Covert & Side Stories: Threats Evolution in Traditional and Modern Technologies

Mauro Conti
February 27, 2024
Can't You Hear Me Knocking: Novel Security and Privacy Threats to Mobile Users

Mauro Conti, University of Padua

Slides prepared with the support of Daniele Lain and Riccardo Spolaor

University of Washington

July 18, 2018 - Seattle, WA, USA
A CRYPTO NERD'S IMAGINATION:

HIS LAPTOP'S ENCRYPTED.
LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.

NO GOOD! IT'S 4096-BIT RSA!

BLAST! OUR EVIL PLAN IS FOILED!

WHAT WOULD ACTUALLY HAPPEN:

HIS LAPTOP'S ENCRYPTED.
DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL
HE TELLS US THE PASSWORD.

GOT IT.
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - *As a side channel: app and sensitive data inference*

- Energy Consumption
  - *As a side channel: user and app inference*
  - *As a covert channel: data exfiltration*

- Device Movement
  - *As a side channel: smartphone user authentication*
  - *Attacks against biometric authentication*

- Keystroke Timing
  - *As a side channel: text typed on keyboards*

- Acoustic Emanations
  - *As a side channel: text typed on keyboards*
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards

Keystroke Inference
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
Side Channels

Devices, and network communication, are usually protected and encrypted
Side Channels

Devices, and network communication, are usually protected and encrypted.

→ Difficult for Attackers to violate such protection.
Side Channels

Observing emanations and patterns

*Can reveal secrets!*

This is called a **side channel**
Covert Channels are used to communicate stealthily.

Either to avoid listeners in the middle...

...or to exfiltrate information.
Outline

- Covert and Side Channels 101

  - **Network Traffic Analysis**
    - *As a side channel: app and sensitive data inference*

  - Energy Consumption
    - *As a side channel: user and app inference*
    - *As a covert channel: data exfiltration*

  - Device Movement
    - *As a side channel: smartphone user authentication*
    - *Attacks against biometric authentication*

  - Keystroke Timing
    - *As a side channel: text typed on keyboards*

  - Acoustic Emanations
    - *As a side channel: text typed on keyboards*

Can't you hear me knocking: Identification of user actions on Android apps via traffic analysis.

In ACM SIGSAC CODASPY 2015

V. F. Taylor, R. Spolaor, M. Conti, I. Martinovic.


In IEEE EuroSP 2016
Traffic Analysis

Traffic patterns
*Can reveal what we are doing!*

Device-platform interaction reveals our actions

Called traffic analysis
Motivation

Encryption is not enough!

Can’t you hear me knocking
(CODASPY ‘14, TIFS ‘15)

[Song et al. '11]

[Wright et al. '08]
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

**Attacker's observations**

- **Coarse features:**
  - Packet lengths
  - Packet directions
  - Packet timings
  - ....

Enable Traffic Analysis Attacks
Attack scenario

Network traffic

Log actions

12:30  Post on wall
11:44  Private message
11:21  Post on wall
10:45  User profile page
10:30  Post on wall
09:21  Open Facebook
Attack scenario

Network traffic

BIG BROTHER
IS WATCHING YOU

Log actions

12.30  Post on wall
11.44  Private message
11.21  Post on wall
10.45  User profile page
10.30  Post on wall
09.21  Open Facebook
Attack scenario

Network traffic

BIG BROTHER IS WATCHING YOU

Log actions

- 12.30 Post on
- 11.44 Private
- 11.21 Post on
- 10.45 User profile
- 10.30 Post on wall
- 09.21 Open Facebook

facebook

- 64 people like this.
- 64 likes and 6 comments

facebook

- We're proud to be joining the Alliance To Save Energy and to be working on making the updates that make Facebook even more efficient.

facebook

- Facebook is the Alliance to Advance the Cause of Saving Energy | Alliance to Save Energy

facebook

- We love one's friends on their favorite Pages, as we've launched a new feature for Page admins to help improve the quality of posts you see. If you like it, be sure to like the Facebook Pages page for more updates.

facebook

- Improving Page Content on Your Wall

facebook

- Facebook is committed to helping people engage and interact with high-quality content from their favorite brands and businesses.

facebook

- 26,439,489 People Like This

facebook

- 26,393,089 People Like This
Other attack scenarios

- To identify communicating parties
  - from sending/receiving pattern

- Behavioural profiling
  - to improve fingerprintings
  - for marketing reasons
  - ...

The goal

Can an attacker recognize actions that a user performs on some android app by analyzing the encrypted network traffic?

Contribution

- We prove that it is possible, with an accuracy > 95%
- Traffic analysis using machine learning techniques
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Key Concepts

Interactions

used to achieve

User actions

produce

Network flows

Input on a device
E.g., tap, swipe, key press

Operation on apps
E.g., send an email, open a page

Sequence of packets
Couple of IP addresses and ports
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Dataset collection

Server
ubuntu

Android Debug Bridge

Python script

Wireshark

Network bridge

Access Point

USB cable

The Internet

Ethernet cable
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Network Traffic Flows Representation

<table>
<thead>
<tr>
<th>Flow ID</th>
<th>Flow time series</th>
</tr>
</thead>
<tbody>
<tr>
<td>Flow 1</td>
<td>[282, -1514, -1514, -315, 188, -113, 514, 96, 1514, 179, 603, 98, 801, 98, -477]</td>
</tr>
<tr>
<td>Flow 2</td>
<td>[282, -1514, -1514, -1266, -582, 188, -113, 692, 423, -661]</td>
</tr>
<tr>
<td>Flow 3</td>
<td>[926, 655, 136, -1245, 913, 1514, 1514, 863, -1514, -107, -465, -172, -111]</td>
</tr>
</tbody>
</table>
The framework

**Phase 1. Training**

**Phase 2. Testing**

Predictions
- Tweet sent
- Email answered
- tweeter contact opened...

Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Training phase

1. Unsupervised learning → **Clusters** of similar flows
   - Dynamic Time Warping (DTW) [Müller 2007] as metric
   - The number of clusters is a parameter to tune

2. Training set building
   - User actions → Classes
   - Cluster labels → Features

<table>
<thead>
<tr>
<th>IDs</th>
<th>user actions</th>
<th>cluster 0</th>
<th>cluster 1</th>
<th>...</th>
<th>cluster k</th>
<th>....</th>
<th>cluster N-1</th>
<th>cluster N</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>send mail</td>
<td>0</td>
<td>1</td>
<td>...</td>
<td>1</td>
<td>...</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>002</td>
<td>send mail</td>
<td>0</td>
<td>1</td>
<td>...</td>
<td>1</td>
<td>...</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>003</td>
<td>send reply</td>
<td>1</td>
<td>0</td>
<td>...</td>
<td>2</td>
<td>...</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

3. Supervised learning → Random Forest **classifier**
Evaluation phase

1. User actions produce **unseen flows**

2. Assign each **unseen flow** to a **cluster**
   - clusters used in **training** phase and **DTW** as metric

3. Test set building
   - (similarly to training set)
   - User actions → **unknown classes**
   - Cluster labels → Features

4. User action **recognition**

Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Accuracy vs. number of clusters

![Graph showing accuracy vs. number of clusters for different platforms like Facebook, Gmail, Twitter, Tumblr, Dropbox, Google+, and Evernote.](image-url)
Can’t you hear me knocking (CODASPY ‘14, TIFS ‘15)

Accuracy per user action
Conclusions

- Encryption does not hide communication patterns
  - We shown that user actions performed on Android apps can be detected by analyzing the encrypted network traffic

- Attackers can leverage our framework to undermine user privacy:
  - Learn user habits
  - Gain commercial or intelligence advantage against some competitor
  - Attribution of social network pseudonyms

- Countermeasures to this type of attacks are needed...
Motivation (1)

From the set of **apps installed** on a device can be inferred private information about her **owner**:

- Age
- Sex
- Religion
- Relationship status
- Spoken languages
- Countries of interest

Motivation (2)

Knowing a presence of a specific app
Hence specific vulnerabilities

Possible ad-hoc attacks
E.g., zero day exploits

AppScanner
(IEEE EuroS&P ‘16)
Motivation

- Given a target app X
- Identify the presence of X in a mobile device
- Using network traffic analysis
Motivation

● Given a target app X
● Identify the presence of X in a mobile device
● Using network traffic analysis

It isn’t so easy!
Motivation

● Given a target app X
● Identify the presence of X in a mobile device
● Using network traffic analysis

It isn’t so easy!

