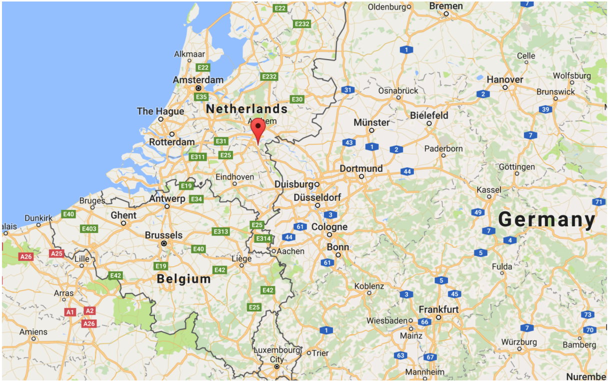
A new categorization system for side-channel attacks on mobile devices & more

Veelasha Moonsamy
Radboud University, The Netherlands

06 February 2017
University of Adelaide, Australia

Radboud University, Nijmegen, NL

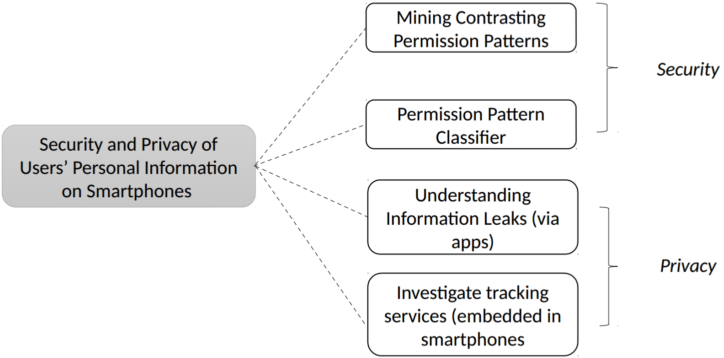


Digital Security (DiS) Group

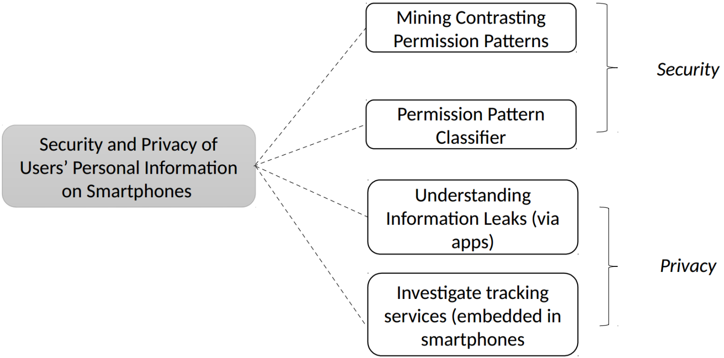
DiS research topics

- (Applied) Crypto
  - Symmetric key crypto
  - Identity-based applications
  - Smart cards and RFID security
- Hardware security
  - Side-channel analysis and countermeasures
  - Fault attacks
- Efficient implementations of crypto: hardware and software
- Post-quantum crypto
- Lightweight crypto: protocols and implementations

PhD research overview



PhD research overview



- Postdoc research interests: hardware- and software-based side channel on mobile devices

Outline of my talk

- **Part I**: Establishing a covert channel via USB charging cable on mobile devices

Outline of my talk

- **Part I**: Establishing a covert channel via USB charging cable on mobile devices
- **Part II**: New categorization system for side-channel attacks on smartphones

Part I

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

Acknowledgment

- Joint collaboration:

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

Riccardo Spolaor
University of Padua
Padua, Italy
rspolaor@math.unipd.it

Laila Abudahi
University of Washington
Seattle, United States
abudahil@uw.edu

Veelasha Moonsamy
Radboud University
Nijmegen, The Netherlands
veelasha@cs.ru.nl

Mauro Conti
University of Padua
Padua, Italy
conti@math.unipd.it

Radha Poovendran
University of Washington
Seattle, United States
rp3@uw.edu

- Paper available at: https://arxiv.org/abs/1609.02750

Motivation

- Increasing use of smartphones

Motivation

- Increasing use of smartphones
- Battery-draining apps (e.g. Pokémon Go)

Motivation

- Current situation: Airports, airplanes, shopping malls, gyms, museums, etc..

