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

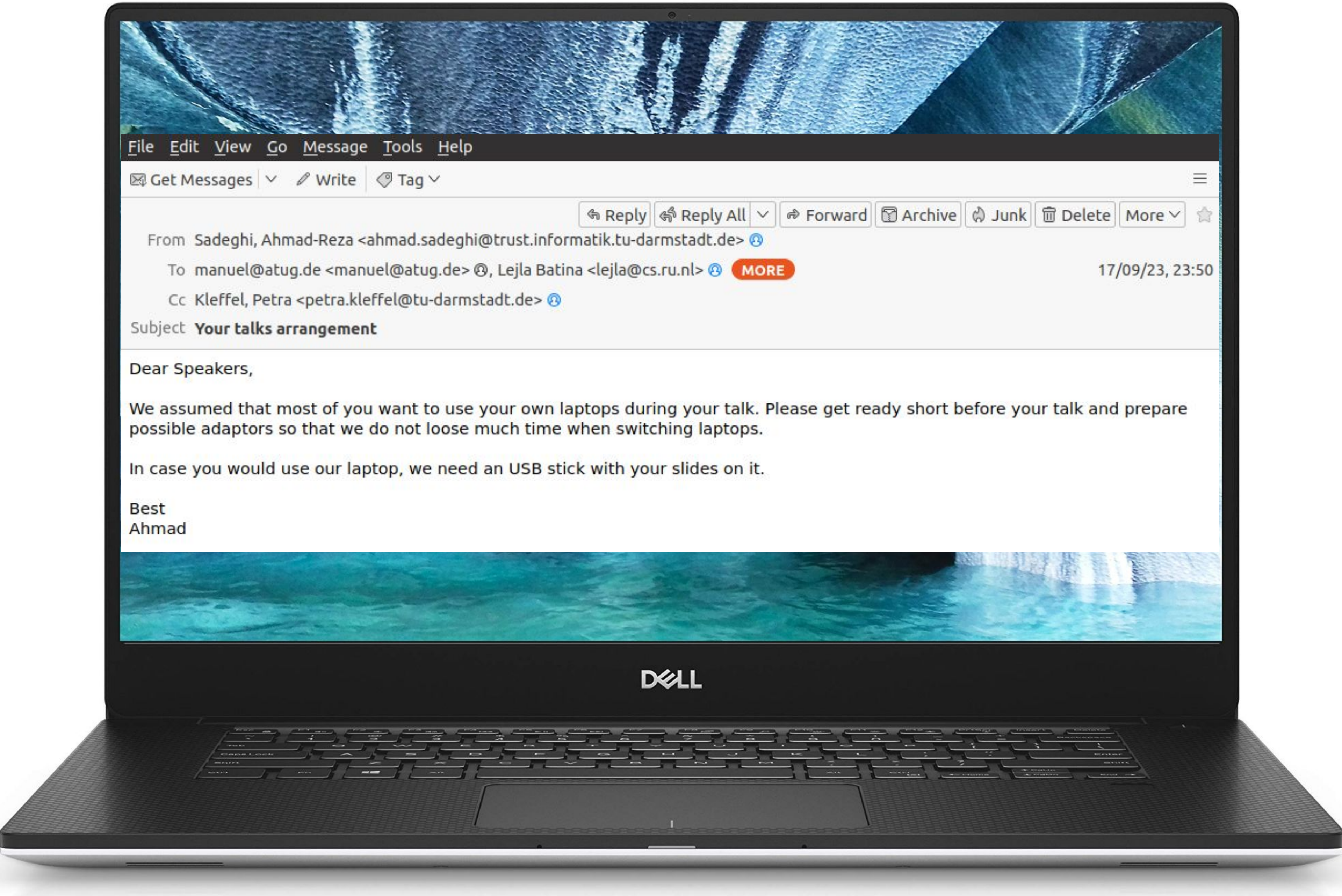
Mauro Conti

CROSSING

Funded by
DFG Deutsche Forschungsgemeinschaft
German Research Foundation

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

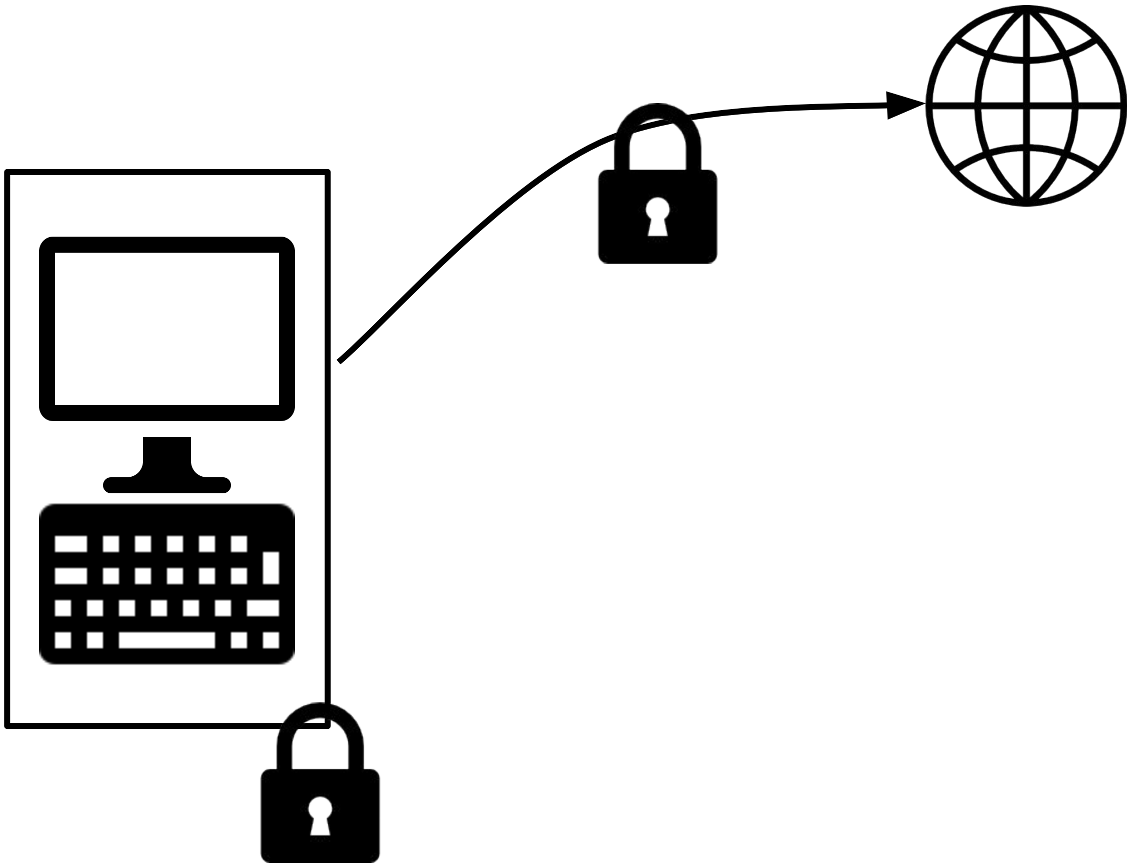

File Edit View Go Message Tools Help
Get Messages
Write
Tag
Reply
Reply All
Forward
Archive
Junk
Delete
More
From Sadeghi, Ahmad-Reza <ahmad.sadeghi@trust.informatik.tu-darmstadt.de>
To manuel@atug.de <manuel@atug.de>, Lejla Batina <lejla@cs.ru.nl>
MORE
17/09/23, 23:50
Cc Kleffel, Petra <petra.kleffel@tu-darmstadt.de>
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
DELL


DELL


SAFUEL
FAST CHARGE

Side Channels

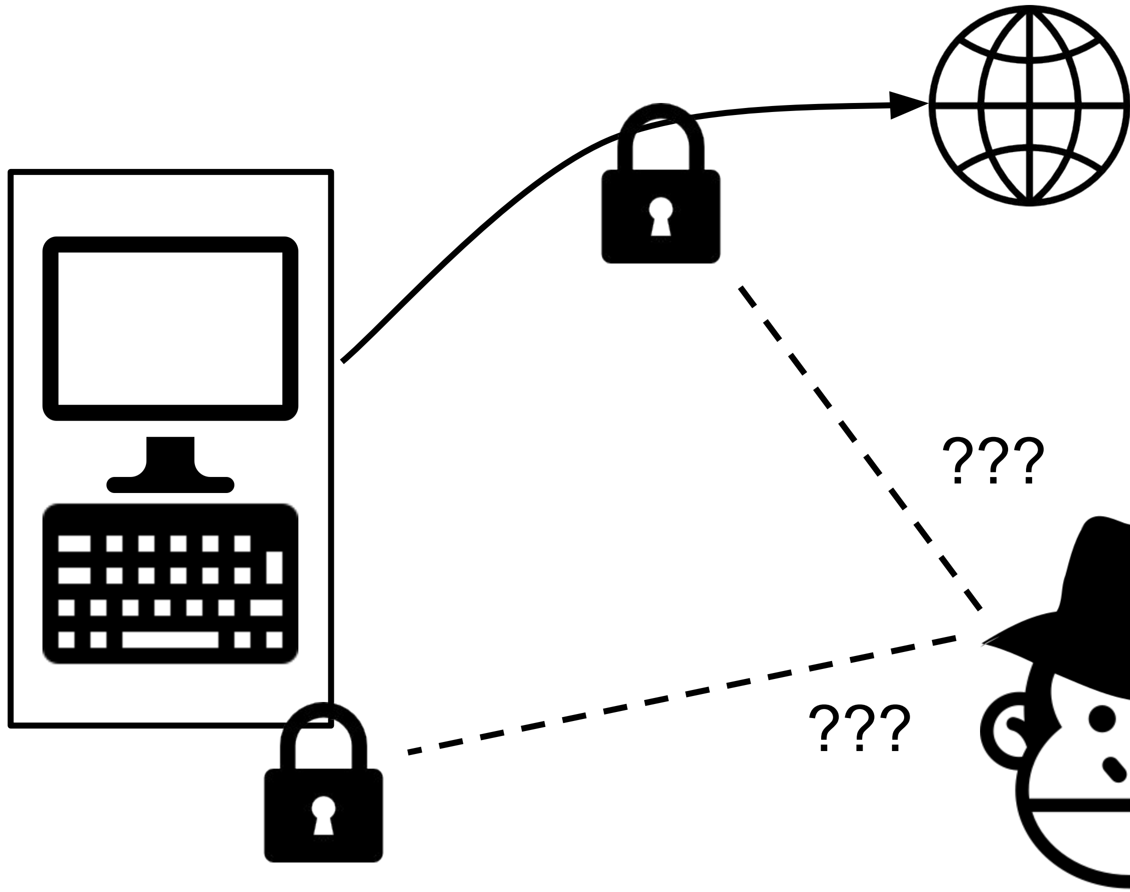
Devices, and network communication, are usually **protected** and **encrypted**



Side Channels

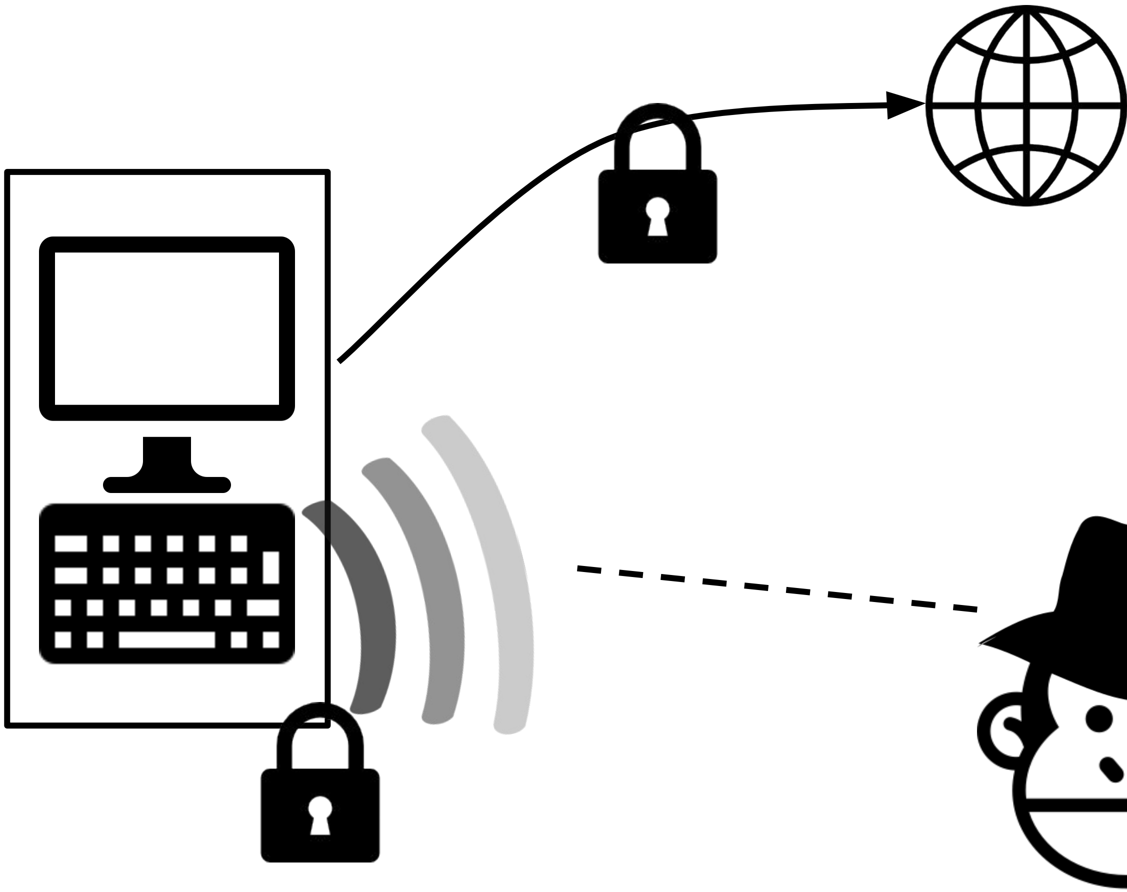
Devices, and network communication, are usually **protected** and **encrypted**

→ Difficult for **Attackers** to violate such protecion



SPRITZ
Security & Privacy
Research Group
Università
degli Studi
di Padova

Side Channels



Observing emanations and patterns

Can reveal secrets!