● Encryption → Payload inspection is not feasible
Motivation

- Given a target app X
- Identify the presence of X in a mobile device
- Using network traffic analysis

It isn’t so easy!

- Encryption → Payload inspection is not feasible
- Owner of Destination IP ≠ App
  - Content Delivery Network (CDN)
  - Proxy
Attacker's observations (similarly to the previous work)

- Packet length
- Packet directions
- Packet timings

Enable Traffic Analysis Attacks

AppScanner
(IEEE EuroS&P ‘16)
AppScanner
(IEEE EuroS&P ‘16)

Traditional Client-Server Architecture

Content Delivery Network CDN
Three different approaches proposed:

1. **Per flow Multi-class** length classification
   - A classifier for each length
   - No out-of-order packets resiliency, but fast
Three different approaches proposed:
Three different approaches proposed:

1. **Per flow Multi-class** length classification
   - A classifier for each length
   - No out-of-order packets resiliency, but fast

2. **Large Multi-class** classification
   - Uses statistics on network flows
   - It works on a set of apps
   - High Accuracy and out-of-order packets resiliency, but slow
Three different approaches proposed:

1. **Per flow Multi-class** length classification
   - A classifier for each length
   - No out-of-order packets resiliency, but fast

2. **Large Multi-class** classification
   - Uses statistics on network flows
   - It works on a set of apps
   - High Accuracy and out-of-order packets resiliency, but slow

3. **Per App** classification
   - Uses statistics on network flows
   - It focuses on a specific app
   - Binary classification (app is present or not)
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSv1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>114</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>796</td>
</tr>
</tbody>
</table>
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSv1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>114</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>796</td>
</tr>
</tbody>
</table>
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSV1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSV1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>114</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSV1</td>
<td>796</td>
</tr>
</tbody>
</table>
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSv1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>796</td>
</tr>
</tbody>
</table>

Per Flow approach (1)

Variable Length Feature Vectors

[74, -74, 66, 287, -66, -1078, ..., -796]
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSv1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>114</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>796</td>
</tr>
</tbody>
</table>

Per Flow approach (1)

- Flow Pre-processor
- Statistical Feature Extraction
- Feature Scaler [0, 1]
- Feature Selection

Variable Length Feature Vectors

- [74, -74, 66, 287, -66, -1078, ..., -796]

Constant Length Feature Vectors

- [0.12, 0.76, 0.32, 0.1, 0.39, ..., 0.88]
Building the dataset

TCP Packets captured

<table>
<thead>
<tr>
<th>SOURCE_IP</th>
<th>DEST_IP</th>
<th>PROTO</th>
<th>LEN</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>74</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>192.168.137.2</td>
<td>23.23.162.140</td>
<td>TLSv1</td>
<td>287</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>66</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>114</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TCP</td>
<td>1078</td>
</tr>
<tr>
<td>23.23.162.140</td>
<td>192.168.137.2</td>
<td>TLSv1</td>
<td>796</td>
</tr>
</tbody>
</table>

Per Flow approach (1)

Statistical approaches (2, 3)
Improving the accuracy of AppScanner

- Classification performed on each network traffic flow
- We aim to identify an app \(\rightarrow\) many flows available
- Flow \(\rightarrow\) Classifier prediction \(\rightarrow\) (App, Probability of prediction)
- Applying a probability threshold (PT)
  - Filter out flows with uncertain predictions
  - Increase classification accuracy tuning PT
AppScanner (IEEE EuroS&P '16)

Performance and Comparison

1. Per Flow SVC
2. Per Flow RF
3. Single Large SVC
4. Single Large RF
5. Per App SVC
6. Per App RF
7. Panchenko
8. Liberatore NB
9. Herrmann TF
10. Herrmann Pure
11. Herrmann Cos
12. Liberatore Jaccard

Classifiers:
- AppScanner pt=0.5
- AppScanner (no pt)
- Competitors

Classifier Accuracy (%)
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards

**Mind The Plug! Laptop-User Recognition Through Power Consumption.**

*In ACM AsiaCCS 2016 workshop IoTPTS 2016*
Power Consumption Side Channel

Power consumption
*Can reveal what we are doing!*

Device drains different power depending on our actions

Works on **laptops** and mobile
Mind the Plug! (IoTPTS @AsiaCCS ’16)

Smartbuilding

Internet of Things applied not only to industry, but also to buildings, such as houses and **offices**
Mind the Plug! (IoTPTS @AsiaCCS ’16)

Wall-socket smartmeters

- Smartmeters are able to measure the electric quantities of the plugged appliances
  - Reactive Power
  - RMS Current
  - Voltage
  - Phase

- IoT testbed in University of Surrey (UK)

- Limitation:
  - only **1Hz** of sampling rate
Definition of “Laptop-User”

A Laptop-user is made of the combination of:

○ Laptop
○ Software installed and running
○ User behavior
Goal & Motivation

Is it possible to recognize a Laptop-user from its energy consumption?

This can bring:

- Benefit on smartbuilding automation,
  - context-aware environments can automatically adjust and trigger predefined actions or services
    - e.g., according to the presence of a specific user
  - Detect un-authorized users

- Threat to user privacy,
  - it is possible to locate and trace a user
Mind the Plug! (IoTPTS @AsiaCCS ’16)

Threat Model

Office
Seven authorized users

Twenty unauthorized users

We aim to:
- Recognize whether the user is in the “authorized” set
- Identify the specific user in the “authorized” set
Laptop-users Recognition

Multiclass classification (8 classes)
- The **seven authorized** laptop-users
- The **intruders** (as a single class)

Classification in three steps:
1. 10-fold cross validation for **parameters selection**
2. Performance **evaluation** on a disjoint test set
3. Classification **validation**
Figure 2: Example of Active Power trace (continuous blue line) and the lower-cutting threshold $\alpha = 12$ Watt (dashed red line). Samples under $\alpha$ are low-energy timespans in which the user does not use the laptop.
Mind the Plug! (IoTPTS @AsiaCCS ’16)

85% of F-measure with Random Forest classifier
Classification validation

Classifiers label all segments in the testset
- Bad for False Positive rate (FPR)

We can leverage also the prediction probability
- Since classifiers output also their confidence

Tuning prediction probability threshold
- It can reduce False Positives

Other implications:
- MTPlug can be more conservative
- May take more segments to identify some laptop-user
Mind the Plug! (IoTPTS @AsiaCCS ’16)

Classification validation results

Considering the 60% of segments
Limitations and Future work

**Structural limitation:**
The plogg wall-socket sensors have a low sampling rate

**Solution:**
Adopt a new generation wall-socket sensors

**Data limitation:**
we collected data of seven users (office)

**Solution:**
Collect more data in order to assess the feasibility of authentication system based on energy consumption
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
R Spolaor, L Abudahi, V Moonsamy, M Conti, R Poovendran.  
**No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices.**  
*In ACNS 2017*  

*Presented at Black Hat Europe 2018*
Power Consumption Covert Channel

Power consumption
*Can be used as a covert channel*

Malware makes device drain more/less power to communicate with a *malicious power outlet*

Thus *exfiltrating secrets*
No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices
USB protection...

Protect your data

SyncStop prevents accidental data exchange when your device is plugged into someone else's computer or a public charging station. SyncStop achieves this by blocking the data pins on any USB cable and allowing only power to flow through. This minimizes opportunities to steal your data or install malware on your mobile device.

SyncStop is the 'cased' version of the original USB Condom. We listened and spent some time designing and manufacturing our own enclosure.