Motivation

- Emerging business model

Research Question

- Is it possible to exfiltrate data from a device while it is connected to a public charging station?

Research Question

- Is it possible to exfiltrate data from a device while it is connected to a public charging station?
- ... and the answer is YES!!

Research Question

- Is it possible to exfiltrate data from a device while it is connected to a public charging station?
- ... and the answer is YES!!
- Contributions:
  - Demonstrated the practicality of using only the power feature of USB charging cable as a covert channel to exfiltrate data from a device while it is connected to a public charging station.

Research Question

- Is it possible to exfiltrate data from a device while it is connected to a public charging station?
- ... and the answer is YES!!
- Contributions:
  - Demonstrated the practicality of using only the power feature of USB charging cable as a covert channel to exfiltrate data from a device while it is connected to a public charging station.
  - Built a proof-of-concept app, *PowerSnitch* to communicate bits of information in the form of power bursts back to the adversary

Research Question

- Is it possible to exfiltrate data from a device while it is connected to a public charging station?
- ... and the answer is YES!!
- Contributions:
  - Demonstrated the practicality of using only the power feature of USB charging cable as a covert channel to exfiltrate data from a device while it is connected to a public charging station.
  - Built a proof-of-concept app, *PowerSnitch* to communicate bits of information in the form of power bursts back to the adversary
  - Implemented a decoder, which resides on the adversary's side, i.e., public charging station, to retrieve the binary information embedded in the power bursts.

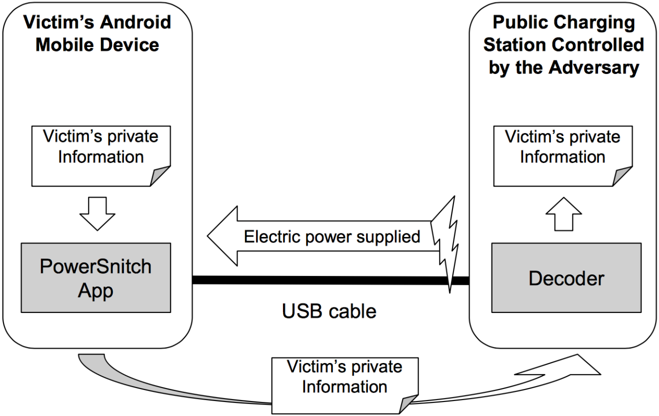
Assumptions

- Energy supplier's side (adversary)
  - Has physical access to the power meter
  - Able to monitor and store energy traces through the power meter

Assumptions

- Energy supplier's side (adversary)
  - Has physical access to the power meter
  - Able to monitor and store energy traces through the power meter
- Victim's side
  - Has installed the *PowerSnitch* app
  - Features of *PowerSnitch* app : requires access to private data (e.g. contacts), **does not** rely on traditional permission to transmit data (e.g. WiFi, Bluetooth)