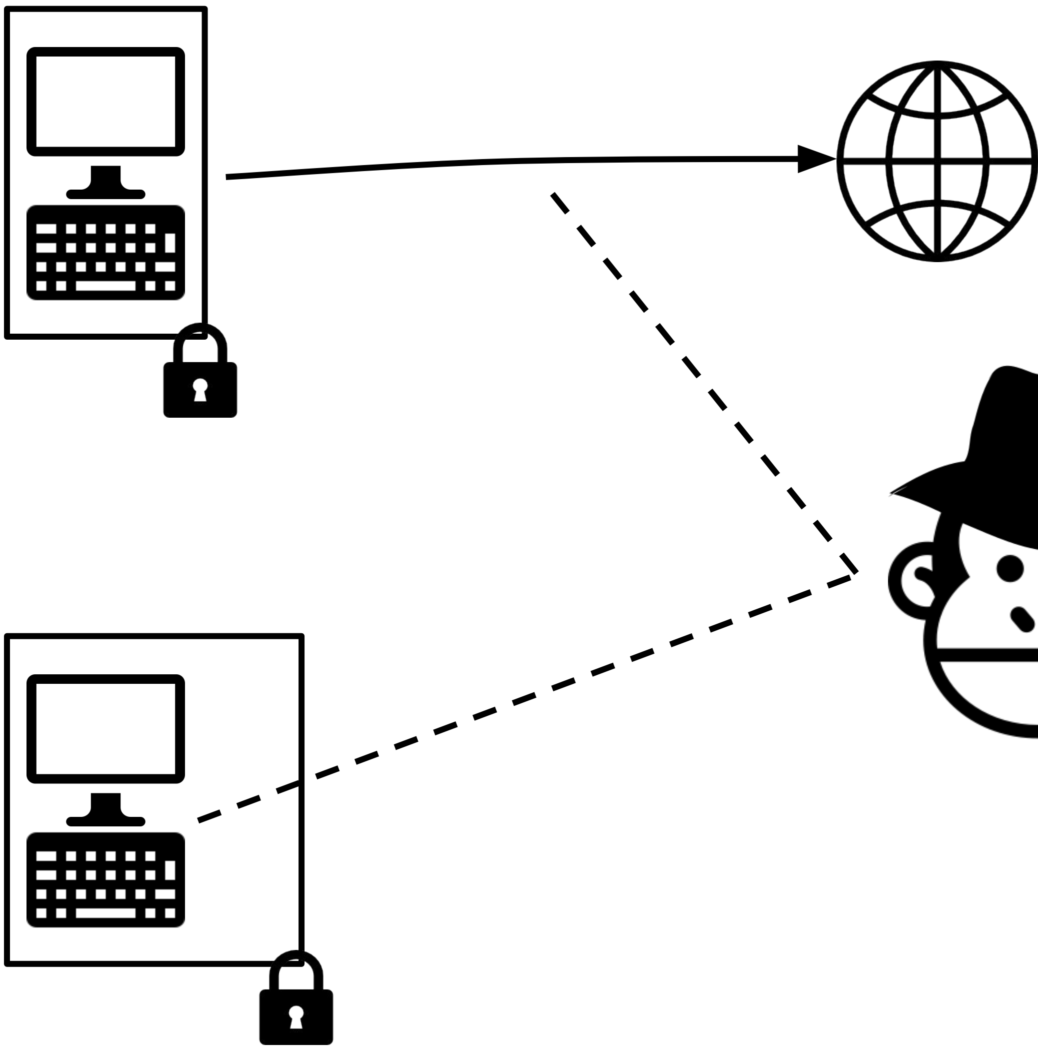
This is called a **side channel**

Covert Channels

Covert Channels are used to communicate stealthily.

Either to **avoid listeners in the middle**...

...or to exfiltrate information.




DELL

M. Conti, M. Nati, E. Rotundo, R. Spolaor.

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

In ACM AsiaCCS 2016 workshop IoTPTS 2016

Power Consumption Side Channel

SPRITZ
Security & Privacy
Research Group

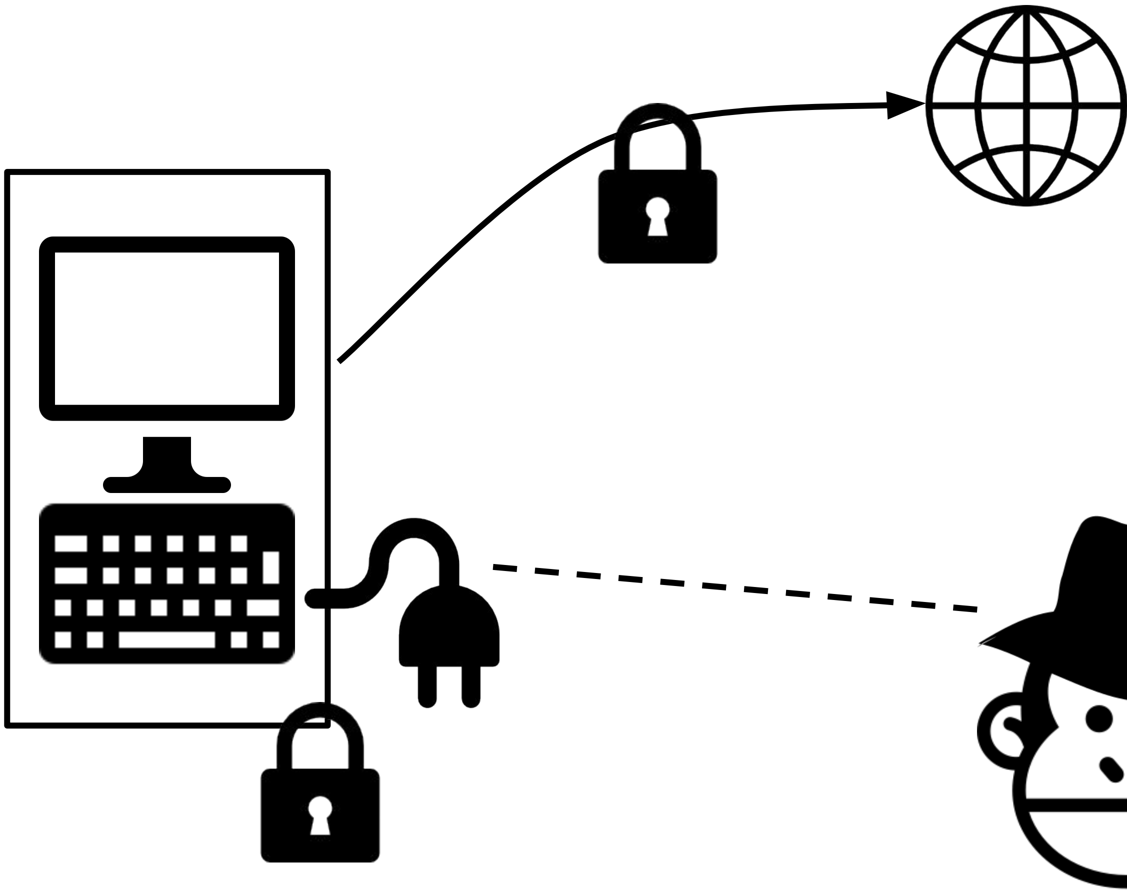
Università
degli Studi
di Padova

Power consumption

Can reveal what we are doing!

Device drains different power depending on our actions

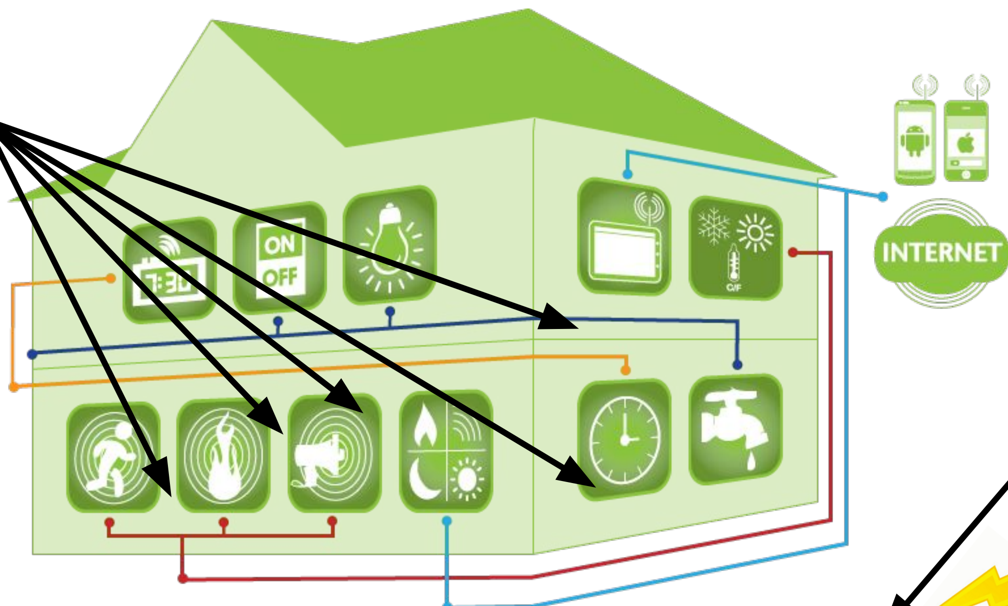
Works on **laptops** and **mobile**



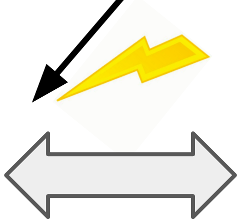
Smartbuilding

Internet of Things applied not only to industry, but also to buildings, such as houses and **offices**

Wall-socket level sensors



household level sensors



Smartgrid

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 **<u>1Hz</u>** of sampling rate

Definition of "Laptop-User"

A **Laptop-user** is made of the **combination** of:

- Laptop
- Software installed and running
- User behavior

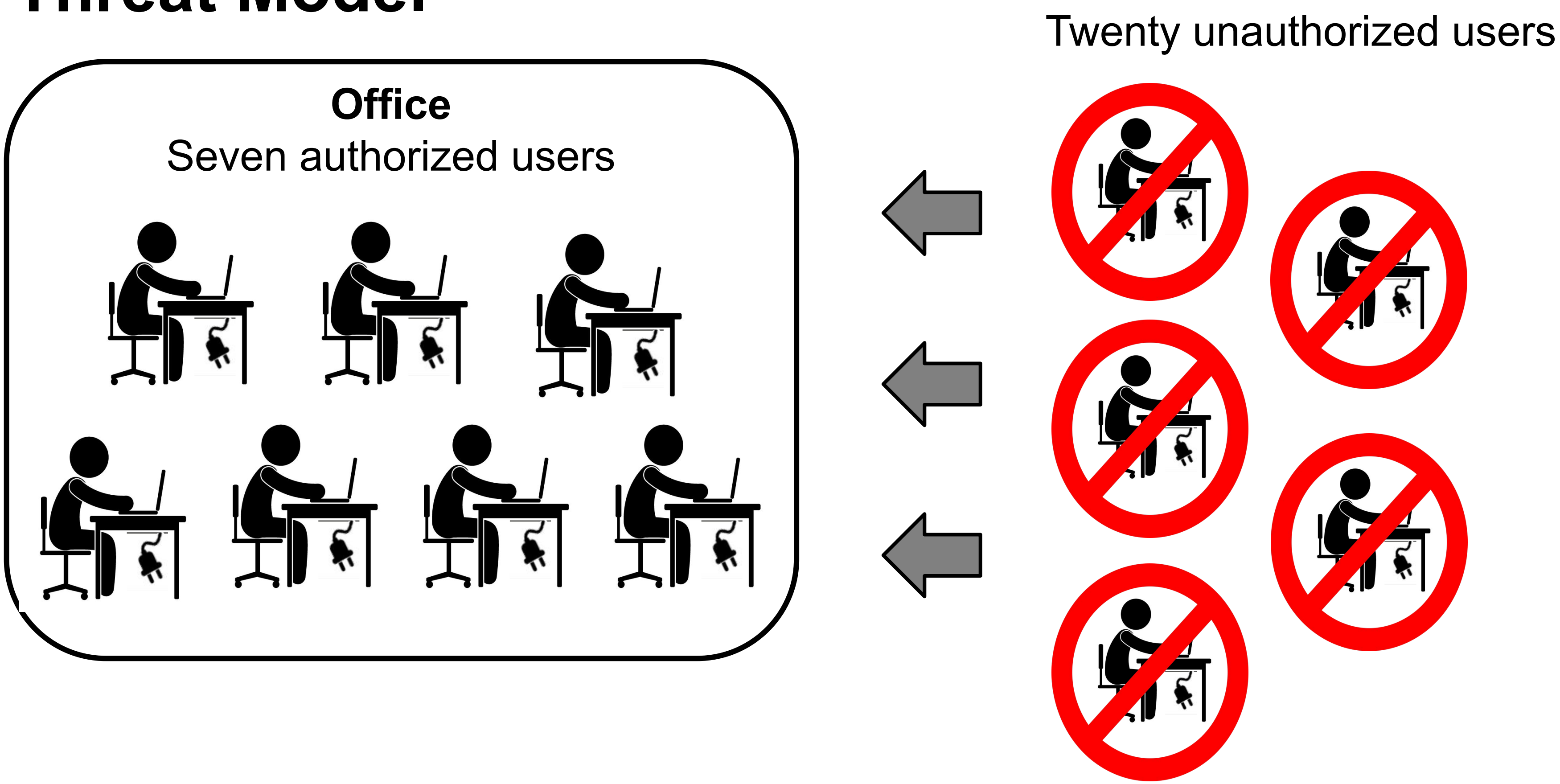
Goal & Motivation

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

Threat Model



We aim to:

- Recognize whether the user is in the “authorized” set
- Identify the specific user in the “authorized” set