SyncStop works with any mobile device:
PowerSnitch Application

Legend: Module  Signals / intents  Input parameters
No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices

Results in terms of Bit Error Ratio (BER)

<table>
<thead>
<tr>
<th>Device</th>
<th>Period (milliseconds)</th>
<th>1000</th>
<th>900</th>
<th>800</th>
<th>700</th>
<th>600</th>
<th>500</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nexus 4</td>
<td>13.5</td>
<td>0.78</td>
<td>0.0</td>
<td>0.0</td>
<td>13.33</td>
<td>16.21</td>
<td></td>
</tr>
<tr>
<td>Nexus 5</td>
<td>21.0</td>
<td>0.0</td>
<td>0.95</td>
<td>36.82</td>
<td>40.35</td>
<td>13.4</td>
<td></td>
</tr>
<tr>
<td>Nexus 6</td>
<td>1.07</td>
<td>0.0</td>
<td>0.21</td>
<td>0.0</td>
<td>4.05</td>
<td>7.42</td>
<td></td>
</tr>
<tr>
<td>Samsung S5</td>
<td>12.5</td>
<td>13.5</td>
<td>13.31</td>
<td>16.33</td>
<td>17.9</td>
<td>21.42</td>
<td></td>
</tr>
</tbody>
</table>

PowerSnitch app does not require any permission !!!
Power Bank Prototype
Power Bank - DEMO TIME

https://drive.google.com/file/d/1JXzoyOM3xpQqaM8exWF07htp67G5m82y/view?usp=sharing
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
Keystroke Dynamics 101
Keystroke Dynamics 101
Keystroke Dynamics 101
Keystroke Dynamics 101

Digram \( t_{AB} \)  \( t_{AC} \)  Trigram
Keystroke Dynamics 101

- Inter-keystroke times as a personal *signature*
- Used as biometric in authentication systems
Kamil Majdanik, Cristiano Giuffrida, Mauro Conti, Herbert Bos.

I Sensed It Was You: Authenticating Mobile Users with Sensor-enhanced Keystroke Dynamics.

In DIMVA 2014
I Sensed It Was You

Our system: Unagi

User authentication with Sensor enhanced Keystroke Dynamics

Scenario: User typing 'HELLO'
I Sensed It Was You

Keystroke dynamics
I Sensed It Was You

Keystroke dynamics

Sensor-enhanced keystroke dynamics
I Sensed It Was You

Accuracy (EER) for different considered algorithms
I Sensed It Was You

Accuracy vs. Sensors Sampling Frequency

EER - Equal Error Rate (rate at which both acceptance and rejection errors are equal)
Key Results

- Movement sensors are suitable for biometric authentication
- Sensors can dramatically enhance keystroke dynamics accuracy
- Effective even with short passwords and low sampling frequencies

Future work

- Applicability to free-text authentication
- Robustness against statistical attacks
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
V. D. Stanciu, R. Spolaor, M. Conti, C. Giuffrida

**On the Effectiveness of Sensor-enhanced Keystroke Dynamics Against Statistical Attacks**

*in ACM CODASPY 2016*
The previous behavioral biometric authentication system relies on:

- Secret of the password
- Keystroke dynamics (touch gestures)
- Accelerometer and Gyroscope sensors data

Previous work: we used kNN (with $k=1$) and mean values combined with several metrics (e.g., euclidean, Manhattan)

**Question:** is our system resilient to **Statistical attacks**?
Statistical Attack

Population

User 1 samples
User 2 samples
User 3 samples
User 4 samples
User 5 samples
User 6 samples
User 7 samples
Statistical Attack

Population

User 1 samples
User 2 samples
User 3 samples
User 4 samples
User 5 samples
User 6 samples
User 7 samples

Statistical analysis

User X forged samples
Statistical Attack

Population

User 1 samples
User 2 samples
User 3 samples
User 4 samples
User 5 samples
User 6 samples
User 7 samples

Statistical analysis

User X forged samples

Input

User X trained profile
Sensor-enhanced keystroke dynamics biometric authentication mechanism
Results

low Equal Error Rate (EER) == accurate authentication method

(a) Keystroke-Dynamics Only.
Results

low Equal Error Rate (EER) == accurate authentication method

(a) Keystroke-Dynamics Only.

(b) Sensors only.
Results

low Equal Error Rate (EER) == accurate authentication method
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- **Keystroke Timing**
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
Kiran Balagani, Mauro Conti, Paolo Gasti, Martin Georgiev, Tristan Gurtler, Daniele Lain, Charissa Miller, Kendall Molas, Nikita Samarin, Eugen Saraci, Gene Tsudik, Lynn Wu

SILK-TV: Secret Information Leakage From Keystroke Timing Videos.

In ESORICS 2018
Timing Information Leak - 1

Guest Session
Remote Login
VIC \neq ATK
VIC
Contributions

- Quantify information leakage of on-screen keystroke feedback

- Novel attack: SILK-TV
  - Uses public datasets only from multiple sources ("population data")
  - Machine Learning to guess typed text (passwords and PINs)
<t_0, t_1, ... >

ML
SILK-TV

<\(t_0, t_1, \ldots\)>

ML

Training data

CV
SILK-TV

<\( t_0, t_1, \ldots \)>

\( \text{CV} \)

\( \text{ML} \)

\( c_1 \quad c_2 \quad c_3 \)

\[ [ab, [jk, xy, rs, \ldots ], \ldots ] \]

Training data
CV → <t₀, t₁, …>

ML

Training data

C₁ C₂ C₃

[ab, jk, xy, rs, … ]

password
iloveryou
12345678
qwertyui
princess
…
Data Collection - Passwords

- Data from **projector** and **laptop screen** @ 60Hz
- Recorded with a smartphone
- 62 users - 3 times each pwd - **touch typing** on keyboard
- Randomly selected 4 passwords from **rockyou**
  
    - 123brian, jillie02, lamondre, william1

1 - [http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2](http://downloads.skullsecurity.org/passwords/rockyou.txt.bz2)
Baseline: password list sorted by frequency
- “Best” strategy for a zero-information attacker

- 123brian - 93,874th
- jillie02 - 1,753,571st
- lamondre - 397,213rd
- william1 - 187th ← very frequent password

Evaluation scenarios
- “Single shot”
- “Multiple recordings” (e.g., professor at lectures)
Password - “Single Shot” results

(a) 123brian (183 auth. attempts).
(b) jillie02 (186 auth. attempts).
(c) lamondre (184 auth. attempts).
(d) william1 (183 auth. attempts).
Password - “Single Shot” results

(a) 123brian (183 auth. attempts).

(b) jillie02 (186 auth. attempts).

(c) lamondre (184 auth. attempts).

(d) william1 (183 auth. attempts).
Password - “Single Shot” results

(a) 123brian (183 auth. attempts).

(b) jillie02 (186 auth. attempts).

(c) lamondre (184 auth. attempts).