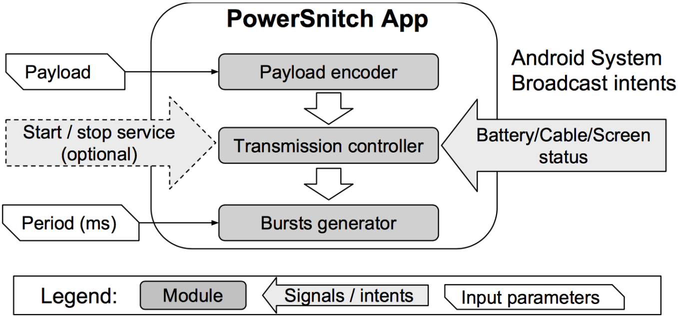
Overview of the attack



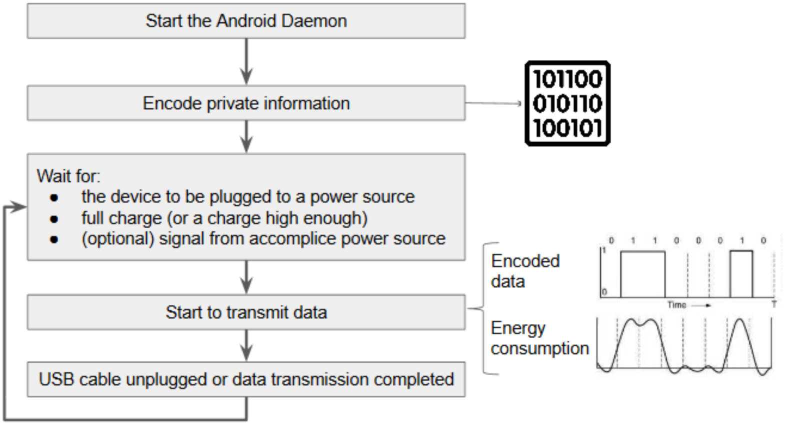
PowerSnitch app

- Used to establish a covert channel
  - Covert channel can be considered as a secret channel used to exfiltrate information from a secured environment in an undetected manner
- Can be deployed as a standalone app or as a library in a repackaged app
- Runs as a background service
- Uses `WAKE_LOCK` permission to wake up the CPU while phone is in deep sleep mode in order to start transmitting the payload
- Works even when user authentication mechanisms (i.e PIN) are in place
- Does not use any conventional communication technology (e.g., Wi-Fi, Bluetooth, NFC); can exfiltrate information even if the phone is in **airplane mode**
- Defeats existing USB charging protection dongles, since app only requires the USB power pins to exfiltrate data.

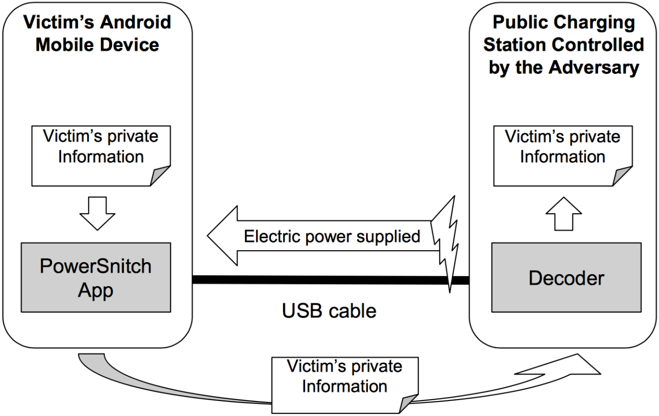
Components of the app



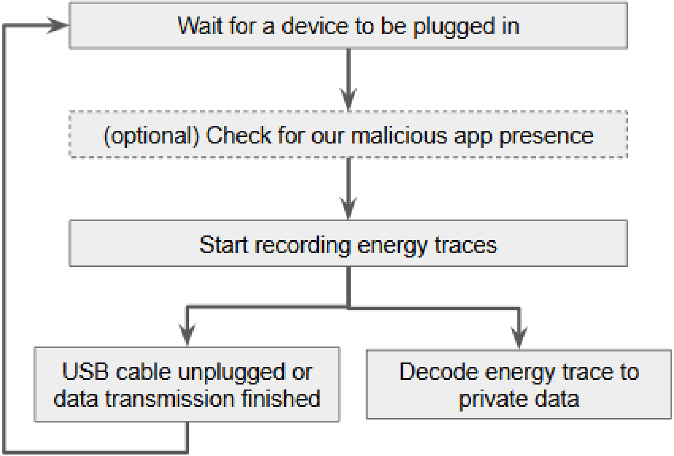
How does it work? (victim's side)



Overview of the attack - Decoder

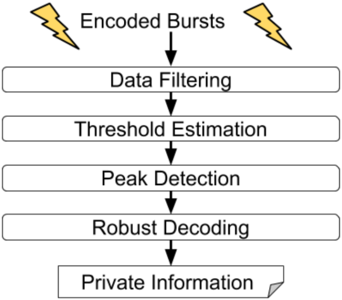


How does it work? (adversary's side)