Mind the Plug! (IoTPTS @AsiaCCS '16)

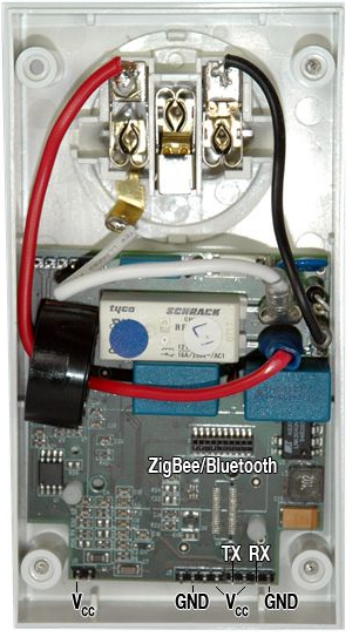
SPRITZ
Security & Privacy
Research Group

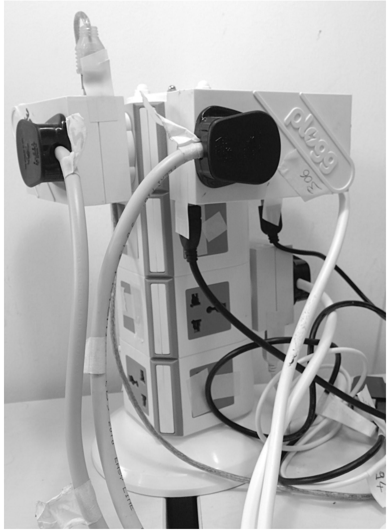
Università
degli Studi
di Padova

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**

Mind the Plug! (IoTPTS @AsiaCCS '16)

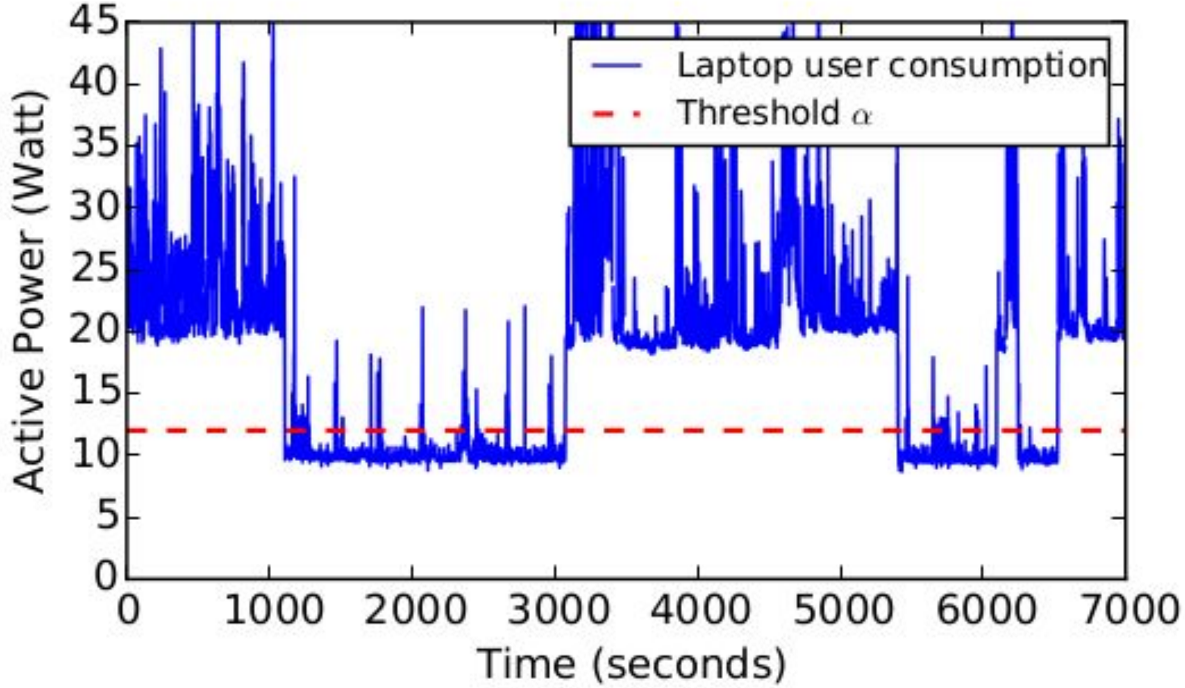
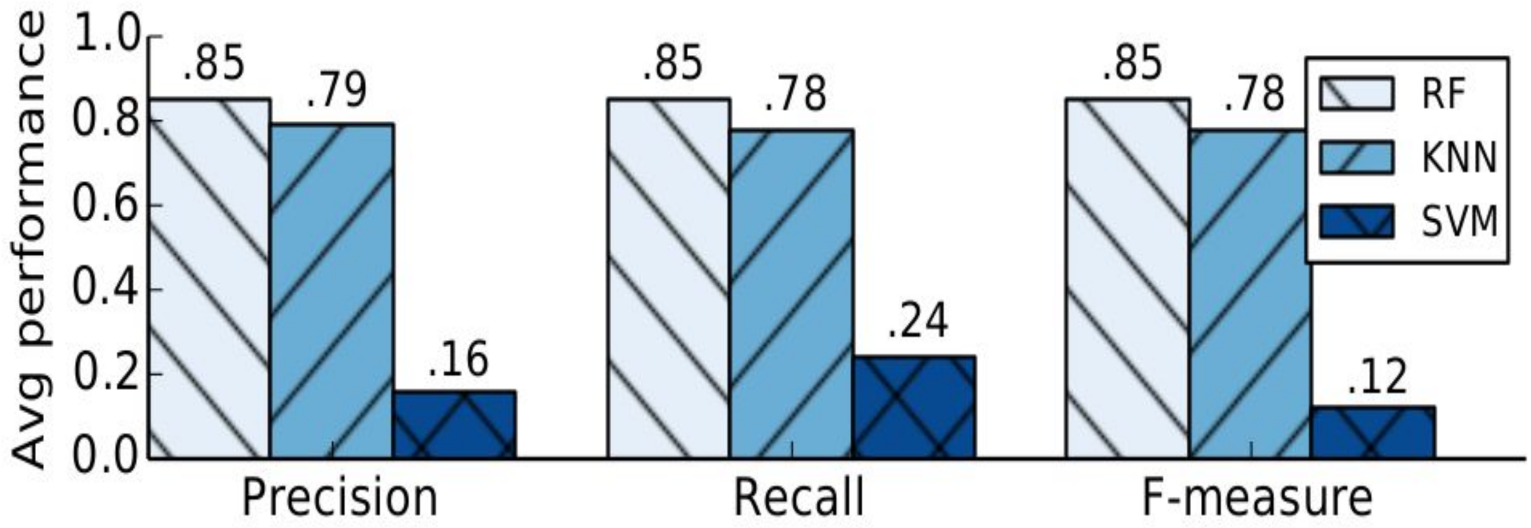


Figure 2: Example of *Active Power* trace (continuous blue line) and the lower-cutting threshold $\alpha = 12$ Watt (dashed red line). Samples under α are low-energy timespans in which the user does not use the laptop.

Mind the Plug! (IoTPTS @AsiaCCS '16)



85% of F-measure with Random Forest classifier

Classification validation

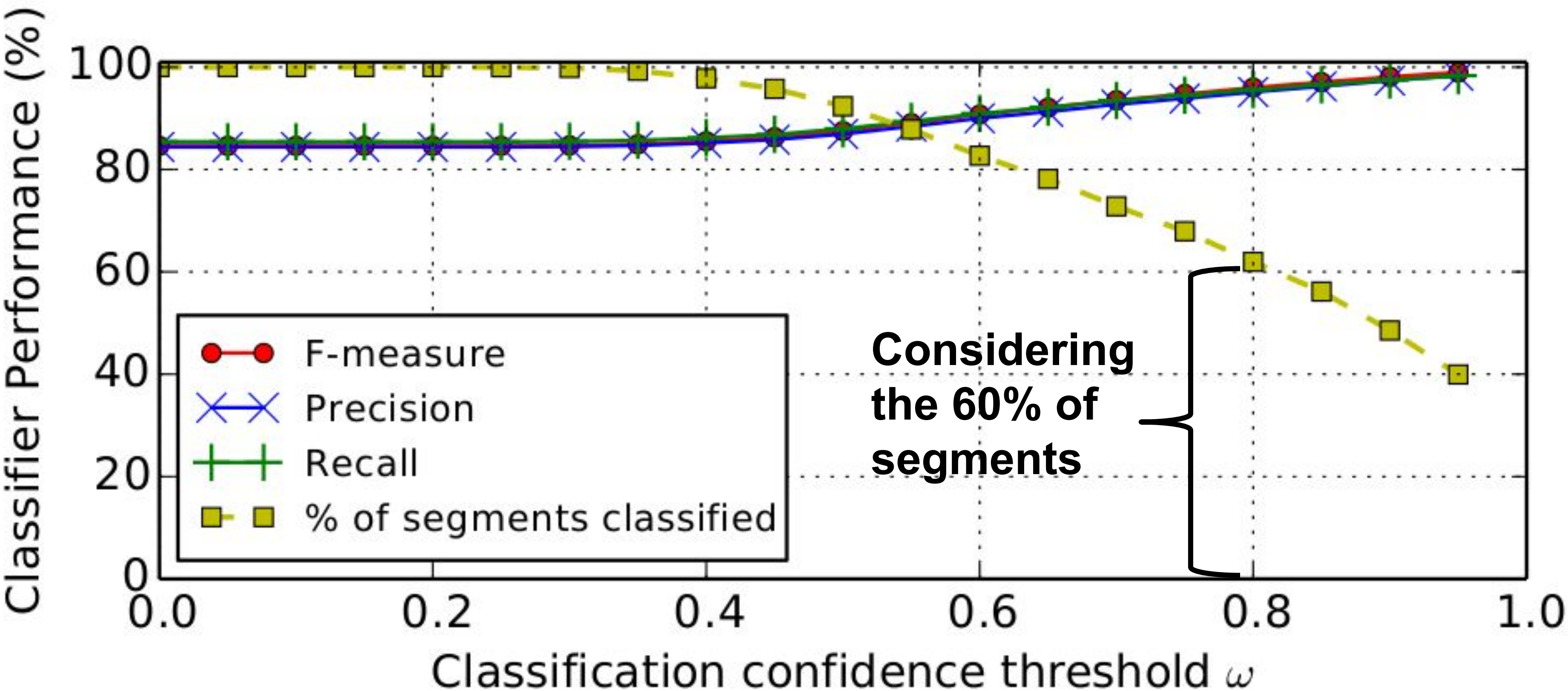
Classifiers label all segments in the testset
- Bad for False Positive rate (FPR)

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

Classification validation results



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


DELL


SAFUEL
FAST CHARGE
%00

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

SPRITZ
Security & Privacy
Research Group

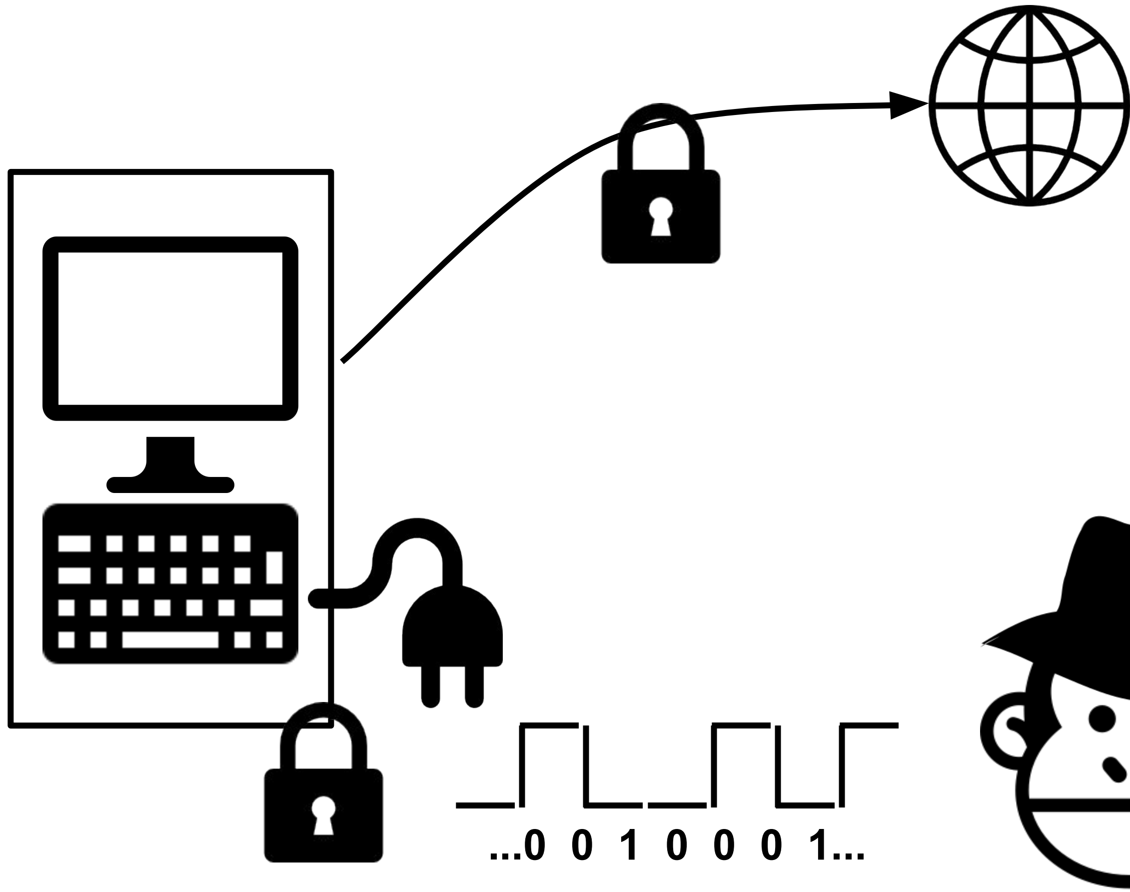
Università
degli Studi
di Padova

Power consumption

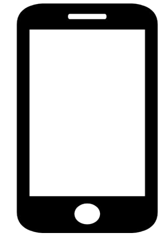
Can be used as a covert channel

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



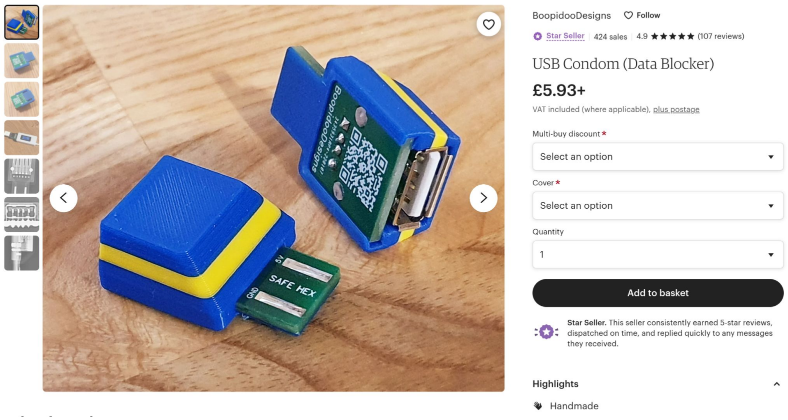
USB protection...