(d) william1 (183 auth. attempts).
## Password - “Single Shot” results

<table>
<thead>
<tr>
<th></th>
<th>Avg</th>
<th>Stdev</th>
<th>Med</th>
<th>Rnd</th>
<th>&lt;Rnd</th>
<th>Best</th>
<th>&lt;20k</th>
<th>&lt;100k</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Random Forest</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>581,743</td>
<td>414,761</td>
<td>508,332</td>
<td>93,874</td>
<td>8.7%</td>
<td>5,535</td>
<td>1.1%</td>
<td>9.3%</td>
</tr>
<tr>
<td>jillie02</td>
<td>749,718</td>
<td>448,319</td>
<td>656,754</td>
<td>1,753,571</td>
<td>97.8%</td>
<td>28,962</td>
<td>0.0%</td>
<td>2.7%</td>
</tr>
<tr>
<td>lamondre</td>
<td>301,906</td>
<td>334,681</td>
<td>199,344</td>
<td>397,213</td>
<td>75.0%</td>
<td>145</td>
<td>13.0%</td>
<td>33.7%</td>
</tr>
<tr>
<td>william1</td>
<td>246,437</td>
<td>264,090</td>
<td>145,966</td>
<td>187</td>
<td>0.5%</td>
<td>68</td>
<td>10.9%</td>
<td>39.9%</td>
</tr>
<tr>
<td><strong>Neural Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>923,534</td>
<td>165,454</td>
<td>886,802</td>
<td>93,874</td>
<td>0.0%</td>
<td>577,739</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>jillie02</td>
<td>456,811</td>
<td>210,512</td>
<td>383,230</td>
<td>1,753,571</td>
<td>100.0%</td>
<td>164,754</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>lamondre</td>
<td>517,472</td>
<td>189,355</td>
<td>493,713</td>
<td>397,213</td>
<td>28.8%</td>
<td>148,403</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>william1</td>
<td>265,813</td>
<td>140,753</td>
<td>215,840</td>
<td>187</td>
<td>0.0%</td>
<td>45,176</td>
<td>0.0%</td>
<td>3.8%</td>
</tr>
</tbody>
</table>

Avg, Stdev, Median of SILK-TV cracking attempts

Rnd average baseline cracking attempts

<Rnd, Best, <20k, <100k highlights of SILK-TV performance
### Password - “Single Shot” results

<table>
<thead>
<tr>
<th></th>
<th>Avg</th>
<th>Stdev</th>
<th>Med</th>
<th>Rnd</th>
<th>&lt;Rnd</th>
<th>Best</th>
<th>&lt;20k</th>
<th>&lt;100k</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Random Forest</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>581,743</td>
<td>414,761</td>
<td>508,332</td>
<td>93,874</td>
<td>8.7%</td>
<td>5,535</td>
<td>1.1%</td>
<td>9.3%</td>
</tr>
<tr>
<td>jillie02</td>
<td>749,718</td>
<td>448,319</td>
<td>656,754</td>
<td>1,753,571</td>
<td>97.8%</td>
<td>28,962</td>
<td>0.0%</td>
<td>2.7%</td>
</tr>
<tr>
<td>lamondre</td>
<td>301,906</td>
<td>334,681</td>
<td>199,344</td>
<td>397,213</td>
<td>75.0%</td>
<td>145</td>
<td>13.0%</td>
<td>33.7%</td>
</tr>
<tr>
<td>william1</td>
<td>246,437</td>
<td>264,090</td>
<td>145,966</td>
<td>187</td>
<td>0.5%</td>
<td>68</td>
<td>10.9%</td>
<td>39.9%</td>
</tr>
<tr>
<td><strong>Neural Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>923,534</td>
<td>165,454</td>
<td>886,802</td>
<td>93,874</td>
<td>0.0%</td>
<td>577,739</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>jillie02</td>
<td>456,811</td>
<td>210,512</td>
<td>383,230</td>
<td>1,753,571</td>
<td>100.0%</td>
<td>164,754</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>lamondre</td>
<td>517,472</td>
<td>189,355</td>
<td>493,713</td>
<td>397,213</td>
<td>28.8%</td>
<td>148,403</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>william1</td>
<td>265,813</td>
<td>140,753</td>
<td>215,840</td>
<td>187</td>
<td>0.0%</td>
<td>45,176</td>
<td>0.0%</td>
<td>3.8%</td>
</tr>
</tbody>
</table>

Avg, Stdev, Median of SILK-TV cracking attempts

Rnd average baseline cracking attempts

<Rnd, Best, <20k, <100k highlights of SILK-TV performance
### Password - “Single Shot” results

<table>
<thead>
<tr>
<th></th>
<th>Avg</th>
<th>Stdev</th>
<th>Med</th>
<th>Rnd</th>
<th>&lt;Rnd</th>
<th>Best</th>
<th>&lt;20k</th>
<th>&lt;100k</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Random Forest</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>581,743</td>
<td>414,761</td>
<td>508,332</td>
<td>93,874</td>
<td>8.7%</td>
<td>5,535</td>
<td>1.1%</td>
<td>9.3%</td>
</tr>
<tr>
<td>jillie02</td>
<td>749,718</td>
<td>448,319</td>
<td>656,754</td>
<td>1,753,571</td>
<td>97.8%</td>
<td>28,962</td>
<td>0.0%</td>
<td>2.7%</td>
</tr>
<tr>
<td>lamondre</td>
<td>301,906</td>
<td>334,681</td>
<td>199,344</td>
<td>397,213</td>
<td>75.0%</td>
<td>145</td>
<td>13.0%</td>
<td>33.7%</td>
</tr>
<tr>
<td>william1</td>
<td>246,437</td>
<td>264,090</td>
<td>145,966</td>
<td>187</td>
<td>0.5%</td>
<td>68</td>
<td>10.9%</td>
<td>39.9%</td>
</tr>
<tr>
<td><strong>Neural Network</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>123brian</td>
<td>923,534</td>
<td>165,454</td>
<td>886,802</td>
<td>93,874</td>
<td>0.0%</td>
<td>577,739</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>jillie02</td>
<td>456,811</td>
<td>210,512</td>
<td>383,230</td>
<td>1,753,571</td>
<td>100.0%</td>
<td>164,754</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>lamondre</td>
<td>517,472</td>
<td>189,355</td>
<td>493,713</td>
<td>397,213</td>
<td>28.8%</td>
<td>148,403</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>william1</td>
<td>265,813</td>
<td>140,753</td>
<td>215,840</td>
<td>187</td>
<td>0.0%</td>
<td>45,176</td>
<td>0.0%</td>
<td>3.8%</td>
</tr>
</tbody>
</table>

Avg, Stdev, Median of SILK-TV cracking attempts

Rnd average baseline cracking attempts

<Rnd, Best, <20k, <100k highlights of SILK-TV performance
Timing Information Leak - 2

Keypad not visible - but the screen is!
Conclusions

- Timing information from videos is **accurate**

- Password masking leak timing $\rightarrow$ useful information
  - *Reduces number of attempts*
  - *More useful on uncommon passwords!*

- Performances on PIN... not great (close to random guess)
Keypad not visible - but the screen is!
PILOT
Password and PIN Information Leakage from Obfuscated Typing Videos
Kiran Balagani, Matteo Cardaioli, Mauro Conti, Paolo Gasti, Martin Georgiev, Tristan Gurtler, Daniele Lain, Charissa Miller, Kendall Molas, Nikita Samarin, Eugen Saraci, Gene Tsudik, and Lynn Wu

In Journal of Computer Security 2019
PILOT

CV

<\(t_0, t_1, \ldots\)>

ML
PILOT

CV

<t_0, t_1, ... >

ML

Training data
PILOT

CV

\( <t_0, t_1, \ldots > \)

ML

Inter-key distances

PIN Guesser

Training data
Covert and Side Channels

PILOT

Mauro Conti

CV

<\(t_0, t_1, \ldots\)>

Inter-key distances

ML

PIN Guesser

5566
5544
2233
2211
5522
...

Training data

PIN Guesser
Percentage of PINs recovered with PILOT vs Random Guessing

- 4 digit PIN (USA ATM card)
Your PIN Sounds Good!
On The Feasibility of PIN Inference Through Audio Leakage
Matteo Cardaioli, Mauro Conti, Kiran Balagani, and Paolo Gasti

IEEE Transactions on Information Forensics and Security 2019 (Submitted)
Neither keypad nor screen are visible
Inter-keystroke timing identification through sound analysis

- **Signal filtering**
  
  *To extract feedback sound characteristic frequency*

- **Signal processing**
  
  *To remove residual noise and to identify time distance between peaks*
Your PIN Sounds Good!

Adversarial additional knowledge about the user or the PIN

- Knowledge of typing behavior
  
  *Hunt-and-peck vs. touch typing*

- Knowledge of a digit
  
  Adversary knows one digit of the PIN

- Heatmap
  
  Adversary performs a thermal attack
  
  - Better on plastic and rubber
  - Not so good on metal
Your PIN Sounds Good!

