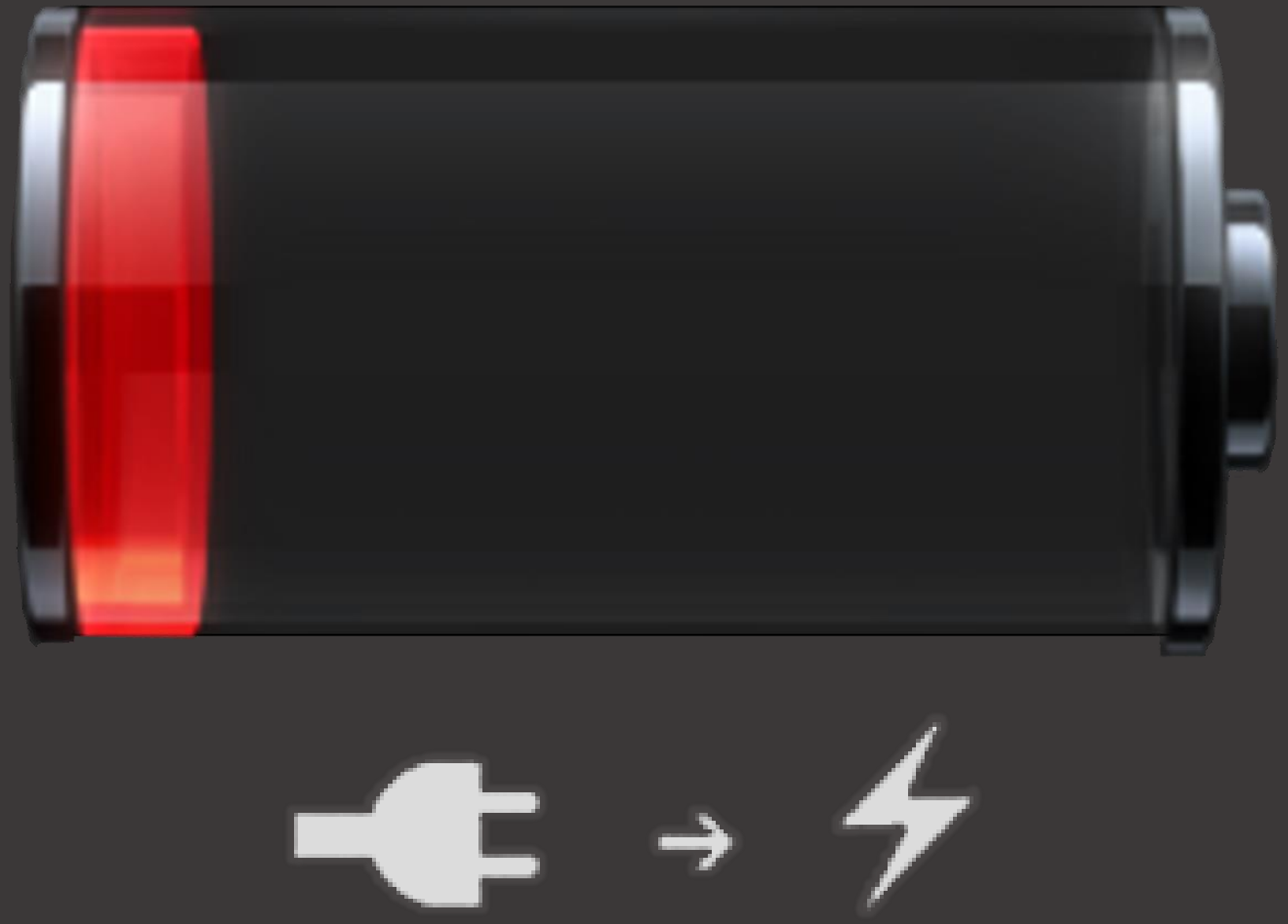
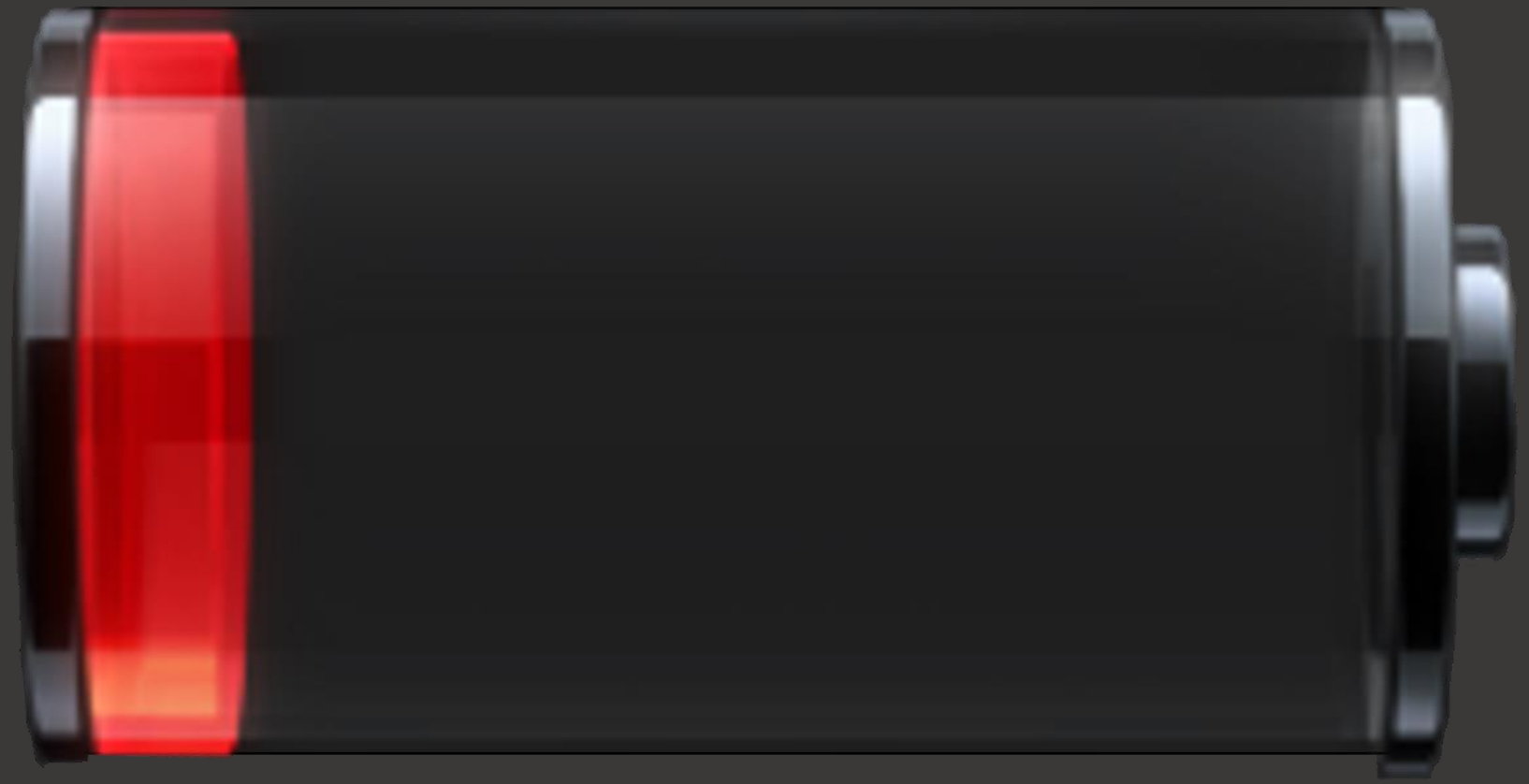
Power to peep-all:
Inference Attacks by Malicious Batteries on Mobile Devices