Decoder design

- Components of the decoder

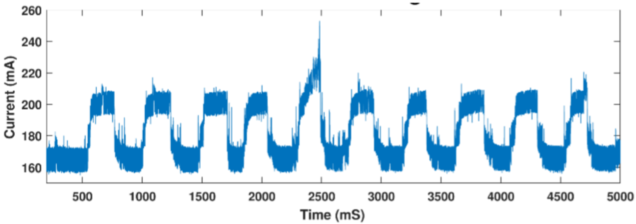


Components of the decoder

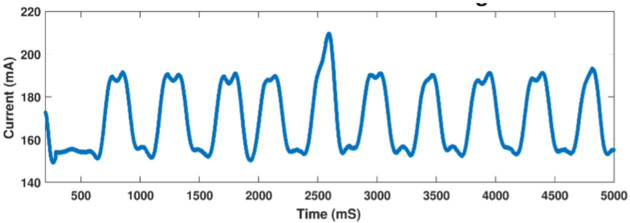
- 1. Data filtering:
    - Received signal is passed through a low-pass filter to get rid of high-frequency noises
    - Helps to smooth the signal and make threshold-based detection of peaks easier

Components of the decoder

- Data filtering - an example:



(a) Raw received signal.



(b) Low-pass filtered received signal.

Components of the decoder

- 2. Threshold estimation & 3. Peak detection:
  - Presence or absence of a peak at a certain time and for a specific period is translated to a corresponding bit

Components of the decoder

- 2. Threshold estimation & 3. Peak detection:
  - Presence or absence of a peak at a certain time and for a specific period is translated to a corresponding bit
  - Peak detection is done by setting an appropriate threshold; anything above the threshold is a peak, else it is just noise

Components of the decoder

- 2. Threshold estimation & 3. Peak detection:
  - Presence or absence of a peak at a certain time and for a specific period is translated to a corresponding bit
  - Peak detection is done by setting an appropriate threshold; anything above the threshold is a peak, else it is just noise
  - We make use of a ‘start’ and ‘end’ of transmission preamble to set the threshold

Evaluation

- Android phones: Nexus 4 with Android 5.1.1 (API 22), Nexus 5 with Android 6.0 (API 23), Nexus 6 with Android 6.0 (API 23) and Samsung S5 with Android 5.1.1 (API 22)
- Transmitted a payload (from the device) comprising of letters and numbers of ASCII code for a total of 512 bits
- Results in terms of Bit Error Ratio (BER) in the transmission of the payload; the lower the BER, the better the quality of the transmission

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

Making PowerSnitch more incognito...

- Keep a duty cycle (i.e. the time of power burst in a period) under 50%
  - Temperature of the device could increase significantly
  - If attack takes place during battery charge phase, battery will take more time to recharge due to high amount of energy consumed by the CPU

Making PowerSnitch more incognito...

- Keep a duty cycle (i.e. the time of power burst in a period) under 50%
  - Temperature of the device could increase significantly
  - If attack takes place during battery charge phase, battery will take more time to recharge due to high amount of energy consumed by the CPU
- Android Debug Bridge (ADB)
  - It is possible to monitor the CPU power consumption via the ADB
  - PowerSnitch could easily detect whether ADB setting is active through `Settings.Global.ADB_ENABLED`, once again provided by an Android API

Part II

New categorization system for side-channel attacks on smartphones

Side Channel Analysis (SCA)

- Previous work:
  - Smudge attacks on smartphone touch screens (WOOT 2010)
  - Inferring Keystrokes on Touch Screen from Smartphone Motion (HotSec 2011)
  - Practicality of accelerometer side channels on smartphones (ACSAC 2012)
  - ACCessory: Password Inference using Accelerometers on Smartphones (HotMobile 2012)

Side Channel Analysis (SCA)

