Great pick!
Our approach
Simple Threat Model

- **Requirement 1**
  - iPhone-like visual feedback mechanism

- **Requirement 2**
  - Template of the target screen known in advance
Requirement 1 is often satisfied
Requirement 2 is very easy to satisfy

**SCREEN TEMPLATE**

(screenshot)

**KEY TEMPLATES**

(synthetic, hi-res)

**MAGNIFIED LAYOUT**

(x,y-coordinates)
Outline of the Approach

- **Phase 1**
  - Screen detection and rectification

- **Phase 2**
  - Magnified key detection

- **Phase 3**
  - Keystroke sequence reconstruction
Phase 1

- **Input**
  - Image depicting the current scene (current frame)

- **Output**
  - Synthetic image of the rectified, cropped screen

- **Procedure**
  - Screen detection
  - Screen rectification
The current frame is searched for the screen template (Requirement 1)
Screen Detection via Template Matching

- **SURF features**
  - Edges
  - Corners

- **Invariant to:**
  - Rotation
  - Scale
  - Skew
  - Occlusions

- **Homography estimation**
Screen Rectification via Homography

- Estimate during screen detection
- Successfull matches improve matches in subsequent frames
Phase 2

- **Input**
  - Image of the rectified screen

- **Output**
  - Areas where magnified keys appeared

- **Procedure**
  - Background subtraction
Pixelwise Background Subtraction

CURRENT FRAME  -  SCREEN TEMPLATE  =  FOREGROUND
Spurious output

HIGHLIGHTED KEY (MAGNIFIED-KEY CANDIDATE)

OTHER FOREGROUND ELEMENTS (NOISE)

FOREGROUND
Phase 3

- **Input**
  - Magnified-key candidates

- **Output**
  - Sequence of typed symbols

- **Procedure**
  - Approximate neighbors lookup
  - Best matching key identification
  - Fast pruning
  - Key sequence analysis
Approximate Neighbor Lookup

- Known keyboard layout (Requirement 2)
- Centroid identification
- Match centroids with keyboard layout
Known keyboard layout
Centroid identification
Match centroids with layout

CENTROID 1

CENTROID 2

CENTROID 3
Key similarity

- Region of interest
- Key template (Req. 2)
Computing the key similarity is expensive.

Black-white distribution of the ROI.

%B/W-heuristic is way faster.

Baseline
Key Sequence Analysis

- Find maxima of the key similarity
Phase 1
- C++
- OpenCV

Phase 2-3
- Matlab
- Compiled into C

Threshold estimation
- Confidence interval (mean, variance)
- Video samples collected in “no typing” conditions
DEMO

http://www.youtube.com/watch?v=aPuS8kNI30U

http://www.youtube.com/watch?v=t9BxB3dO0KQ
Experimental Evaluation

- Types of text
  - Context-free
  - Context-sensitive
- 3 attackers, 3 victims
- Goals
  - Precision and speed
  - Resilience to disturbances
Overall evaluation procedure

- **Typing**
  - 3 victims are given the input text
  - Victims type text on their iPhones

- **Recording**
  - A recording camera was used for repeatability

- **Attack**
  - 3 attackers are provided with the videos
  - Attackers have “infinite” time to analyze videos

- **Comparison**
  - Automatic attack vs. human attackers
spent chapter foundation identified because first which material notation summarized time spent volume much technical little system reference figured number measurement lorem referring abstract text introductory shown in the we observing request second objective books relationship astute formidable quantile convenient remainder between utilizable tool law resident minutes exemplified the product then temporarily number will per systematic average accumulated south specialty terminal numerous introduce
close your eyes and begin to relax take a deep breath and let it out slowly concentrate on your breathing with each breath you become more relaxed imagine a brilliant white light above you focusing on this light as it flows through your body allow yourself to drift off as you fall deeper and deeper into a more relaxed state of mind now as i
Almost as precise as a human

Hit rate: context-free text  □□□□□
Error rate: context-free text  □□□□□

context-rich text □□□□□
context-rich text □□□□□

10.2% bound

Hit or error rate [0,1]

Way faster than a human

Decoding speed: context-free text
context-rich text

<table>
<thead>
<tr>
<th>Speed (symbols per second)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.9</td>
</tr>
<tr>
<td>0.8</td>
</tr>
<tr>
<td>0.7</td>
</tr>
<tr>
<td>0.6</td>
</tr>
<tr>
<td>0.5</td>
</tr>
<tr>
<td>0.4</td>
</tr>
<tr>
<td>0.3</td>
</tr>
<tr>
<td>0.2</td>
</tr>
</tbody>
</table>

## Extreme conditions

<table>
<thead>
<tr>
<th>Aberration</th>
<th>Phase 1</th>
<th>Phase 2-3</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) Permanent occlusion</td>
<td>difficult</td>
<td>44.44</td>
</tr>
<tr>
<td>2) Shake device</td>
<td>feasible</td>
<td>67.74</td>
</tr>
<tr>
<td>3) Shake camera</td>
<td>feasible</td>
<td>96.00</td>
</tr>
<tr>
<td>4) Shake device + camera</td>
<td>unfeasible</td>
<td>0.00</td>
</tr>
</tbody>
</table>
Limitations

- **Non-magnifying keys**
  - Space (on iPhone only)
  - Layout-switching keys
  - **Mitigation**
    - Device-specific heuristics
    - E.g., on iPhone, exploit color-changing spacebar

- **Alternative layouts** (minor limitation)
  - **Mitigation**
    - Detect switch
    - Loop through different templates during detection
Alternative layouts
iSpy: A Happy Coincidence

- [Raguram, CCS 2011]
- Appeared at the same conference
- Completely different approach
  - Classification-based
  - They require training
- Really, the very same accuracy 97~98%
Conclusions

- Touchscreen mobile devices are widespread
- Shoulder surfing is automatable
- Automatic shoulder surfing is precise too
- Counteract these attacks with privacy screens
- But...
Finger tracking

- **Challenge**
  - How to detect tapping?
THANKS!