Pavel Lifshits, Roni Forte , Yedid Hoshen, Matt Halpern, Manuel Philipose, Mohit Tiwari, and Mark Silberstein

Speaker: Pavel Lifshits





Asking a total stranger to charge their smartphone

39%

Arguing with a significant other or romantic interest because of unanswered calls or texts

23%

Ordering something at a bar or restaurant just to use their power outlet

22%

Skipping the gym to charge their smartphone

33%

Secretly 'borrowing' someone else's charger

35%

PNAS
Proceedings of the
National Academy of Sciences
of the United States of America

OPINION

No Moore's Law for batteries

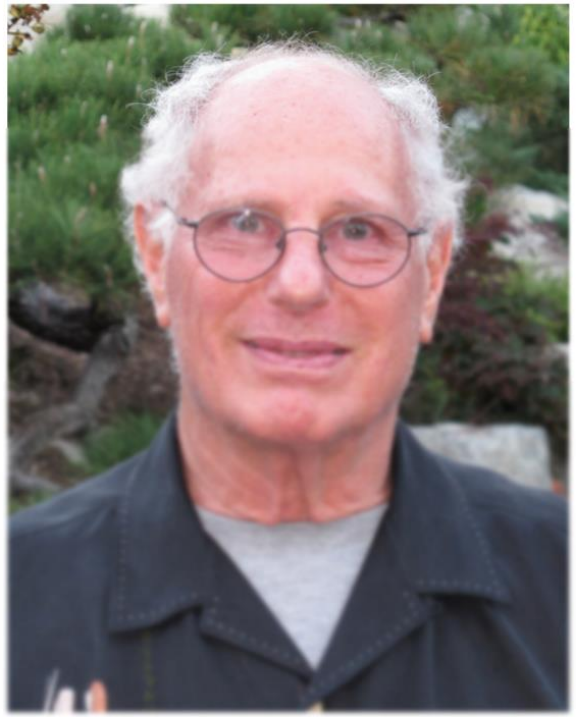
Fred Schlachter[1]
American Physical Society, Washington, DC 20045

The public has become accustomed to rapid progress in mobile phone technology, computers, and access to information; tablet computers, smart phones, and other powerful new devices are familiar to most people on the planet.

These developments are due in part to the ongoing exponential increase in computer processing power, doubling approximately every 2 years for the past several decades. This pattern is usually called Moore's Law and is named for Gordon Moore, a cofounder of Intel. The law is not a law like that for gravity; it is an empirical observation, which has become a self-fulfilling prophecy. Unfortunately, much of the public has come to expect that all technology does, will, or should follow such a law, which is not consistent with our everyday observations: For example, the maximum speed of cars, planes, or ships does not increase exponentially; maximum speed barely increases at all.

there is a Moore's Law for computer processors is that electrons are small and they do not take up space on a chip. Chip performance is limited by the lithography technology used to fabricate the chips; as lithography improves ever smaller features can be made on processors. Batteries are not like this. Ions, which transfer charge in batteries, are large, and they take up space, as do anodes, cathodes, and electrolytes. A D-cell battery stores more energy than an AA-cell. Potentials in a battery are dictated by the relevant chemical reactions, thus limiting eventual battery performance. Significant improvement in battery capacity can only be made by changing to a different chemistry.

Scientists and battery experts, who have been optimistic in the recent past about improving lithium-ion batteries and about developing new battery chemistries—lithium/air and lithium/sulfur are the leading candidates—are considerably less optimistic



Fred Schlachter.

breakthrough in battery technology, we do have a valuable and underutilized resource: energy efficiency, which in many cases is free or even has a negative cost. Cars can be made more energy efficient by reducing size, weight, and power. Incentives to re-