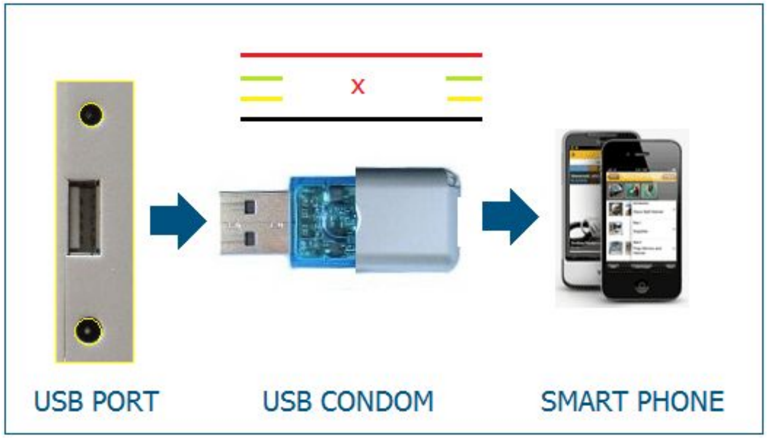
Protect your data

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.

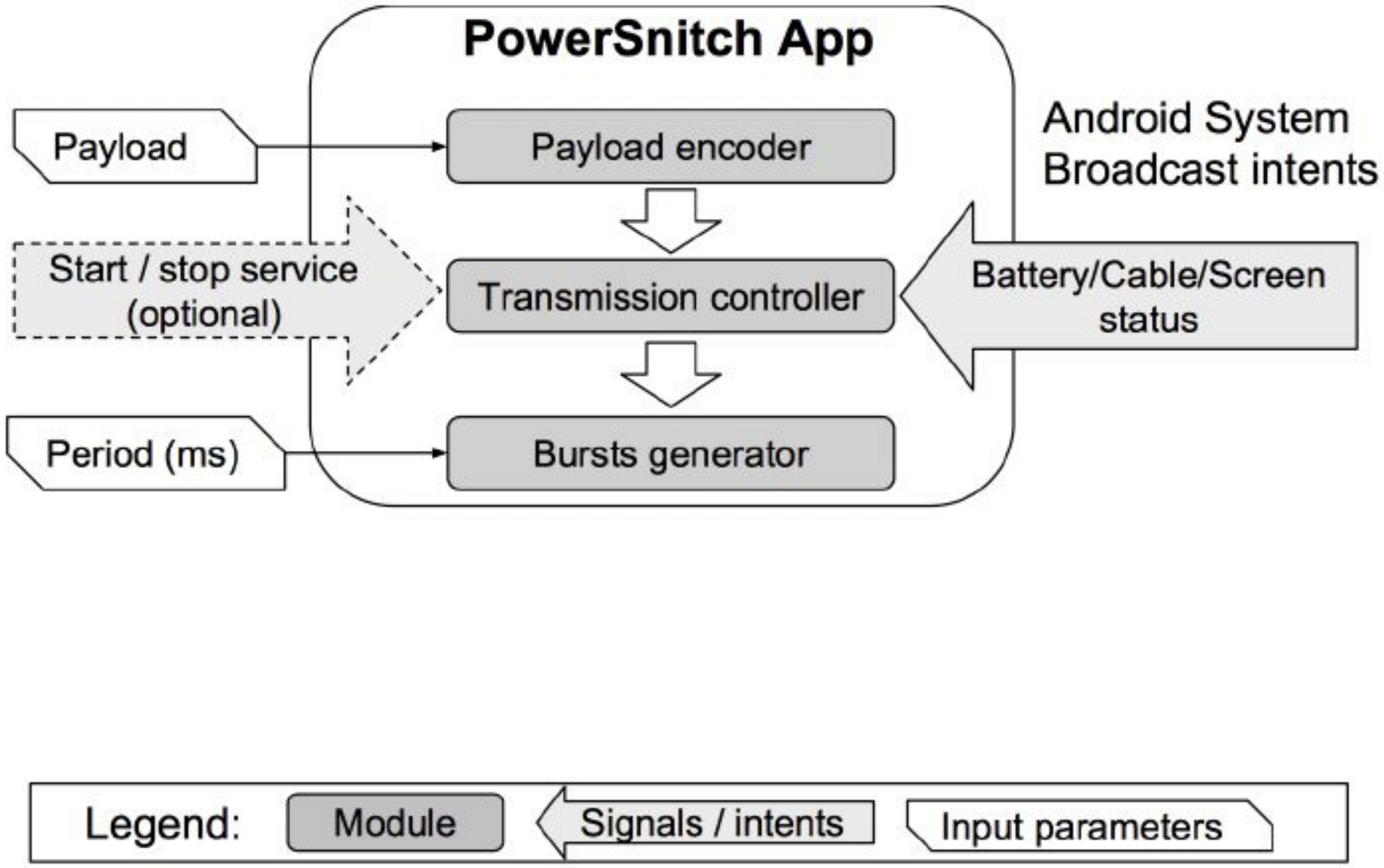
SyncStop is the 'cased' version of the original USB Condom. We listened and spent some time designing and manufacturing our own enclosure.

SyncStop works with any mobile device:

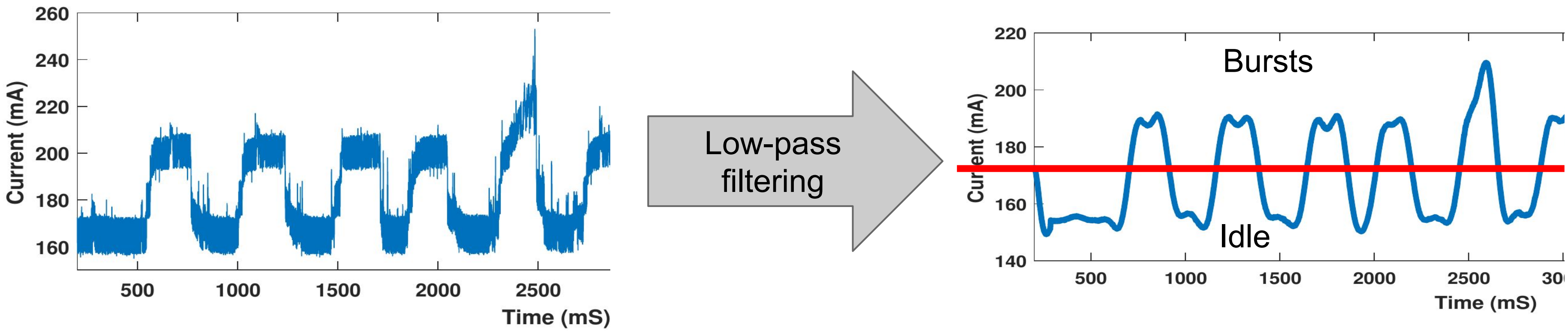




PowerSnitch Application

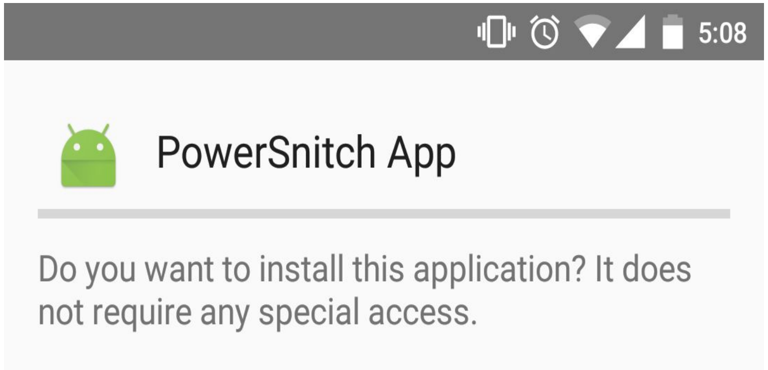


No Free Charge Theorem: a Covert Channel via USB Charging Cable on Mobile Devices



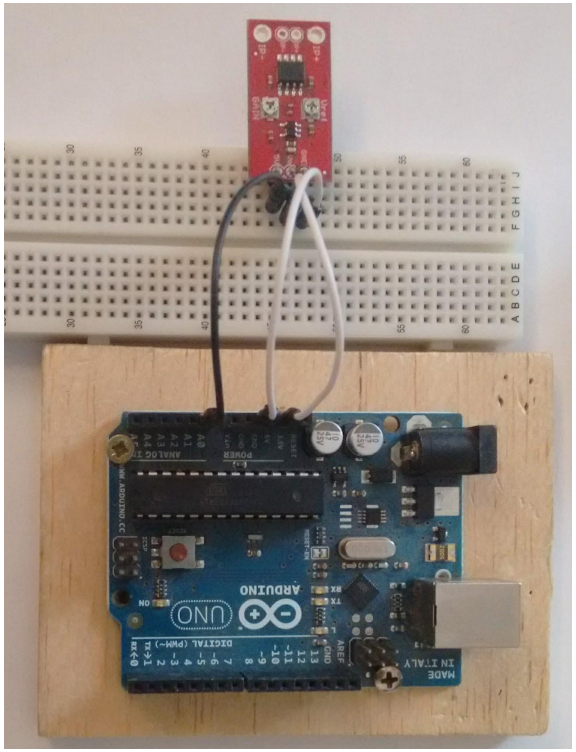
Results in terms of Bit Error Ratio (BER)

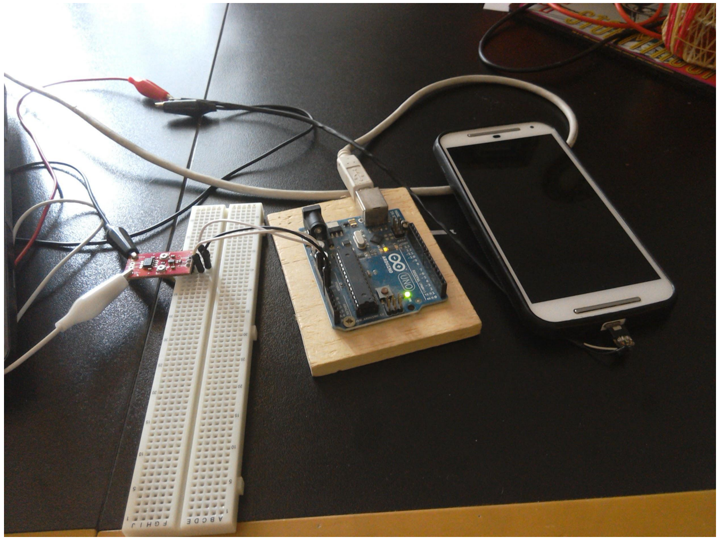
Device	Period (milliseconds)					
	1000	900	800	700	600	500
Nexus 4	13.5	0.78	0.0	0.0	13.33	16.21
Nexus 5	21.0	0.0	0.95	36.82	40.35	13.4
Nexus 6	1.07	0.0	0.21	0.0	4.05	7.42
Samsung S5	12.5	13.5	13.31	16.33	17.9	21.42

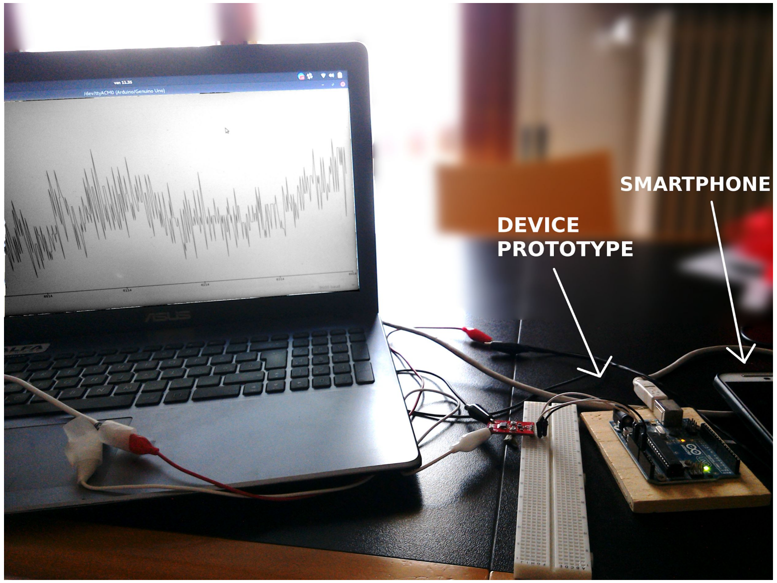


PowerSnitch app does not require any permission !!!