ML

<\( t_0, t_1, \ldots >

PIN Guesser

Inter-key distances

CV

Training data

PIN Guesser
Your PIN Sounds Good!

ML

<\(t_0, t_1, \ldots\)>

CV

Inter-key distances

PIN Guesser

· Behavior
· Digit
· Heatmap

Training data
Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!

Your PIN Sounds Good!
Your PIN Sounds Good!

% PINs recovered: inter-keystroke timing + other informations
Your PIN Sounds Good!

% PINs recovered: inter-keystroke timing + other informations

![Graph showing PIN recovery rates across different types of information and number of guesses.](image-url)
Your PIN Sounds Good!

ALL MEN ARE CREATED EQUAL
THOMAS JEFFERSON (1742–1826)
Your PIN Sounds Good!

ALL MEN ARE CREATED EQUAL?
THOMAS JEFFERSON (1742–1826)
Your PIN Sounds Good!

All Men Are Created Equal?

Thomas Jefferson (1742–1826)

User Chosen
Your PIN Sounds Good!

ALL MEN ARE CREATED EQUAL?
THOMAS JEFFERSON (1742–1826)

PIN

User Chosen

Random
Your PIN Sounds Good!

User Chosen

PIN

Random

DEFINITELY... NOT!
Your PIN Sounds Good!

Not all PINs are born the same

Knowing inter-key distance only
Your PIN Sounds Good!

Not all PINs are born the same

Knowing *inter-key distance only*  →  PINs probability distribution is no longer uniform

Showing just a subset of PINs

- 1216
- 1219
- 1215
- 2120
- 1213
- 1212
- 1211
- 2110
- 2116
- 2119
- 2115
- 1220
- 2113
- 2112
- 2111

**Number of Guesses**

- 0
- 128 attempts on average
- 2 attempts on average
DEMO time!
Hand Me Your PIN!
Inferring ATM PINs of Users Typing with a Covered Hand
Matteo Cardaioli, Stefano Cecconello, Mauro Conti, and Simone Milani

In USENIX Security Symposium 2022
Hand me Your PIN

Hidden camera recording the PIN pad

 Victim’s covering strategy to avoid shoulder surfing attacks
Experimental Setting

**Training**
- ATM Replication
- Train data collection
- Labels: 53776 87326 ...
- Model Training

**Video Recording**
- Hidden camera positioning
- Victims recording
- Videos retrieval

**PIN Inference**
- Keystroke timestamp identification
- Keys labels Prediction
- PIN Ranking

<- identify frame with “pressing”
<-input: window of frames close to the press
Out: single keys probabilities

<- Rank PINS according to single key prob.
**Attack Scenarios**

- **Single PIN pad:**
  - the adversary knows the target PIN pad model and owns a copy

- **PIN pad Independent:**
  - the adversary trains the machine learning model on a PIN pad with a similar (but not the same) layout to the target one.

- **Mixed:**
  - the adversary owns both a copy of the target PIN pad and a PIN pad similar to the target one

---

**Results**

**Heatmap for prediction of Digit “1”**
Results

Human Vs Machine assessment

Survey:
- **30 videos** of people entering **5-digit PINs** by covering the PIN pad with the non-typing hand
- Videos from the **Mixed scenario** test set (i.e., the only one including both PIN pads)
- Participants had to indicate **the three most likely** PINs

Participants:
- **45 participants** performed the questionnaire **without any training**
- **33 participants** **pre-trained** on other covered PIN videos from the test set.
## Results

### Covering strategy

<table>
<thead>
<tr>
<th>Covering strategy</th>
<th>Scenario</th>
<th>Key accuracy</th>
<th>PIN TOP-3 accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Side</td>
<td>Single</td>
<td>0.64</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>Independent</td>
<td>0.42</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Mixed</td>
<td>0.77</td>
<td>0.53</td>
</tr>
<tr>
<td>Over</td>
<td>Single</td>
<td>0.52</td>
<td>0.12</td>
</tr>
<tr>
<td></td>
<td>Independent</td>
<td>0.31</td>
<td>0.10</td>
</tr>
<tr>
<td></td>
<td>Mixed</td>
<td>0.46</td>
<td>0.07</td>
</tr>
<tr>
<td>Top</td>
<td>Single</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td></td>
<td>Independent</td>
<td>0.41</td>
<td>0.13</td>
</tr>
<tr>
<td></td>
<td>Mixed</td>
<td>NA</td>
<td>NA</td>
</tr>
</tbody>
</table>

### Experiment

<table>
<thead>
<tr>
<th>Experiment</th>
<th>Key accuracy</th>
<th>PIN TOP-3 accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input resolution 125 x 125</td>
<td>0.55</td>
<td>0.23</td>
</tr>
<tr>
<td>Input resolution 64 x 64</td>
<td>0.47</td>
<td>0.15</td>
</tr>
<tr>
<td>Left-corner camera</td>
<td>0.46</td>
<td>0.10</td>
</tr>
<tr>
<td>Right-corner camera</td>
<td>0.62</td>
<td>0.31</td>
</tr>
<tr>
<td>Multi-camera training</td>
<td>0.53</td>
<td>0.22</td>
</tr>
<tr>
<td>No data augmentation</td>
<td>0.44</td>
<td>0.11</td>
</tr>
<tr>
<td>Blacklisted excluded in training</td>
<td>0.54</td>
<td>0.18</td>
</tr>
</tbody>
</table>

(a) *Side:* hand resting on the side of the palm.

(b) *Over:* raised hand not touching the surface.

(c) *Top:* hand resting on fingers and vertically covering the PIN pad.

(a) *Left-corner camera.*

(b) *Center camera.*

(c) *Right-corner camera.*
Countermeasures

(a) 25% of PIN pad surface covered (i.e., digits form 1 to 3).
(b) 50% of PIN pad surface covered (i.e., digits form 1 to 6).
(c) 75% of PIN pad surface covered (i.e., digits form 1 to 9).
(d) 100% of PIN pad surface covered (i.e., no digit is visible).

<table>
<thead>
<tr>
<th>Coverage percentage</th>
<th>Key accuracy</th>
<th>PIN TOP-3 accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>25%</td>
<td>0.54</td>
<td>0.22</td>
</tr>
<tr>
<td>50%</td>
<td>0.55</td>
<td>0.22</td>
</tr>
<tr>
<td>75%</td>
<td>0.50</td>
<td>0.17</td>
</tr>
<tr>
<td>100%</td>
<td>0.33</td>
<td>0.01</td>
</tr>
</tbody>
</table>
Outline

- Covert and Side Channels 101

- Network Traffic Analysis
  - As a side channel: app and sensitive data inference

- Energy Consumption
  - As a side channel: user and app inference
  - As a covert channel: data exfiltration

- Device Movement
  - As a side channel: smartphone user authentication
  - Attacks against biometric authentication

- Keystroke Timing
  - As a side channel: text typed on keyboards

- Acoustic Emanations
  - As a side channel: text typed on keyboards
For your voice only
Exploiting side channels in voice messaging for environment detection
Matteo Cardaioli, Mauro Conti, and Arpita Ravindranath

In ESORICS 2022
Is GPS the only way to locate you?
Can audio messages be used in identification of the location/room?
Experimental Setting

DATA ACQUISITION
- Recording
- Word Segmentation

DATA PROCESSING
- Feature Extraction
  - \([f_{1,1}, f_{2,1}, \ldots, f_{n,1}]\)
  - \([f_{1,2}, f_{2,2}, \ldots, f_{n,2}]\)
  - \([f_{1,m}, f_{2,m}, \ldots, f_{n,m}]\)
- Feature Aggregation
  - \([f_1, f_2, \ldots, f_m, s_1, s_2, \ldots, s_n]\)

MODEL TRAINING
- Training set (labelled)
- Testing set (unlabelled)

LOCATION INFERENCE
Experimental Setting

Age distribution

- Number of subjects
- Age

Gender Ratio
- Male: 33.3%
- Female: 66.7%

LOCATIONS:
- 3 INDOOR
- 1 OUTDOOR

AUDIO CONTENT/SYLLABLES:
- AND
- OF
- THE

DEVICE: 14 DIFFERENT DEVICE MODELS
- {SAMSUNG, ONEPLUS, IPHONE, MOTO}
Experimental Setting
Experimental Setting

Indoor 1 (I1)

Indoor 2 (I2)

Indoor 3 (I3)

Outdoor (O1)
Scenarios

**SPEAKER KNOWN**
Complete Profiling ("Investigator" case)

**SPEAKER UNKNOWN**
Location Profiling

ADV has samples on
- ALL locations (room and specific position inside)
- but NOT from Victim

**LOCATION KNOWN**

**LOCATION UNKNOWN**

ADV has samples
- OF the victim
- In the correct room but in **unknown specific position** (inside that known room)

User Profiling
Scenarios (just in case...)