- Previous work:
  - Smudge attacks on smartphone touch screens (WOOT 2010)
  - Inferring Keystrokes on Touch Screen from Smartphone Motion (HotSec 2011)
  - Practicality of accelerometer side channels on smartphones (ACSAC 2012)
  - ACCessory: Password Inference using Accelerometers on Smartphones (HotMobile 2012)
  - (Smart)watch your taps: side-channel keystroke inference attacks using smartwatches (ISWC 2015)
  - An empirical study of cryptographic misuse in android applications (CCS 2013)

Acknowledgment

SoK: Systematic Classification of Side-Channel Attacks on Mobile Devices

Raphael Spreitzer*, Veelasha Moonsamy†, Thomas Korak* and Stefan Mangard*
**Graz University of Technology, IAIK, Graz, Austria*
†*Radboud University, Digital Security Group, Nijmegen, The Netherlands*

- Paper available at: https://arxiv.org/pdf/1611.03748v1.pdf

Traditional SCA categorization

- Active vs. Passive
- Invasive vs. semi-invasive vs. non-invasive

Traditional SCA categorization

- Active vs. Passive
  - Depending on whether the attacker actively influences the behavior of the device or only passively observes leaking information
- Invasive vs. semi-invasive vs. non-invasive

Traditional SCA categorization

- Active vs. Passive
  - Depending on whether the attacker actively influences the behavior of the device or only passively observes leaking information
- Invasive vs. semi-invasive vs. non-invasive
  - Depending on whether or not the attacker removes the passivation layer of the chip, depackages the chip, or does not manipulate the packaging at all

Traditional SCA categorization

- Active vs. Passive
  - Depending on whether the attacker actively influences the behavior of the device or only passively observes leaking information
- Invasive vs. semi-invasive vs. non-invasive
  - Depending on whether or not the attacker removes the passivation layer of the chip, depackages the chip, or does not manipulate the packaging at all
- While early attacks required attackers to be in physical possession of the device, newer side-channel attacks, e.g., cache-timing attacks or DRAM row buffer attacks, are conducted remotely by executing malicious software in the targeted cloud environment

Traditional SCA categorization

- Active vs. Passive
  - Depending on whether the attacker actively influences the behavior of the device or only passively observes leaking information
- Invasive vs. semi-invasive vs. non-invasive
  - Depending on whether or not the attacker removes the passivation layer of the chip, depackages the chip, or does not manipulate the packaging at all
- While early attacks required attackers to be in physical possession of the device, newer side-channel attacks, e.g., cache-timing attacks or DRAM row buffer attacks, are conducted remotely by executing malicious software in the targeted cloud environment
- Majority of recently published side-channel attacks rely on passive attackers and are strictly non-invasive

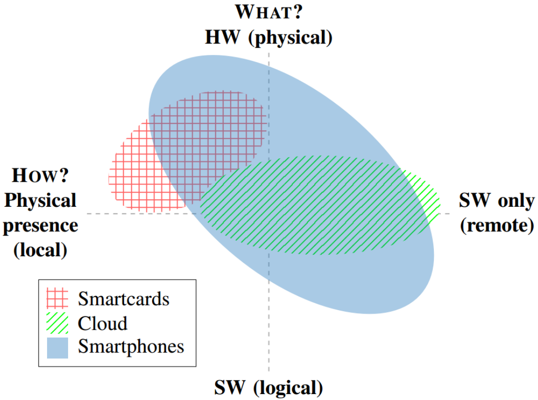
The 5 key enablers

- Always-on and portability
- Bring Your Own Device
- Ease of software installation
- OS based on Linux kernel
- Features and sensors

The 5 key enablers

- Always-on and portability
- Bring Your Own Device
- Ease of software installation
- OS based on Linux kernel
- Features and sensors
- Today's smartphones are vulnerable to (all or most of the) existing side-channel attacks against smartcards and cloud computing infrastructures. However, due to the above mentioned key enablers, a new area of side-channel attacks has evolved.