SMART BATTERY

- Programmability
- Sensors: current, voltage, temperature

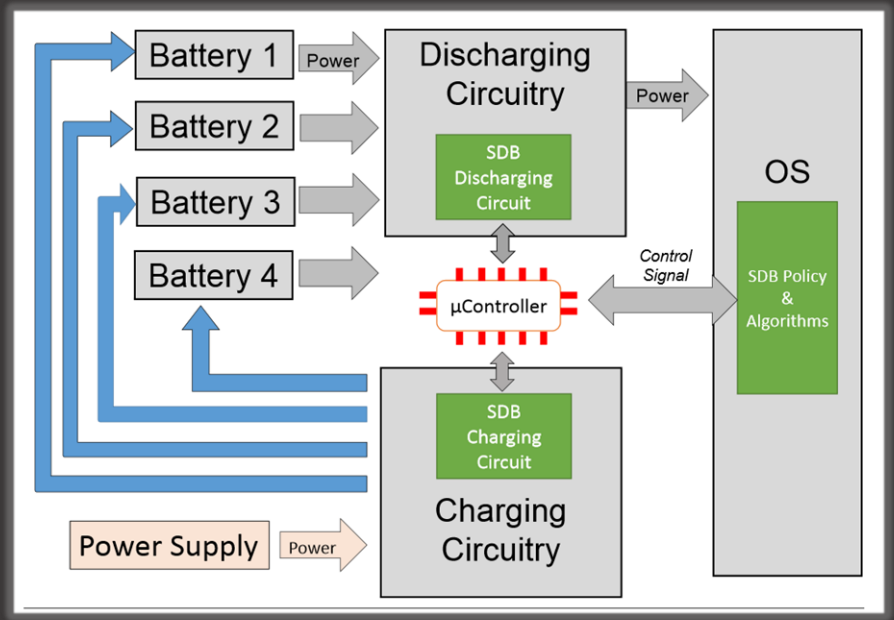
Why?

- ✓ Safety *overheating, over/under voltage*
- ✓ Extend battery life
- ✓ Performance

SMART BATTERY - PROGRAMMABILITY

Software defined battery (SOSP '15)

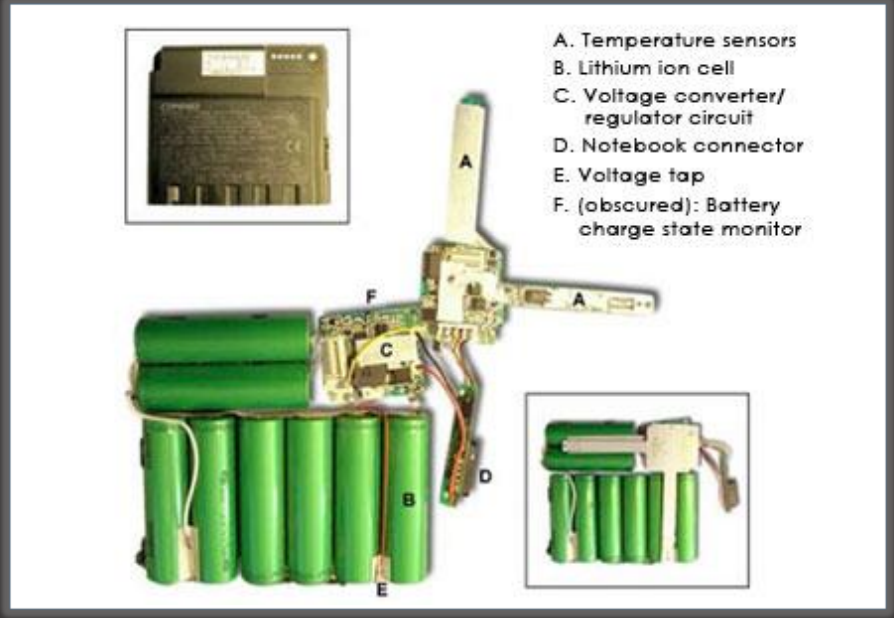
By Microsoft & Tesla



Smart battery System

See spec.