- **Complete Profiling**: This scenario occurs when the attacker asks the victim to send voice messages from specific locations. For example, an investigator (i.e., the attacker) might ask a suspect (i.e., the victim) to stand in a specific part of a room to verify that the suspect was there or elsewhere at the time a voice message was sent. In this scenario, the attacker has recordings of the victim in all the selected locations. Moreover, the attacker also knows the victim’s specific position in the selected locations (e.g., a room corner). In this scenario, the attacker has the highest knowledge to execute his attack.

- **Location Profiling**: In this scenario, the attacker cannot access any of the victim’s voice messages other than the one he wants to infer the location. The attacker knows that the victim has sent the voice message from a selected location (e.g., the attacker knows that the victim is in a specific building). Therefore, the attacker can have WhatsApp audio recordings of different speakers but the victim. The speakers are assumed to have recorded their messages at the same locations where the victim is sending the voice message. Hence, the victim is “unknown” while the location position is “known” to the attacker.

- **User Profiling**: This scenario occurs when the attacker owns the victim’s voice messages and knows the recording location but does not know the specific position in the location (e.g., a corner of a room) from which they were recorded. The attacker wants to infer the location of a new voice message sent by the victim. Different from the Complete Profiling scenario, the attacker cannot ask the victim to send more voice messages from specific positions of the selected locations (e.g., the victim is no longer reachable). The victim is “known” while the position is “unknown” to the attacker in this situation.
Results
Results
F. Marchiori, M. Conti

*Your Battery Is a Blast!*

*Safeguarding Against Counterfeit Batteries with Authentication*

*In ACM Conference on Computer and Communications Security (CCS’ 23)*
Battery Authentication

How many Lithium-ion batteries are around you right now?
Battery Authentication

- Store as chemical energy -> turned into electrical energy
How many **safe** Lithium-ion batteries are around you right now?

Lithium-ion (Li-ion) batteries market was estimated to be up to **48 billion U.S. dollars in 2022**

In 2003, roughly **5 million counterfeit cellular phone** batteries were seized worldwide. [https://www.wilsonelser.com/files/repository/PL_eNews0308_LithiumIonBatteries.pdf](https://www.wilsonelser.com/files/repository/PL_eNews0308_LithiumIonBatteries.pdf)

In 2016, in a case related to hoverboards with counterfeit batteries, the U.S. customs and border protection agency seized over 16 thousand counterfeit hoverboards with an estimated value of over **USD 6 million** [https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-record-amount-counterfeit-hoverboards](https://www.cbp.gov/newsroom/local-media-release/cbp-seizes-record-amount-counterfeit-hoverboards)
Battery Authentication

How have we checked it until now? *(tick means defence is successful)*

<table>
<thead>
<tr>
<th>Method</th>
<th>Cloning</th>
<th>Replay Attacks</th>
<th>Unscalability</th>
<th>Rewrapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>Markings</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>External Features</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Form Factor</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Resistor</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Chip</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR (in clear)</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CR (encrypted)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td><strong>DCAuth</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td><strong>EISthentication</strong></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

CR = Challenge and Response Protocols
Our contribution

- Leverage only internal characteristics of the batteries
- Scalable to many models and architectures
- Small computational cost

We make dataset and code available.

https://github.com/Mhackiori/DCAuth
https://github.com/Mhackiori/EISthentication
Battery Authentication

Differential Capacity Analysis (DCA)

- Measuring change in capacity response in the electrodes
- It tracks increase/decrease in capacity when charged/discharged
- Plot of differential capacity versus voltage
Battery Authentication

Electrochemical Impedance Spectroscopy (EIS)

- Analytical technique for electrochemical system characterization
- Measures the electrical impedance
- Dependence on several environment/external factors

![Graphs showing dependence on SOC, SOH, and temperature](image)

(a): Dependence on SOC.
(b): Dependence on SOH.
(c): Dependence on temperature.
Battery Authentication

System Model

Data Collection

- Battery

- DCA

- EIS

Raw Data

Data Processing

- Data Filtering

- Feature Extraction

Model

Authentication Result
Battery Authentication

Datasets

- Issues in finding collaborations with companies or organization
- Collection of available datasets
- 20 datasets (17 for DCA, 3 for EIS)
  - That includes 11 different models, 5 different architectures

Processing (available on GitHub)
Battery Authentication

Models
- Machine Learning
- Avoiding complex DL to keep low computational cost
- Commonly used in literature

Evaluation Metrics
- Precision
- Recall
- F1 Score
- False Acceptance Rate (FAR)
- False Rejection Rate (FRR)

<table>
<thead>
<tr>
<th>Models</th>
<th>Hyperparameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdaBoost (AB)</td>
<td>• Number of estimators</td>
</tr>
<tr>
<td>Decision Tree (DT)</td>
<td>• Criterion</td>
</tr>
<tr>
<td></td>
<td>• Maximum Depth</td>
</tr>
<tr>
<td>Gaussian Naive Bayes (GNB)</td>
<td>• Variance Smoothing</td>
</tr>
<tr>
<td>Nearest Neighbors (KNN)</td>
<td>• Number of neighbors</td>
</tr>
<tr>
<td></td>
<td>• Weight function</td>
</tr>
<tr>
<td>Neural Network (NN)</td>
<td>• Hidden layer sizes</td>
</tr>
<tr>
<td></td>
<td>• Activation function</td>
</tr>
<tr>
<td></td>
<td>• Solver</td>
</tr>
<tr>
<td>Quadratic Discriminant Analysis (QDA)</td>
<td>• Regularization Parameter</td>
</tr>
<tr>
<td>Random Forest (RF)</td>
<td>• Criterion</td>
</tr>
<tr>
<td></td>
<td>• Number of estimators</td>
</tr>
<tr>
<td>Support Vector Machine (SVM)</td>
<td>• Kernel</td>
</tr>
<tr>
<td></td>
<td>• Regularization parameter</td>
</tr>
<tr>
<td></td>
<td>• Kernel coefficient</td>
</tr>
</tbody>
</table>
Battery Authentication

Results - Identification

DCAuth

EISthentication
Battery Authentication

Results - Authentication

![Graph showing F1 scores for different models and methods for DCAuth and EISfhentication]
Battery Authentication

Results - FAR/FRR on Dataset Balance

DCAuth
### Table 12: Complexity.