Scope of Attacks



New Categorization System - I

- Passive vs. Active

- Physical properties vs. logical properties

- Local attackers vs. vicinity attackers vs. remote attackers

New Categorization System - I

- Passive vs. Active
  - Distinguishes between attackers that passively observe leaking side-channel information and attackers that also actively influence the target via any side-channel vector. For instance, an attacker can manipulate the target, its input, or its environment via any side-channel vector in order to subsequently observe leaking information via abnormal behavior of the target
- Physical properties vs. logical properties
- Local attackers vs. vicinity attackers vs. remote attackers

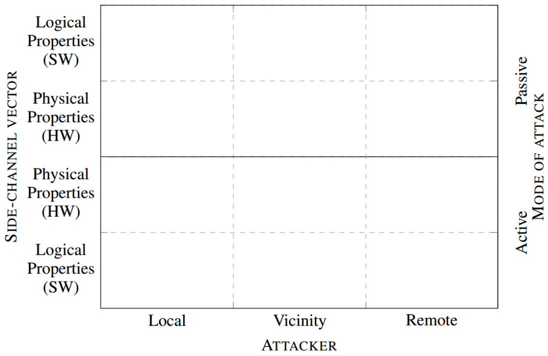
New Categorization System - I

- Passive vs. Active
  - Distinguishes between attackers that passively observe leaking side-channel information and attackers that also actively influence the target via any side-channel vector. For instance, an attacker can manipulate the target, its input, or its environment via any side-channel vector in order to subsequently observe leaking information via abnormal behavior of the target
- Physical properties vs. logical properties
  - Classifies side-channel attacks according to the exploited information, i.e., depending on whether the attack exploits physical properties (hardware) or logical properties (software features)
- Local attackers vs. vicinity attackers vs. remote attackers

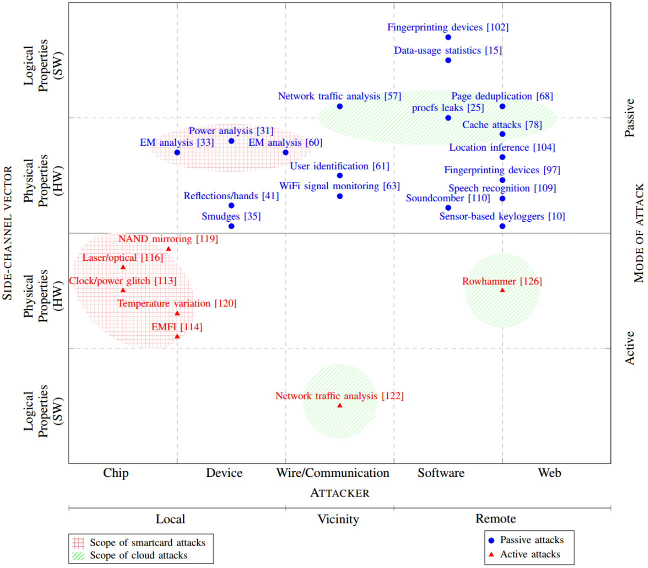
New Categorization System - I

- Passive vs. Active
  - Distinguishes between attackers that passively observe leaking side-channel information and attackers that also actively influence the target via any side-channel vector. For instance, an attacker can manipulate the target, its input, or its environment via any side-channel vector in order to subsequently observe leaking information via abnormal behavior of the target
- Physical properties vs. logical properties
  - Classifies side-channel attacks according to the exploited information, i.e., depending on whether the attack exploits physical properties (hardware) or logical properties (software features)
- Local attackers vs. vicinity attackers vs. remote attackers
  - Side-channel attacks are classified depending on whether or not the attacker must be in physical proximity/vicinity of the target. *Local attackers* clearly must be in (temporary) possession of the device or at least in close proximity. *Vicinity attackers* are able to wiretap or eavesdrop the network communication of the target or to be somewhere in the vicinity of the target. *Remote attackers* only rely on software execution on the targeted device.

Overview of new categorization system



Classification of SCAs on mobile devices



Thank you for your attention!

veelasha@cs.ru.nl
http://www.cs.ru.nl/~vmoonsamy/