Power Bank Prototype







Power Bank - DEMO TIME

https://drive.google.com/file/d/1JXzoyOM3xpQqaM8exWF07htp67G5m82v/view?usp=sharing


DELL

F. Marchiori, M. Conti

Your Battery Is a Blast!
Safeguarding Against Counterfeit Batteries with Authentication

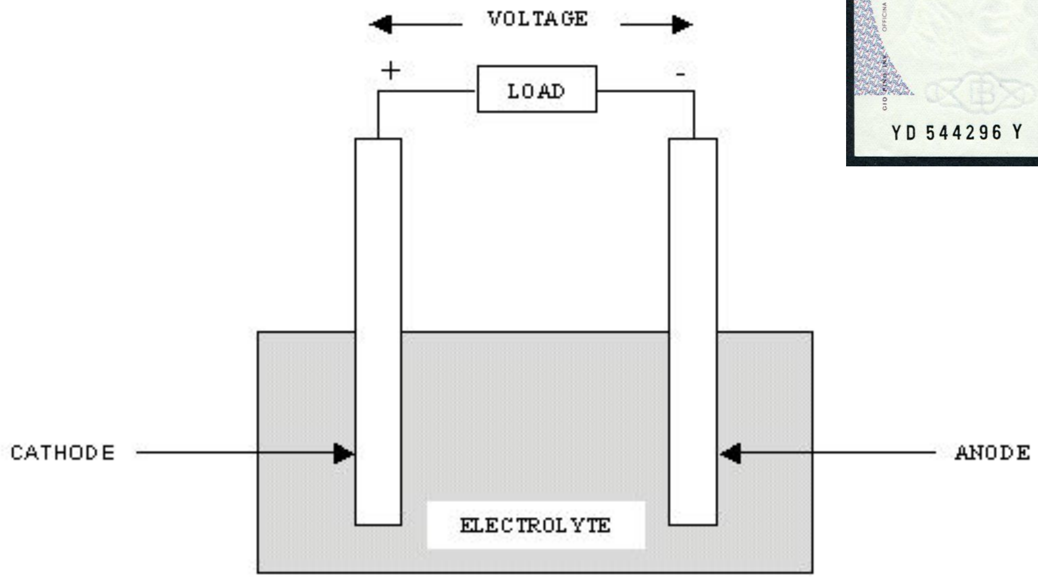
In ACM Conference on Computer and Communications Security (CCS' 23)

Battery Authentication

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

Battery Authentication

- Store as chemical energy -> turned into electrical energy



Battery Authentication

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

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

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

Battery Authentication

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

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

	Attacks			
Method	**Cloning**	**Replay Attacks**	**Unscalability**	**Rewrapping**
Markings		✓	✓	
External Features		✓	✓	
Form Factor		✓	✓	
Resistor		✓	✓	
Chip	✓			
CR (in clear)	✓			
CR (encrypted)	✓	✓		
DCAuth	✓	✓	✓	✓
EISthentication	✓	✓	✓	✓

CR = Challenge and Response Protocols

Battery Authentication

Our **contribution**

DCAuth EISthentication

- 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

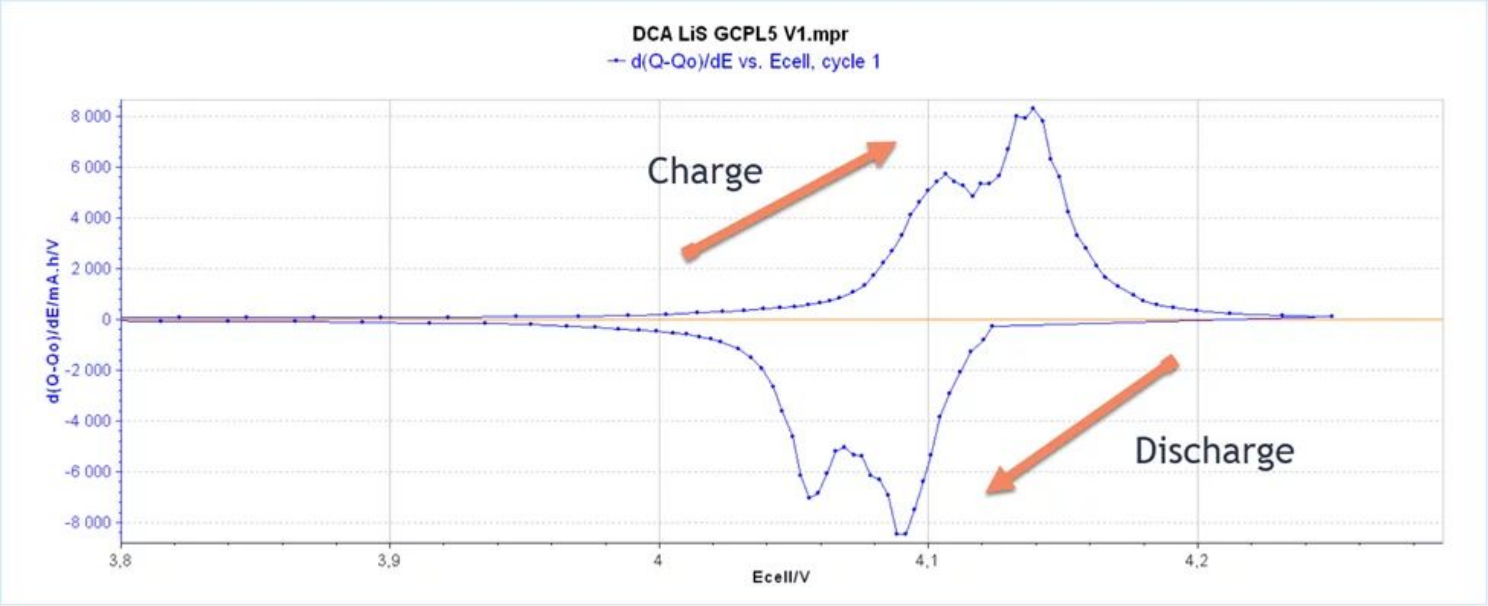
https://github.com/Mhackiori/EISthentication

SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

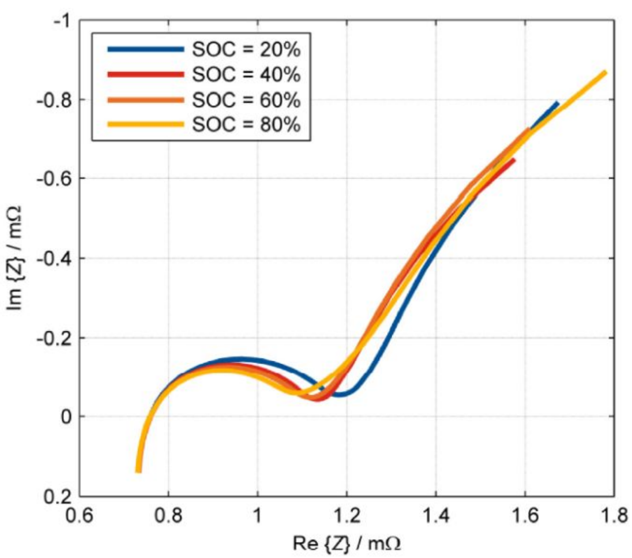
Differential Capacity Analysis (DCA)

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

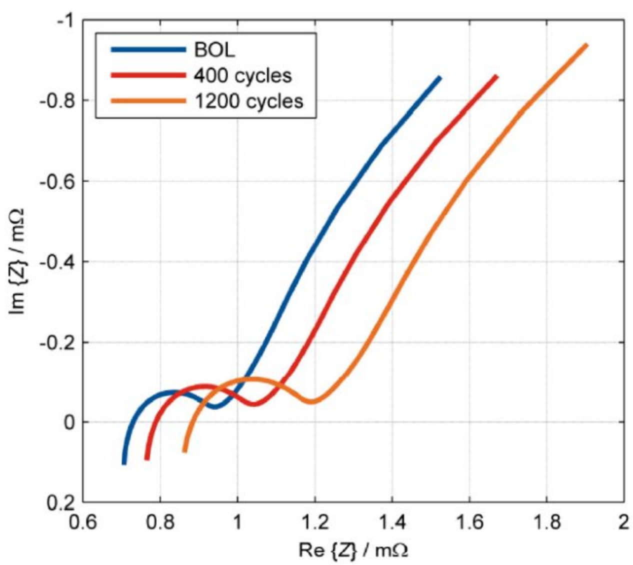


Electrochemical Impedance Spectroscopy (EIS)

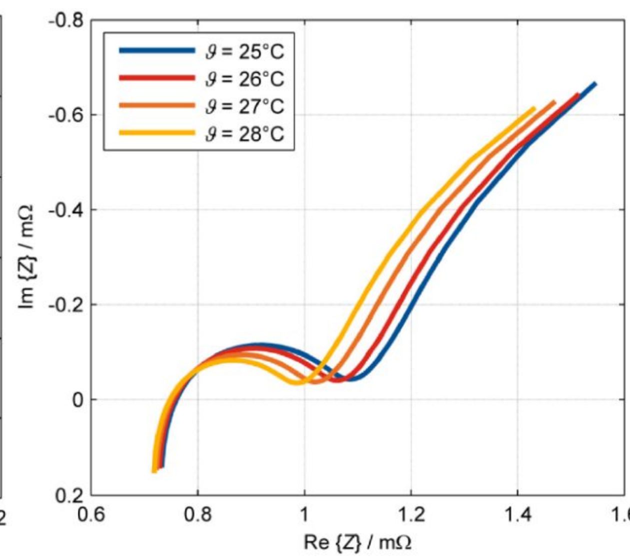
- Analytical technique for electrochemical system characterization
- Measures the electrical impedance
- Dependance on several environment/external factor



(a): Dependence on SOC.



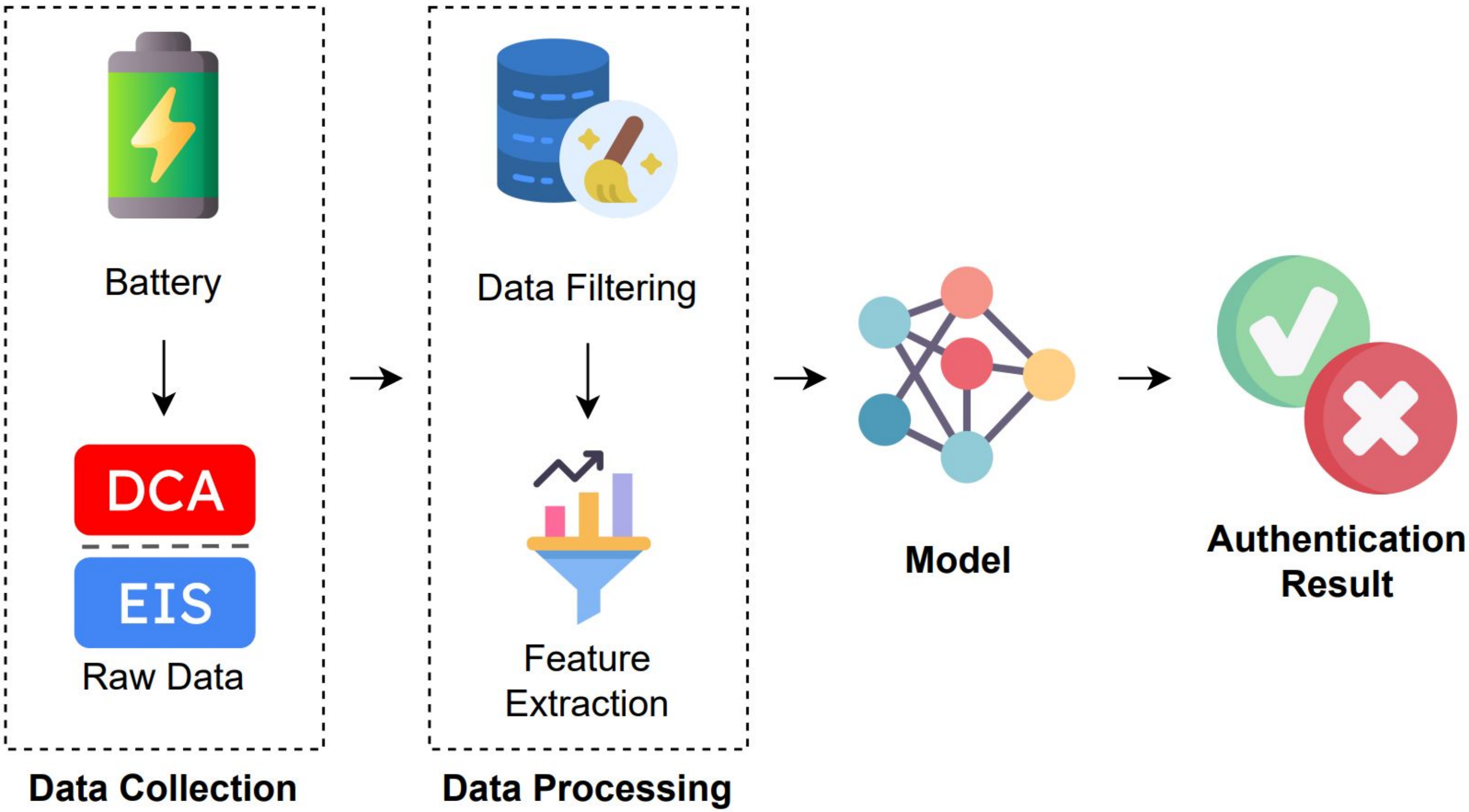
(b): Dependence on SOH.



(c): Dependence on temperature.