<table>
<thead>
<tr>
<th>Model</th>
<th>$\text{Time}_{DCA}$</th>
<th>$\text{Size}_{DCA}$</th>
<th>$\text{Time}_{EIS}$</th>
<th>$\text{Size}_{EIS}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>AB</td>
<td>15.492 ms</td>
<td>75 kB</td>
<td>8.523 ms</td>
<td>59 kB</td>
</tr>
<tr>
<td>DT</td>
<td>3.892 ms</td>
<td>31 kB</td>
<td>2.881 ms</td>
<td>20 kB</td>
</tr>
<tr>
<td>GNB</td>
<td>4.687 ms</td>
<td>53 kB</td>
<td>3.192 ms</td>
<td>33 kB</td>
</tr>
<tr>
<td>KNN</td>
<td>12.951 ms</td>
<td>4800 kB</td>
<td>7.1 ms</td>
<td>263 kB</td>
</tr>
<tr>
<td>NN</td>
<td>4.595 ms</td>
<td>2600 kB</td>
<td>3.204 ms</td>
<td>1200 kB</td>
</tr>
<tr>
<td>QDA</td>
<td>7.856 ms</td>
<td>3100 kB</td>
<td>4.435 ms</td>
<td>271 kB</td>
</tr>
<tr>
<td>RF</td>
<td>13.661 ms</td>
<td>348 kB</td>
<td>13.288 ms</td>
<td>221 kB</td>
</tr>
<tr>
<td>SVM</td>
<td>9.854 ms</td>
<td>500 kB</td>
<td>2.99 ms</td>
<td>158 kB</td>
</tr>
</tbody>
</table>
Conclusions and Follow-ups

- Important issue to address for user safety
- More data can improve the methodology
- Collecting data in various condition can enhance the adaptability of the system

https://arxiv.org/abs/2309.03607
R. Spolaor, H. Liu, F. Turrin, M. Conti, X. Cheng

*Plug and Power: Fingerprinting USB Powered Peripherals via Power Side-channel*

In IEEE International Conference on Computer Communications (INFOCOM) 2023
USB Devices

- Widely used in everyday life
  - Peripheral devices, smartphone, IoT
- Data Transfer + Power supply
- **No security** measure by design
- Common attack vectors
  - Malware, BadUSB, USBkill
Idea

Exploit Power Side-Channel to identify **authorized devices**

- Identification of **legitimate devices**
- Recognize **legitimate actions**
- Detect **malicious devices**

Use cases

- End-user Personal Protection
- Organization Assets Protection
Data Collection

USB Power traces collection

- 82 different devices
  - 8 types
    - HDD, USB stick, WiFi & Bluetooth adapters, mouse, keyboard, webcam, microphone
  - 35 models

- Automated collection

- Different action
  - Boot
  - On (operating mode)
  - Actions (e.g., read, write, connect)

- Univariate time series
Analysis Goals

1. **Type** (during *Boot* and *On states*)
2. **Model** (*Boot* and *On*)
3. Specific **Device** among the ones with same model
4. **Action** given a device type
5. Given a type, **Device via action**
6. **Good vs. Bad** (malicious USB peripherals)
Pipeline

1) **Traces Preprocessing**
   a) Segmentation: sliding window (1 second with a 75% overlap)
   b) Feature extraction with *tsfresh* libraries (740 features per segment)

2) **Model tuning**
   a) Random Forest classifier (each task)
   b) 70% training, 10% validation, and 20% test (stratified)
   c) SMOTE to balance classes

3) **Classification approaches**
   a) Multiclass with “Other” class
   b) Binary (One-vs-All strategy) with Unknown devices in test

4) **Evaluation Metrics:** Precision, Recall, F1-Score, G-Mean, AUC
Type Recognition - Results (1/6)

- Recognize the type during *Boot* and *On* states
- **Multiclass** approach
  - 8 classes
  - *Other* includes random traces
- **Boot**: Mouse and Keyb (upon visual inspection)
  - Very quick (below 0.5 second)
  - LEDs may introduce noise
- **On**: simple to detect

We can discriminate USB type for *Boot* and *On*
Model Recognition - Results (2/6)

- Recognize the model during Boot and On states
- Multiclass approach
  - 35 classes
  - Other includes random traces
- On: high classification performance
- Keyb3 and Fd8 perform worst
  - Very quick (below 0.5 second)
  - LEDs may introduce noise
- Accurate fingerprint with 75 features both Boot and On

We can discriminate USB model for Boot and On
Device Recognition - Results (3/6)

- Given peripherals of the same model identify the specific device
  - Models with \# \geq 4 individual devices
- Binary approach
  - One random class not in Training set
- No good results on Mouse1 and Keyb1 state *Boot*
- WiFi1 model has the lowest score on state *On*
  - Models’ traces are very similar

We can **almost** discriminate the specific USB device
Action Recognition - Results (4/6)

- Recognize an ongoing action given a device type

- **Multiclass** approach
  - *Fd, Hdd, and WiFi*
  - *Other* includes random actions

- WiFi type have a clear fingerprint

- Miss-classification between Write and In-Write
  - *In-Write is derived by the combination of Read and Write*

We can discriminate action given a type
Device via Action - Results (5/6)

- Given an action for a type, identify specific device

- *Binary* approach
  - Fd, Hdd, and WiFi types (46, 10, and 38 classes)

- Good performance for all the types and actions
- Fd and Hdd actions are distinguishable
- WiFi slightly lower performance (similar behavior)

We can fingerprint an individual device from its actions
Bad vs. Good - Results (6/6)

- Discriminate between
  - Flash Drives
  - Bad USBs
- Multiclass approach
  - 3 classes
  - Other legitimate includes other legitimate peripherals
- While collecting traces we run several attacks
  - command injection, WiFi scanning and connection
- Good scores according to all metrics

We can discriminate Bad USBs
Lesson Learned

- **USB devices are a still a common attack vector**
- **Evolution of the standard did not include any security**
- **Power consumption allows USB fingerprinting**
  - State
  - Type
  - Model
  - Specific device
  - Action
  - Malicious devices
- **Protect the host from USB-based threats**
  - Non Intrusive
  - Privacy preserving
M. Conti, E. Losiouk, A. Visintin

**What You See is Not What You Get**

*A Man-in-the-Middle Attack Applied to Video Channels*

*In ACM/SIGAPP Symposium On Applied Computing 2022*
Man-in-the-Middle attack on a video channel.

*Using a Raspberry PI to modify in real-time the HDMI output before it is displayed.*
Phishing replica of Bank of America website.

*Raspberry PI detects and modify the URL into a legit one.*
Measured performances show the practicality of the attack. *The frame rate can be substantially improved using dedicated hardware.*
Attack demo available online.
https://www.youtube.com/watch?v=lvsoJdpNsZA&ab_channel=SPRITZResearchGroupvideos
A. Compagno, M. Conti, D. Lain, G. Tsudik

Don’t Skype & Type! Acoustic Eavesdropping in Voice-over-IP.

In ACM SIGSAC AsiaCCS 2017

Presented at Black Hat USA 2017
Keyboard Acoustic Eavesdropping

- **Supervised Learning** (Asonov, 2004; Halevi, 2012; 2014)
  
  *Less input assumptions, more specific*

- **Unsupervised Learning** (Berger, 2006; Zhuang, 2009)
  
  *More input assumptions, more general*
Keyboard Acoustic Eavesdropping

1 - How to get either:
- A lot of data
- Some labeled data

correct horse
battery staple
Keyboard Acoustic Eavesdropping

1 - How to get either:
   - A lot of data
   - Some labeled data

2 - How to place a compromised microphone close to my victim?
Motivation

VoIP → one of the most used software: in academia, industry, at home

People type private stuff during Skype calls - it happens!
- Login to websites
- Write a sensitive email
- Take notes

We hear the keys’ noise and use it to understand typed text
- Victim is willingly giving us access to his microphone
Skype&Type Attack

Types secret during Skype call with Attacker

Victim

S&T Attack

Extract features

Training data?

Secret

Victim model

Generic model

Attacker
S&T - Tools

- Data windowing and segmentation
  *To extract sound samples*

- Mel frequency cepstral coefficients
  *Best performing and robust*

- Supervised learning paradigm
  *Target text can be possibly:*
    - Short (no clustering)
    - Random (no dictionary)

- Logistic Regression classifier
Data Collection

- Try S&T in many scenarios
  - With 5 different users over Skype (Google Hangouts also vulnerable)
  - Using 3 different common laptops: Macbook Pro, Lenovo, Toshiba
  - With 2 typing styles: single finger, and natural “touch” typing

- Evaluate top-n accuracy of character recognition
  as a function of the number of guesses, focus on top-1 and top-5 accuracy

- Against a “dumb” random guess
  Might be a random password -- we can not use “smarter” approaches
Attack Scenarios

Evaluate the attack on two realistic scenarios

- **Complete Profiling Scenario** *(Asonov, 2004; Halevi, 2012; 2014)*
  - *Profiled the user on his laptop* → *specific training set*
  - *Ground truth disclosure, e.g., a short chat message*

- *(Laptop-)Model Profiling Scenario*
  - *Profiled a laptop of the same model on some users*
  - *Victim is/can be unknown!*
Complete Profiling

Training set with the data the user disclosed

Hunt&Peck typing, unfiltered data

Touch typing, Skype filtered data
Complete Profiling

Is only Skype vulnerable to our attack?