http://sbs-forum.org/specs/



INSIDE SMARTPHONE BATTERY

Btemp

NFC antenna

BSI *(battery size/status/system indicator)*

INSIDE SMARTPHONE BATTERY

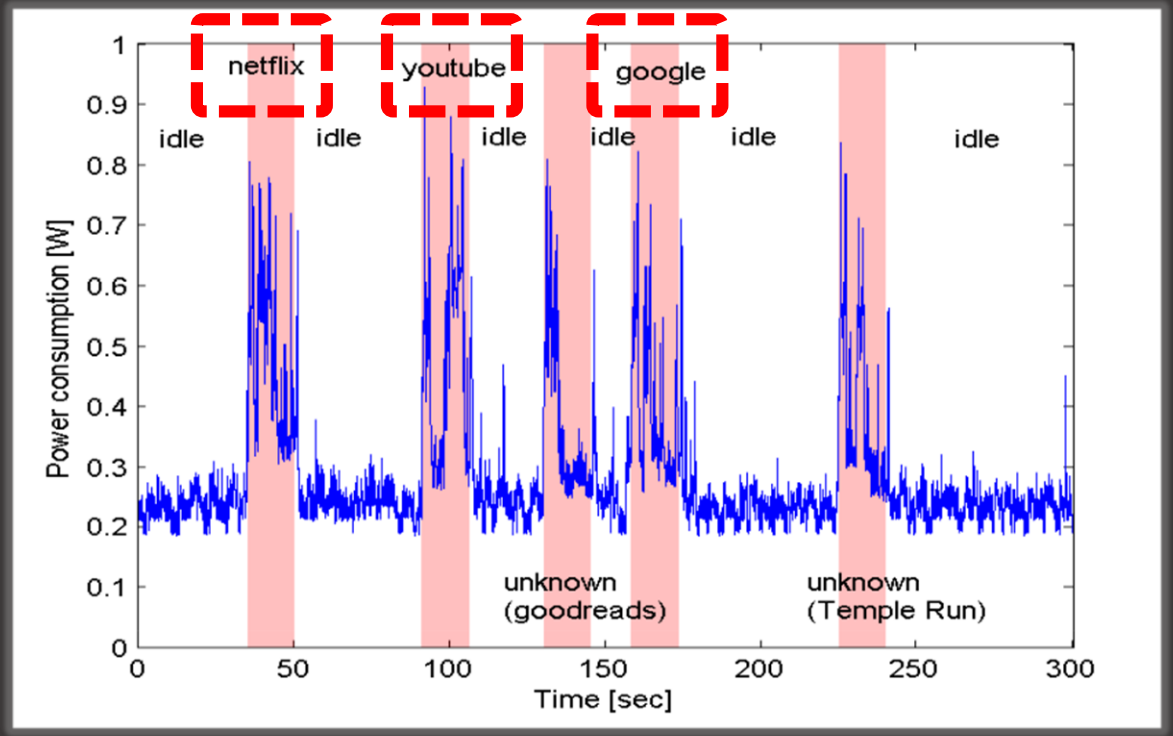
Your phone batteries are getting smarter!

Do the smart batteries create a new privacy threat?

Do the smart batteries create a new privacy threat?