Battery Authentication

System Model

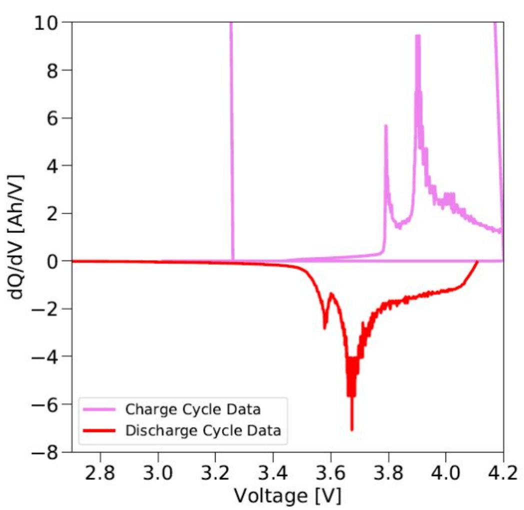


Battery Authentication

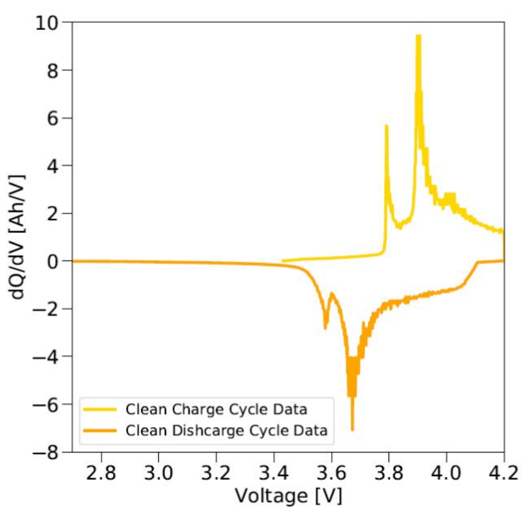
Datasets

- 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*

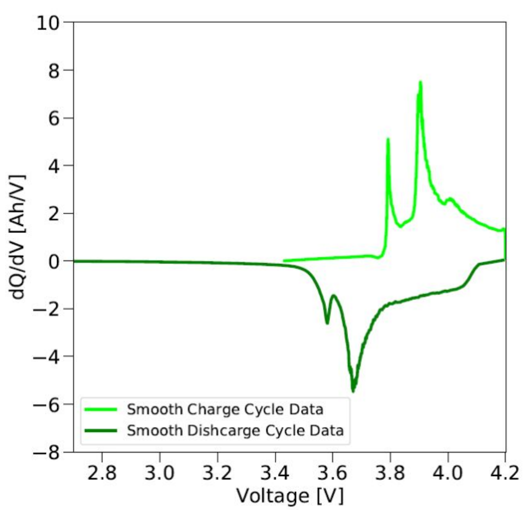
Processing (available on GitHub)



(a): Raw DCA plot.



(b): Clean DCA plot.



(c): Smooth DCA plot.

Battery Authentication

Models

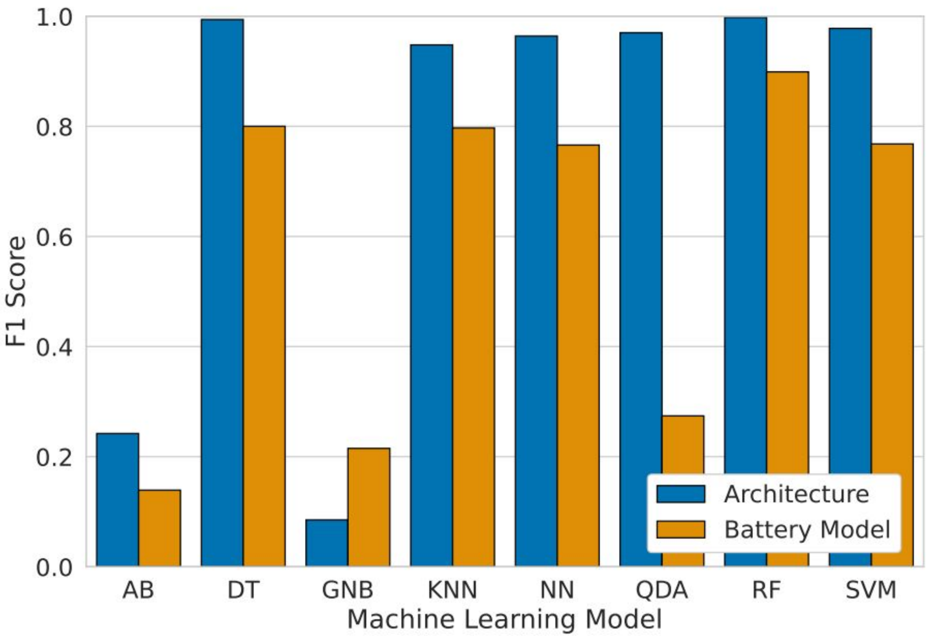
- Machine Learning
- Avoiding complex DL to keep low computational cost
- Commonly used in literature

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

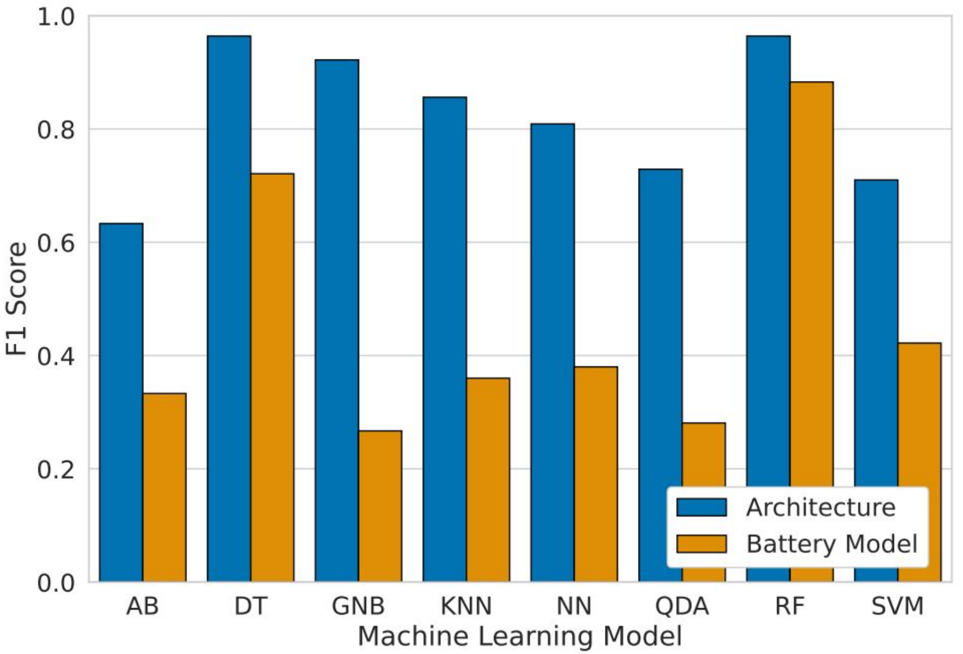
Evaluation Metrics

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

Results - Identification



DCAuth

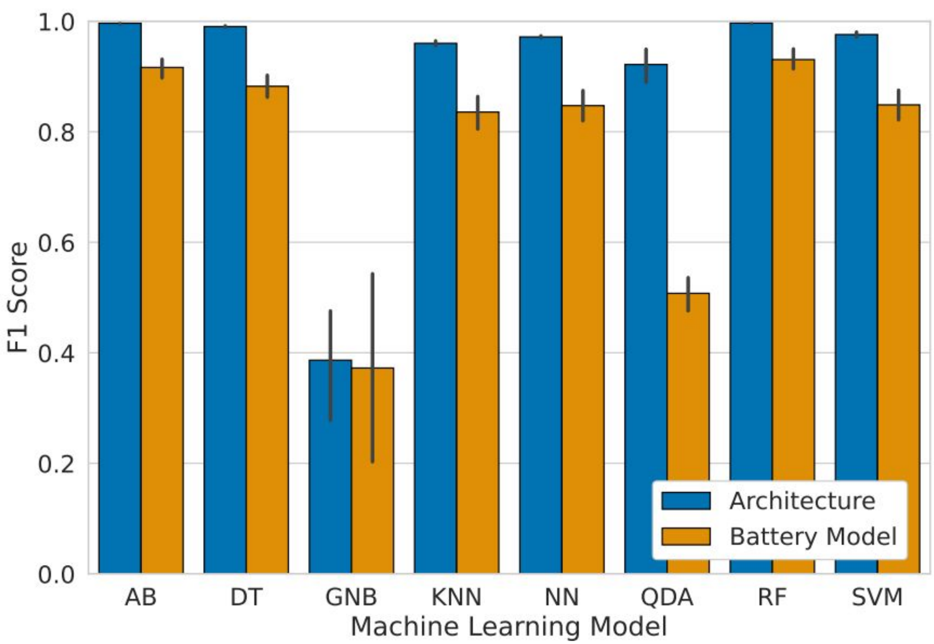


EISthentication

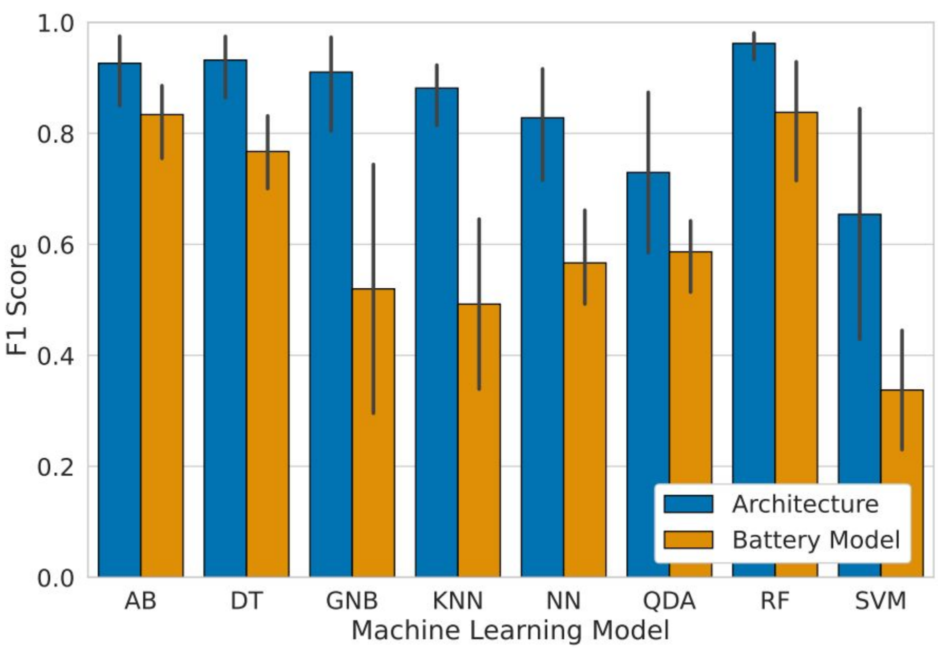
SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Results - Authentication



DCAuth

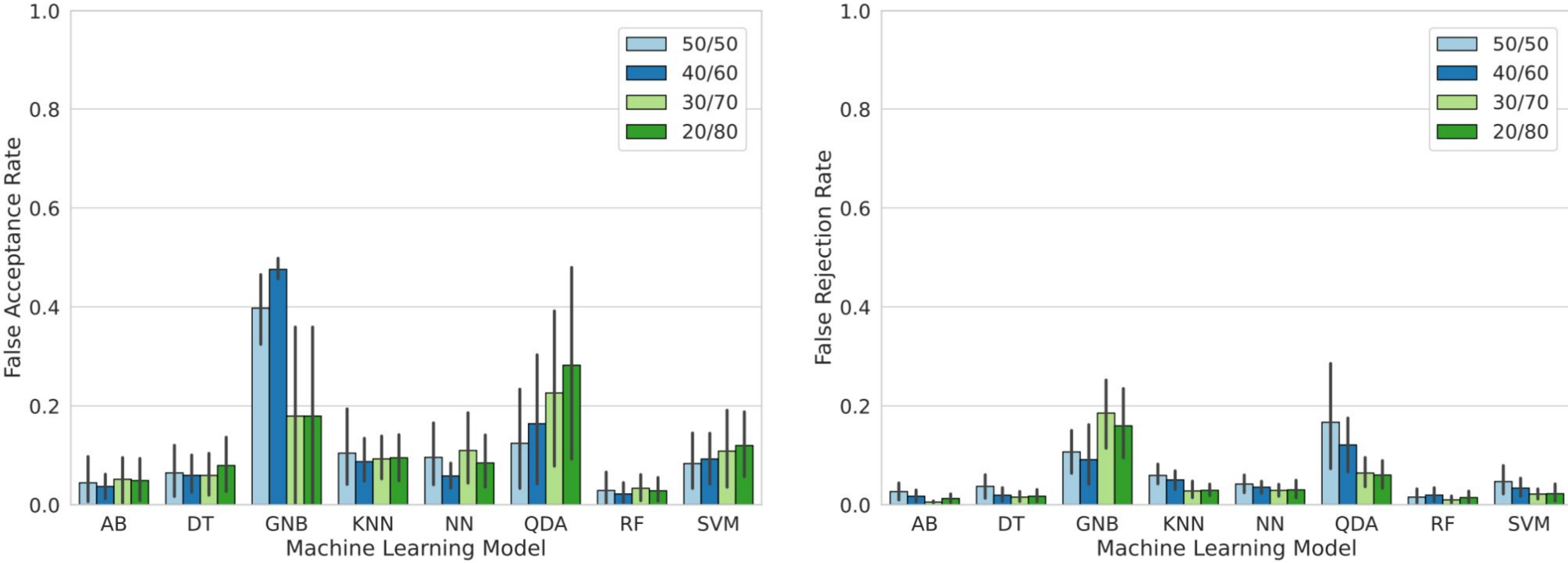


EISthentication

SPRITZ Security & Privacy Research Group

Università degli Studi di Padova

Results - FAR/FRR on Dataset Balance



DCAuth

Battery Authentication

Table 12: Complexity.