Stefano Zanero
stefano.zanero@polimi.it
@raistolo

NECST Lab
Dipartimento di Elettronica e Informazione
Politecnico di Milano
SysSec: A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet
What is the impact of attacks?

“... potential (cyber)attacks against network infrastructures may have widespread and devastating consequences on our daily life: no more electricity or water at home, rail and plane accidents, hospitals out of service”

Viviane Reding,
Vice President European Commission
Government: The Parliament under attack
Transportation: No train signals

Computer Virus Brings Down Train Signals

The virus infected the computer system at CSX's headquarters, shutting down signaling, dispatching, and other systems for trains throughout the East.

By Marty Niland, Associated Press Writer
InformationWeek
August 20, 2003 06:00 PM

NEW YORK (AP) -- A computer virus was blamed for bringing down train signaling systems throughout the East on Wednesday.

The virus infected the computer system at CSX Corp.'s Jacksonville, Fla., headquarters, shutting down signaling, dispatching, and other systems at about 1:15 a.m. EDT, CSX spokesman Adam Hollingsworth said.

"The cause was believed to be a worm virus similar to those that have
Transportation: No cars

Hacker Disables More Than 100 Cars Remotely

By Kevin Poulsen  March 17, 2010 | 1:52 pm  Categories: Breaches, Crime, Cybersecurity, Hacks and Cracks

More than 100 drivers in Austin, Texas found their cars disabled or the horns honking out of control, after an intruder ran amok in a web-based vehicle-immobilization system normally used to get the attention of consumers delinquent in their auto payments.

Police with Austin's High Tech Crime Unit on Wednesday arrested 20-year-old Omar Ramos-Lopez, a former Texas Auto Center employee who was laid off last month, and allegedly sought revenge by bricking the cars sold from the dealership's four Austin area lots.
Energy: No electricity
Defense: fighter planes grounded
What about our lives? Are they next?
What’s next?

**SysSec**: managing threats and vulnerabilities for the future Internet
a Network of Excellence (2010-2014)

Why?
We need to work towards solutions
We need to collaborate
At a European level
With our international colleagues
Around the world

- Poli. di Milano (IT)
- Vrije Universiteit (NL)
- Institute Eurecom (FR)
- BAS (Bulgaria)
- TU Vienna (Austria)
- Chalmers U (Sweden)
- TUBITAK (Turkey)
- FORTH – ICS (Greece)
What is SysSec?

SysSec proposes a *game-changing* approach to cybersecurity: Currently Researchers are mostly reactive:

- they usually track cyberattackers *after* an attack has been launched
- thus, researchers are always one step behind attackers

SysSec aims to break this vicious cycle

Researchers should become more *proactive*:

- Anticipate attacks and vulnerabilities
- Predict and prepare for future threats
- Work on defenses *before* attacks materialize.
SysSec Aim and Objectives (I)

Create an active, vibrant, and collaborating community of Researchers with
the expertise, capacity, and determination to anticipate and mitigate the
emerging threats and vulnerabilities on the Future Internet.

SysSec aims
to create a sense of "community" among those researchers,
to mobilize this community,
to consolidate its efforts,
to expand their collaboration internationally, and
become the single point of reference for Systems Security research in Europe.
SysSec Aim and Objectives (II)

Advance European Security Research well beyond the state of the art
research efforts are fragmented

SysSec aims to provide a research agenda and
align their research activities with the agenda
make SysSec a leading player in the international arena.
SysSec Aim and Objectives (III)

Create a **virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities. By forming a **critical mass** of European Researchers and by aligning their activities,

Have the gravitas needed to play a **leading role internationally**, empowered to undertake large-scale, ambitious and high-impact research efforts.

Create a **Center of Academic Excellence** in the area create an education and training program targeting young researchers and the industry.

lay the foundations for a common graduate degree in the area with emphasis on Systems Security.
Maximize the impact of the project by proactive \textit{dissemination} to the appropriate stakeholders. Disseminate its results to international stakeholders so as to form the needed \textbf{strategic partnerships} (with similar projects and organizations overseas) to play a major role in the area.

Dissemination within the Member States will reinforce SysSec's role as a \textbf{center of excellence} and make SysSec \textbf{a beacon for a new generation of European Researchers.}

\textbf{Create Partnerships and transfer technology to the European Security Industry.}

Create a close partnership with Security Industry facilitate technology transfer wherever possible to further strengthen the European Market.
SysSec: How can you collaborate

Contribute to the research roadmap/agenda
Provide feedback on emerging threats
Share your ideas on future security issues

Contribute to our “systems security” University curriculum
Contribute homeworks/exams
Contribute/use lab exercises

Teach some of the courses at your University
Share some of your course material

Become an “Associated Partner” of the project