No! It looks like a common problem for VoIP software
On the Model Profiling Scenario, the victim can be unknown

*Someone the attacker does not know personally*

First need to understand the laptop of the victim

→ match it with a database of model signatures

- Guess correctly 93% of the times if the model is known
- Statistical measures if the model is unknown
(Laptop-)Model Profiling

One user

“Crowd” of multiple users

![Graph showing accuracy vs. number of guesses for different models and strategies.](image-url)
Summing Up Our Results

- Recognize a single character
  - Complete Profiling: 90%+ accuracy
  - Model Profiling: 40%+ accuracy

- Recognize a single word
  - Complete Profiling: 98% correct letters
  - Model Profiling: 50% correct letters

- Recognize a random password
  - Improves 1-5 orders of magnitude time needed to guess the password
  - From 50 days to 42 seconds on a domestic PC
Countermeasures

- **Don’t Skype & Type**

- Remove volume when we detect a keypress sound
  - *Impacts voice, greatly degrades call quality*

- Disrupt spectral features with random equalization
  - *Assess impact on voice, real time feasibility*
Conclusions & Future Work

- VoIP Keyboard acoustic eavesdropping a serious threat

- Feasible and accurate:
  - Realistic attack scenarios
  - 91.71% on Complete Profiling scenario
    - Halevi (2012; 2014): 85.78%
  - 41.89% on Model Profiling scenario
    - Novel attack vs. unknown victims
  - Robust to degradation and to voice

- Future work:
  - Try more users and different keyboards, and on more VoIP software
  - Try to attack another user in the same room
  - Analyze and improve the countermeasures
Conclusions & Future Work

- VoIP Keyboard acoustic eavesdropping a serious threat

- Feasible and accurate:
  - Realistic attack scenarios
  - 91.71% on Complete Profiling scenario
    - Halevi (2012; 2014): 85.78%
  - 41.89% on Model Profiling scenario
    - Novel attack vs. unknown victims
  - Robust to degradation and to voice

- Future work:
  - Try more users and different keyboards, and on more VoIP software
  - Try to attack another user in the same room
  - Analyze and improve the countermeasures
Does it really work?

vs Forbes, 1984 & the Bible

[Image of a person using a laptop with text on the screen: he had won the victory over himself he loved big brother]

Embrace

[Image of a laptop with text: Well, 'embrace'.]

Thank you!

Questions?
(if you do not have one, please find some suggestions below)
This is the END!

Backup Slides after this point... ;-)
From: Sadeghi, Ahmad-Reza <ahmad.sadeghi@trust.informatik.tu-darmstadt.de>  
To: manuel@atug.de <manuel@atug.de>, Lejla Batina <lejla@cs.ru.nl>  
Cc: Kleffel, Petra <petra.kleffel@tu-darmstadt.de>  
Subject: Your talks arrangement  

Dear Speakers,  

We assumed that most of you want to use your own laptops during your talk. Please get ready short before your talk and prepare possible adaptors so that we do not loose much time when switching laptops.  

In case you would use our laptop, we need an USB stick with your slides on it.  

Best  
Ahmad
Adversarial Machine Learning

Adversarial Examples (Deep Learning/CNNs)

Original image classified as a panda with 60% confidence. Tiny adversarial perturbation. Imperceptibly modified image, classified as a gibbon with 99% confidence.

http://karpathy.github.io/2015/03/30/breaking-convnets/
Classification Accuracy

Classification Accuracy is what we usually mean, when we use the term accuracy. It is the ratio of number of correct predictions to the total number of input samples.

\[
\text{Accuracy} = \frac{\text{Number of Correct predictions}}{\text{Total number of predictions made}}
\]

It works well only if there are equal number of samples belonging to each class.

For example, consider that there are 98% samples of class A and 2% samples of class B in our training set. Then our model can easily get 98% training accuracy by simply predicting every training sample belonging to class A.

When the same model is tested on a test set with 60% samples of class A and 40% samples of class B, then the test accuracy would drop down to 60%. Classification Accuracy is great, but gives us the false sense of achieving high accuracy.
Machine Learning 101

- Precision, Recall, and F-measure

\[
F_1 = 2 \cdot \frac{\text{recall}}{\frac{1}{\text{recall}} + \frac{1}{\text{precision}}} = 2 \cdot \frac{\text{precision} \cdot \text{recall}}{\text{precision} + \text{recall}}
\]

\[
F_\beta = \frac{(1 + \beta^2) \cdot \text{true positive}}{(1 + \beta^2) \cdot \text{true positive} + \beta^2 \cdot \text{false negative} + \text{false positive}}
\]
Attack - Data Processing

- Data windowing and segmentation
  
  *To extract sound samples*

- Feature extraction: *mel frequency cepstral coefficients*
  
  *Selected with a preliminary experiment*
Novelty - Attack Scenarios

Evaluate the attack on three different realistic scenarios

- **Complete Profiling Scenario** (Asonov, 2004; Halevi, 2012; 2014)
  - Profiled the user on his laptop → specific training set
  - Ground truth disclosure, e.g., a short chat message

- **User Profiling Scenario**
  - Profiled the user on a different laptop
  - Social engineering techniques

- **Model Profiling Scenario**
  - Profiled a laptop of the same model on some users
  - The victim can be unknown
10 samples/character aren’t your typical chat message

Training set with realistic letter frequencies
Test against random password

<table>
<thead>
<tr>
<th>Character</th>
<th># Samples</th>
</tr>
</thead>
<tbody>
<tr>
<td>E</td>
<td>10</td>
</tr>
<tr>
<td>A</td>
<td>9</td>
</tr>
<tr>
<td>R</td>
<td>7</td>
</tr>
<tr>
<td>J</td>
<td>1</td>
</tr>
<tr>
<td>Z</td>
<td>1</td>
</tr>
</tbody>
</table>
Evaluation - User Profiling

Accuracy

Number of guesses

0% 20% 40% 60% 80% 100%

0 2 4 6 8 10

Random guess
Macbook Pro
Toshiba
Lenovo
Password Cracking

The goal was to crack the victim’s random password

→ We need brute-force techniques

Random password of 10 lowercase letters

- \( \log_2(26^{10}) = 47 \) bits of entropy

On the Complete Profiling Scenario (high accuracy)

- \( \log_2(5^{10}) = 23.22 \) bits of entropy

On the other scenarios - entropy is not meaningful
Password Cracking

Model Profiling Scenario → improved bruteforce

*Take into account character probabilities*

Evaluate the reduction of the average number of trials
Features

**Fast Fourier Transform coefficients**

\[ S(f(t)) = 20 \log_{10}(|\mathcal{F}(f(t))|) \]

\( f(t) = \text{signal} \)
\( \mathcal{F} = \text{Discrete Fourier Transform function} \)

**Cepstrum coefficients**

\[ C(f(t)) = |\mathcal{F}^{-1}(S(f(t)))|^2 \]

**Mel frequency cepstral coefficients**

\[ MFC(f(t)) = DCT(\log_{10}(mel\{|\mathcal{F}(f(t))|\})) \]

\[ mel(f) = 2595 \log_{10} \left( 1 + \frac{f}{700} \right) \]

\( DCT = \text{Discrete Cosine Transform} \)
Side and Covert Channels: the Dr. Jekyll and Mr Hyde of Modern Technologies

Mauro Conti

2020 WiseML @ WiSec
July 13 2020