Model	Time_{DCA}	Size_{DCA}	Time_{EIS}	Size_{EIS}
AB	15.492 ms	75 kB	8.523 ms	59 kB
DT	3.892 ms	31 kB	2.881 ms	20 kB
GNB	4.687 ms	53 kB	3.192 ms	33 kB
KNN	12.951 ms	4800 kB	7.1 ms	263 kB
NN	4.595 ms	2600 kB	3.204 ms	1200 kB
QDA	7.856 ms	3100 kB	4.435 ms	271 kB
RF	13.661 ms	348 kB	13.288 ms	221 kB
SVM	9.854 ms	500 kB	2.99 ms	158 kB

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


DELL

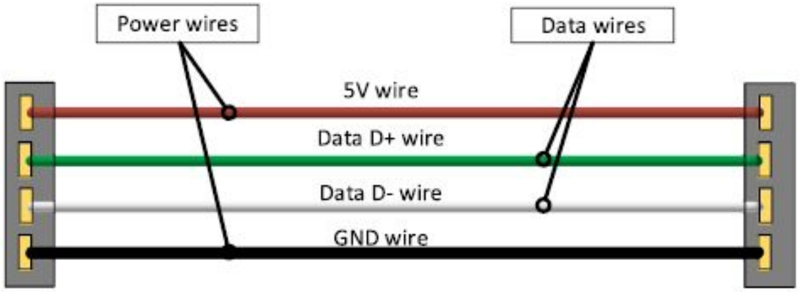
R. Spolaor, H. Liu, F. Turrin, M. Conti, X. Cheng

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

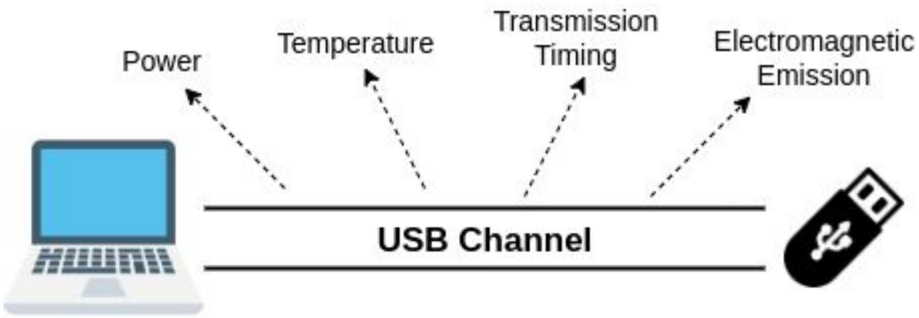


Idea

SPRITZ Security & Privacy Research Group — Università degli Studi di Padova

Exploit Power Side-Channel to identify <u>authorized devices</u>

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



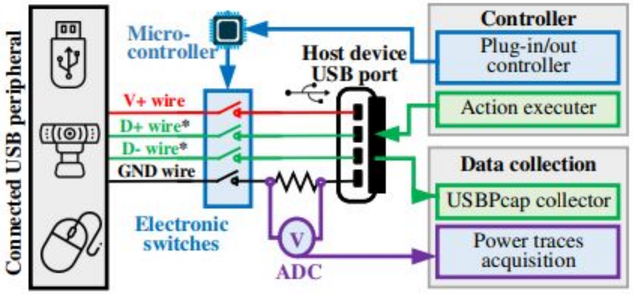
Use cases

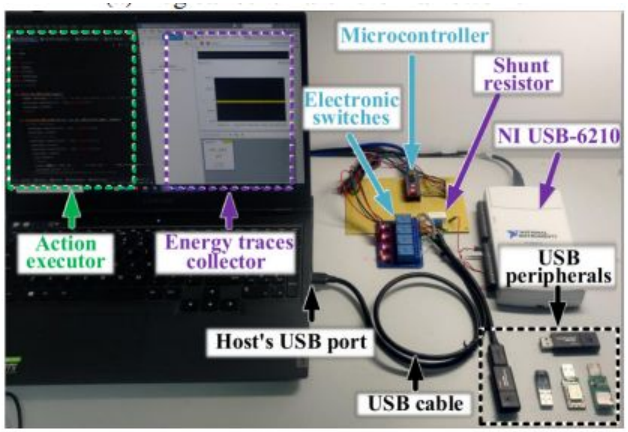
- End-user Personal Protection
- Organization Assets Protection

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



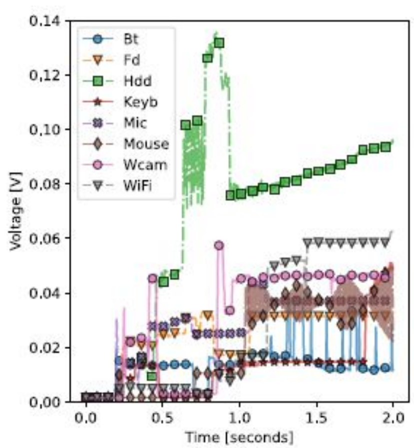


Analysis Goals

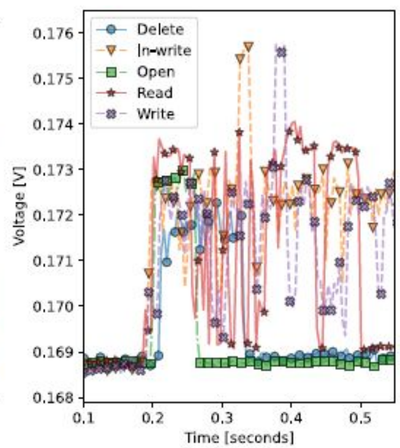
SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

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)



Boot



On

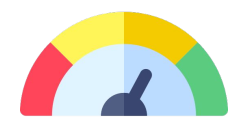
Pipeline

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

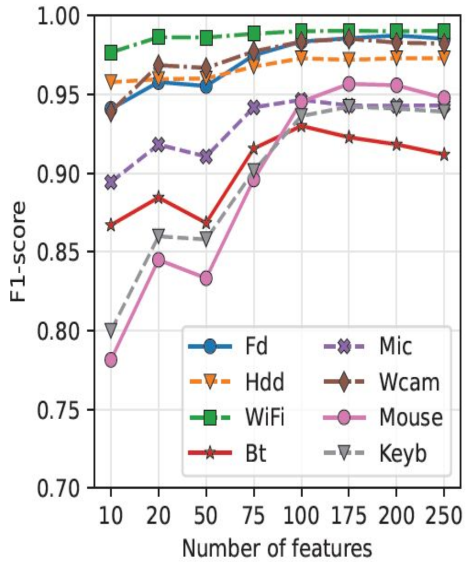
4) **Evaluation Metrics**: Precision, Recall, F1-Score, G-Mean, AUC



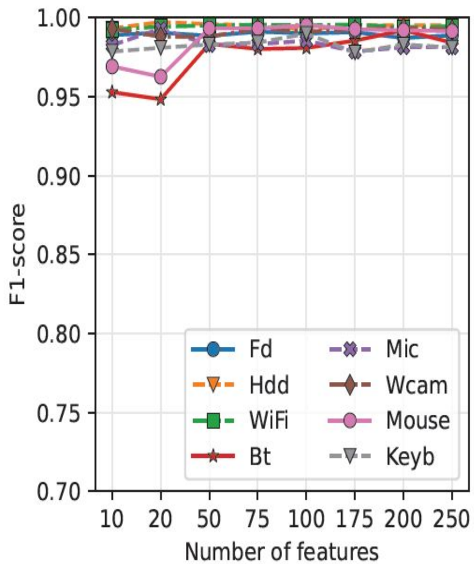
Type Recognition - Results (1/6)

- 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

State Boot



State On



We can discriminate USB type for *Boot* and *On*

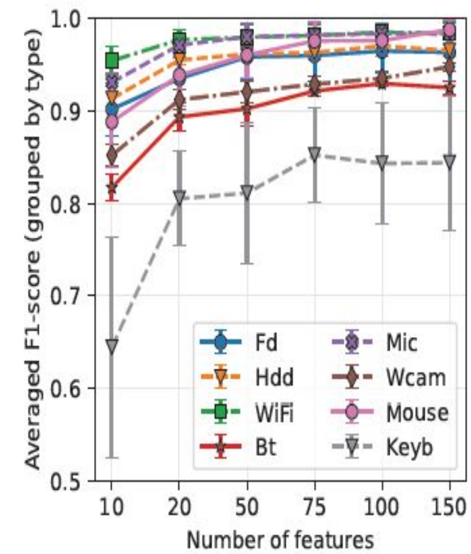
Model Recognition - Results (2/6)

SPRITZ
Security & Privacy
Research Group

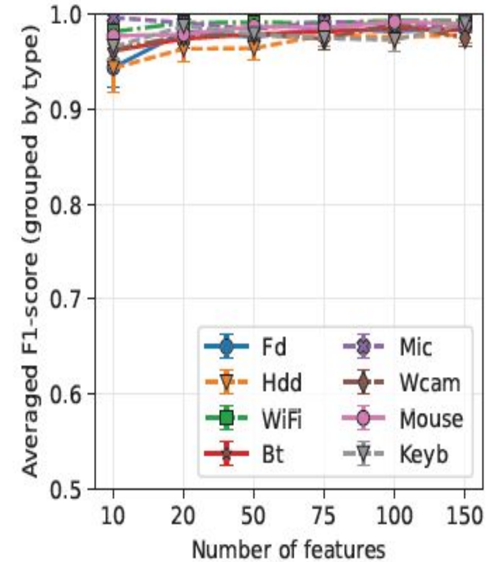
Università
degli Studi
di Padova

- 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

State Boot



State On

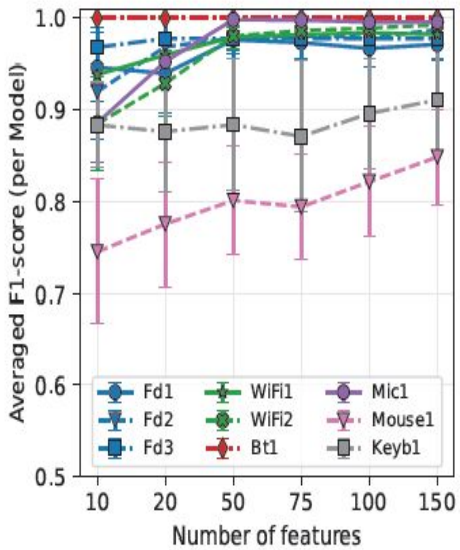


We can discriminate USB model for Boot and On

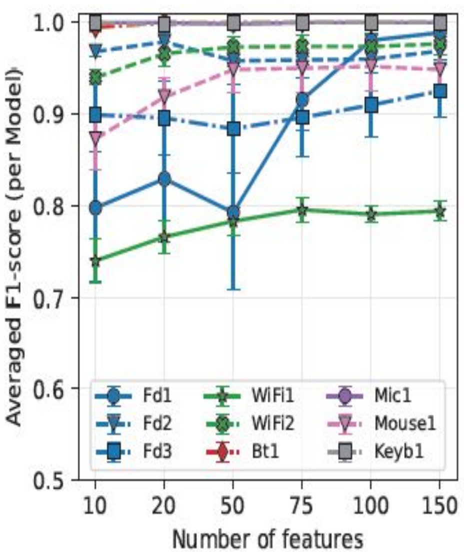
Device Recognition - Results (3/6)

- Given peripherals of the same model identify the specific device
  - *Models with # ≥ 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

State Boot



State On



We can almost discriminate the specific USB device

Action Recognition - Results (4/6)

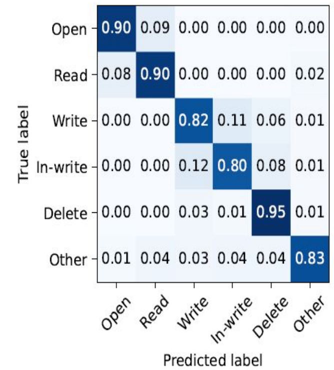
SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

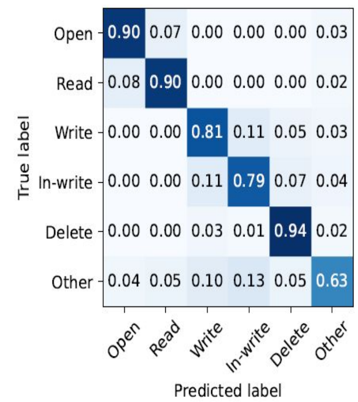
- Recognize an ongoing action given a device type
- *Multiclass* approach
    - *Fd*, *Hdd*, and *WiFi*
    - *Other* includes random actions
- WiFi type have a clear fingerprint
- Miss-classification between Write and In-Write
    - *In-Write is derived by the combination of Read and Write*

We can discriminate action given a type

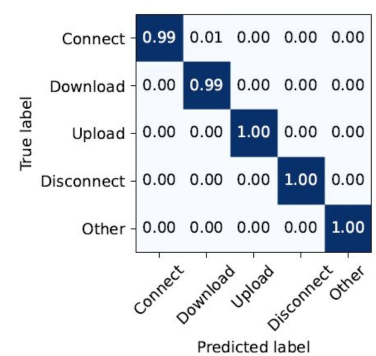
Flash Drive



HDD

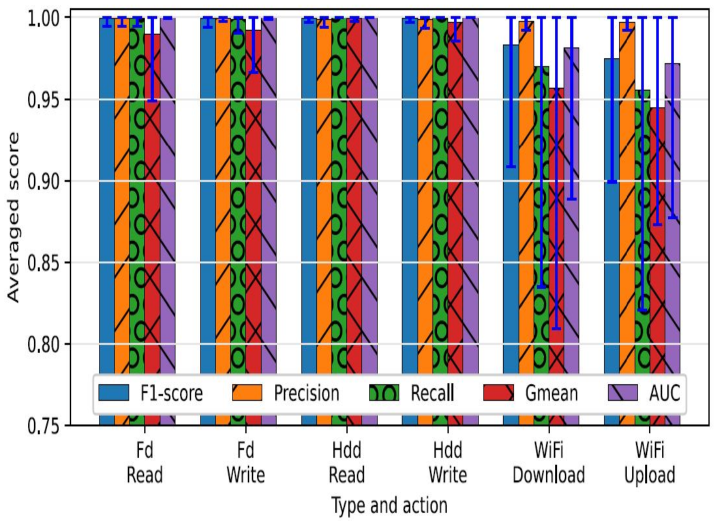


WiFi adapter



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)



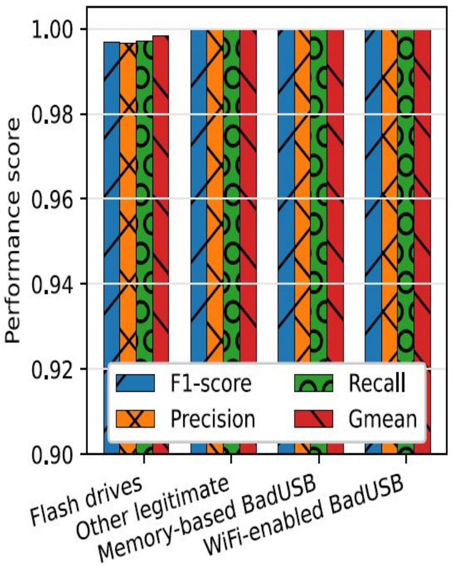
We can fingerprint an individual device from its actions

Bad vs. Good - Results (6/6)

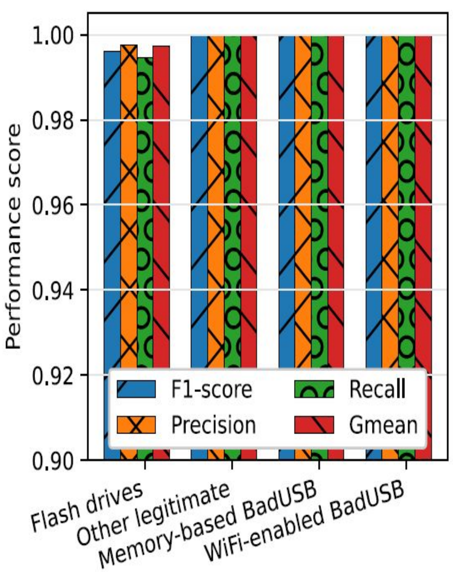
- Discriminate between
  - Flash Drives
  - Bad USBs
- *Multiclass* approach
  - 3 classes
  - *Other legitimate* includes other legitimate peripherals
- While collecting traces we run several attacks
  - command injection, WiFi scanning and connection
- Good scores according to all metrics

We can discriminate Bad USBs

State Boot



State On



Lesson Learned

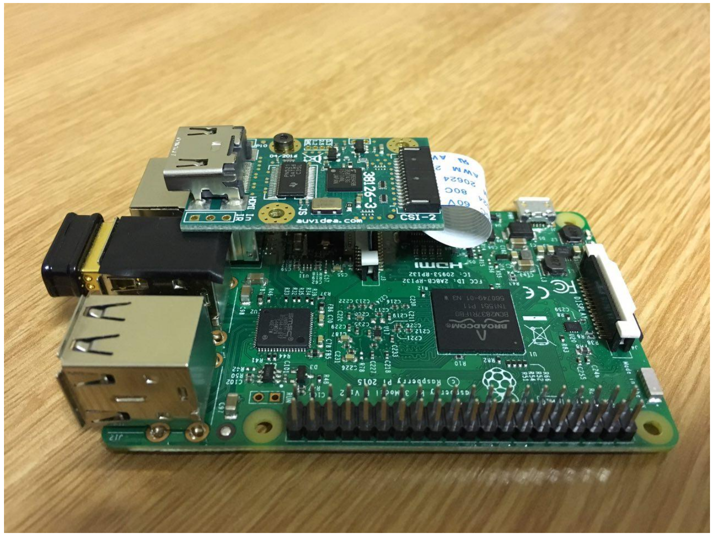
- USB devices are a still a common attack vector
- Evolution of the standard did not include any security
- Power consumption allows USB fingerprinting
    - *State*
    - *Type*
    - *Model*
    - *Specific device*
    - *Action*
    - *Malicious devices*
- Protect the host from USB-based threats
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


DELL

M. Conti, E. Losiouk, A. Visintin

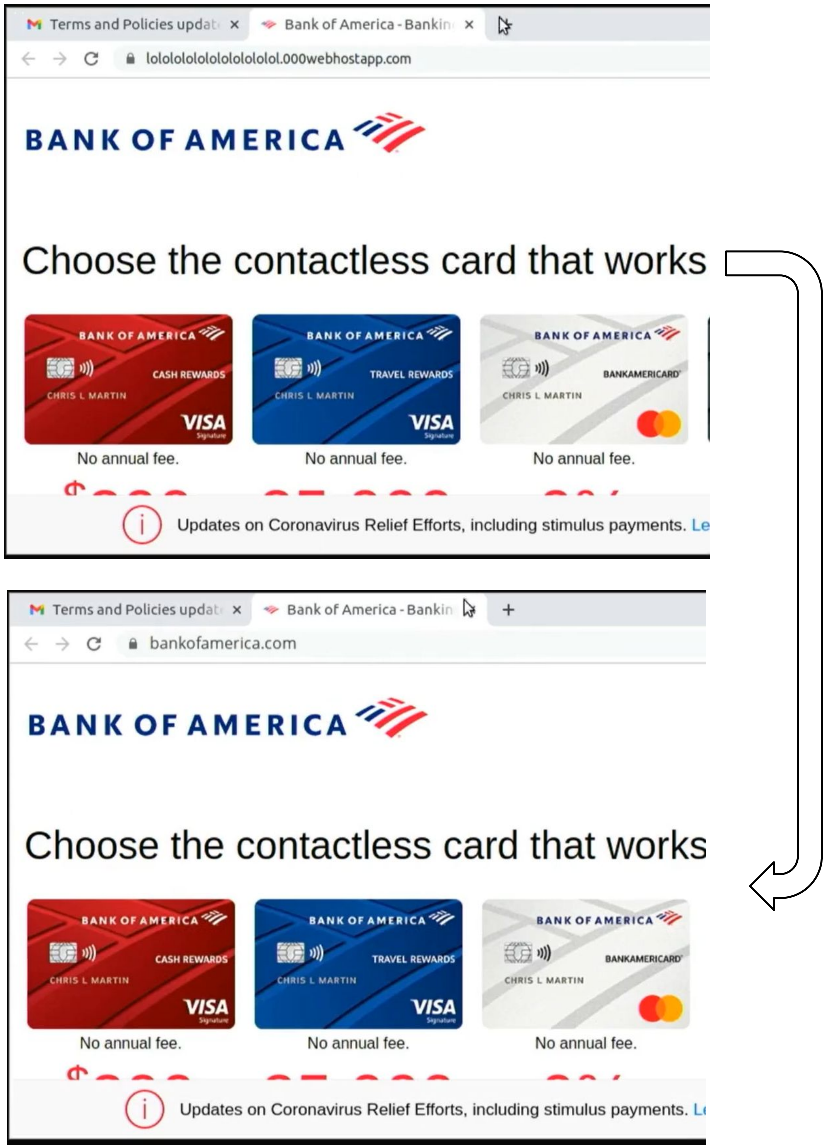
What You See is Not What You Get
A Man-in-the-Middle Attack Applied to Video Channels

In ACM/SIGAPP Symposium On Applied Computing 2022



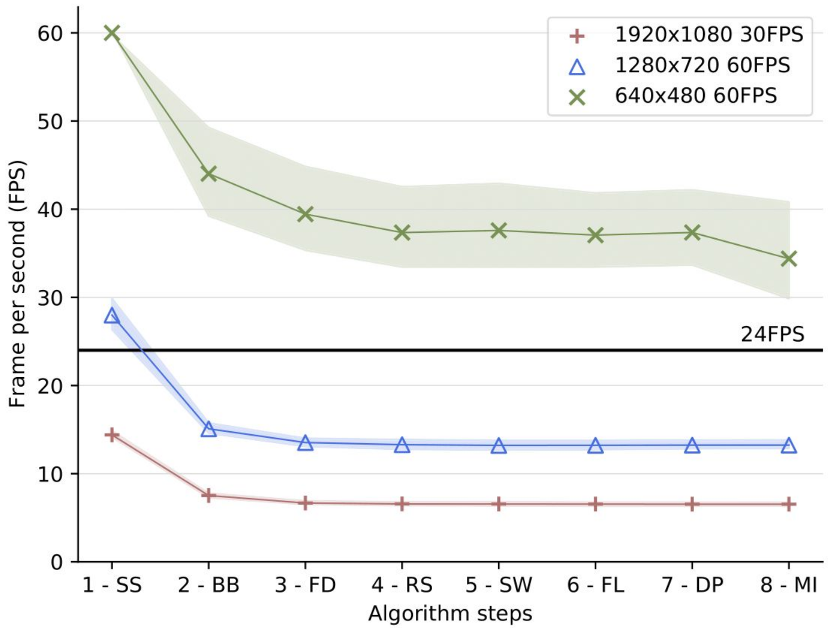
Man-in-the-Middle attack on a video channel.

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.

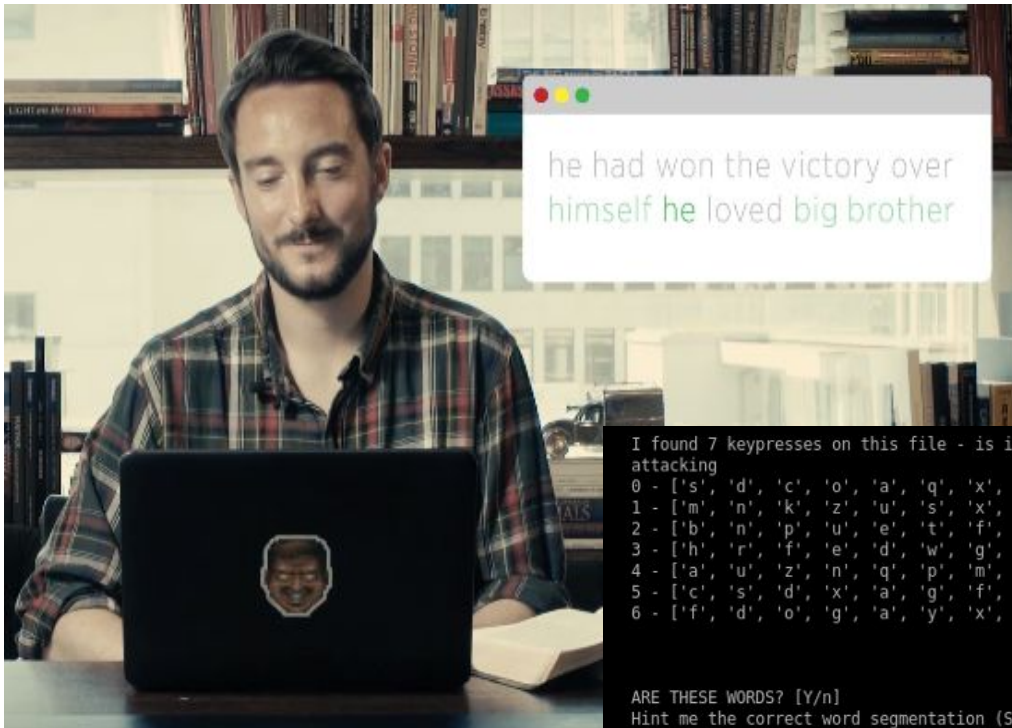
https://www.youtube.com/watch?v=lvsoJdpNsZA&ab_channel=SPRITZResearchGroupvideos

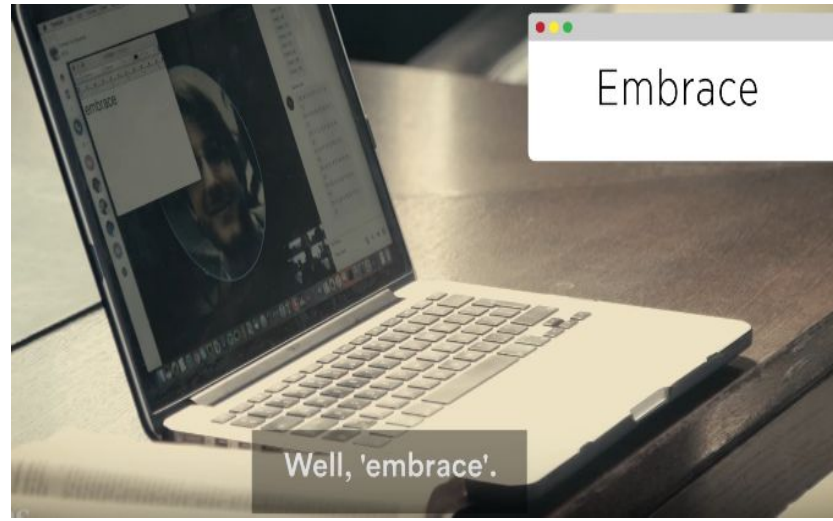
SPRITZ
Security & Privacy
Research Group

Università
degli Studi
di Padova

Does it **really** work?

vs Forbes, 1984 & the Bible






```
I found 7 keypresses on this file - is it correct? [Y/n]
attacking
0 - ['s', 'd', 'c', 'o', 'a', 'q', 'x', 'f', 'g']
1 - ['m', 'n', 'k', 'z', 'u', 's', 'x', 'i', 'a']
2 - ['b', 'n', 'p', 'u', 'e', 't', 'f', 's', 'v']
3 - ['h', 'r', 'f', 'e', 'd', 'w', 'g', 'p', 'c']
4 - ['a', 'u', 'z', 'n', 'q', 'p', 'm', 'c', 's']
5 - ['c', 's', 'd', 'x', 'a', 'g', 'f', 'k', 'z']
6 - ['f', 'd', 'o', 'g', 'a', 'y', 'x', 'h', 'c']


ARE THESE WORDS? [Y/n]
Hint me the correct word segmentation (Suggested spaces in []):
[('embrace', 21), ('surface', 26), ('conduct', 28), ('disease', 29), ('attract', 30), ('courage', 31), ('fantasy', 32), ('contact', 3
3), ('intense', 33), ('library', 33), ('silence', 33), ('already', 34), ('average', 34), ('defense', 34), ('impress', 34), ('subject'
, 34), ('suppose', 34), ('discuss', 35), ('expense', 35), ('offense', 36), ('science', 36), ('storage', 36), ('absence', 37), ('stoma
ch', 37), ('finance', 38), ('operate', 38), ('overall', 38), ('suspect', 38), ('century', 39), ('funding', 39)]
```

https://drive.google.com/file/d/1uLDDI_eESswOm6pQs59I4NeOjXwjOq1M/view?usp=sharing

Forbes Credits: https://www.forbes.com/sites/thomasbrewster/2017/07/06/skype-and-type-attack-steals-passwords

Thank you!

Questions?

(if you do not have one, please find some suggestions below)