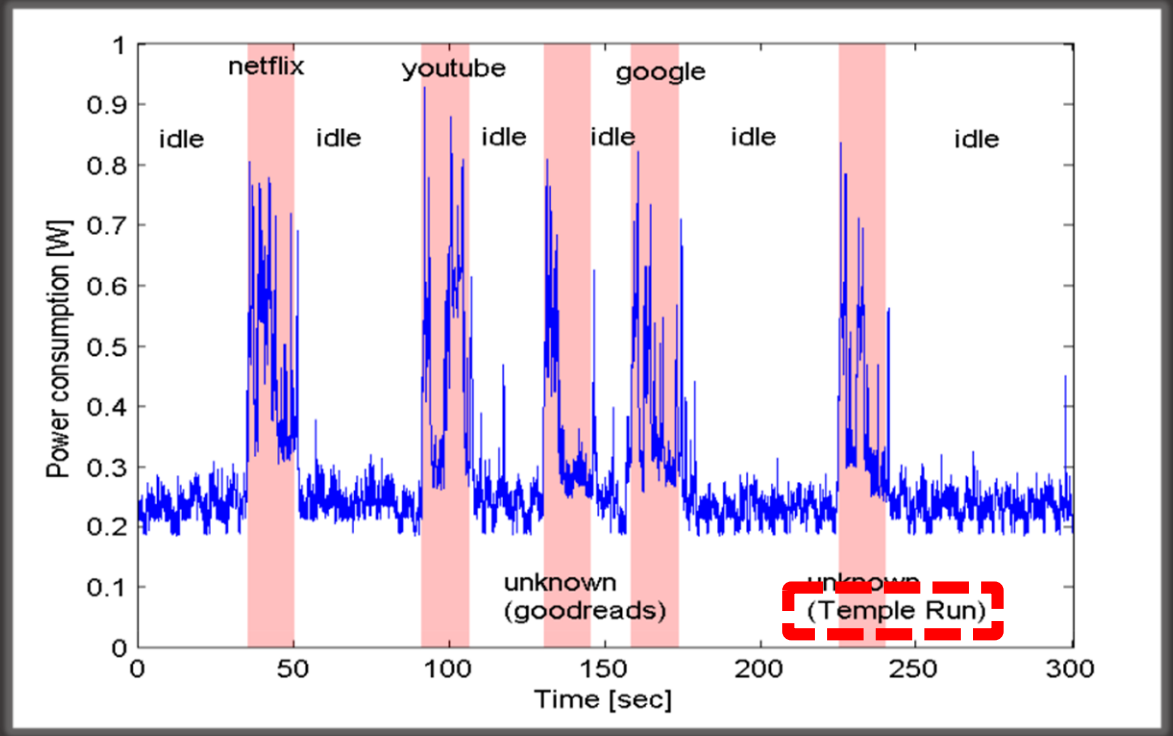
IF THE ATTACKER GETS ON YOUR BATTERY

- Browsing History



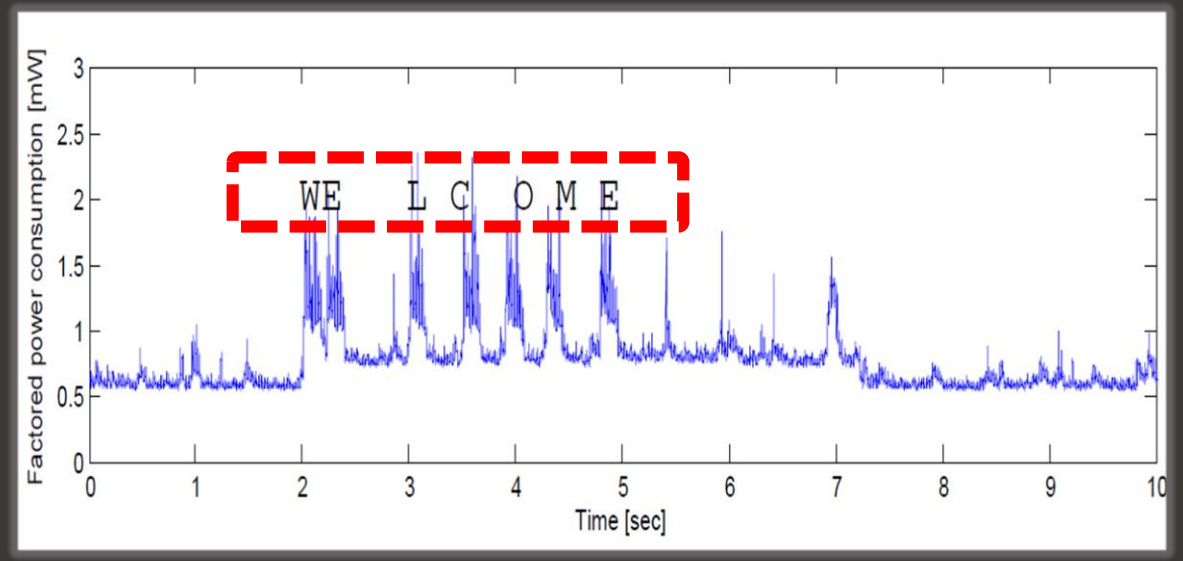
IF THE ATTACKER GETS ON YOUR BATTERY

- Browsing History
- Applications



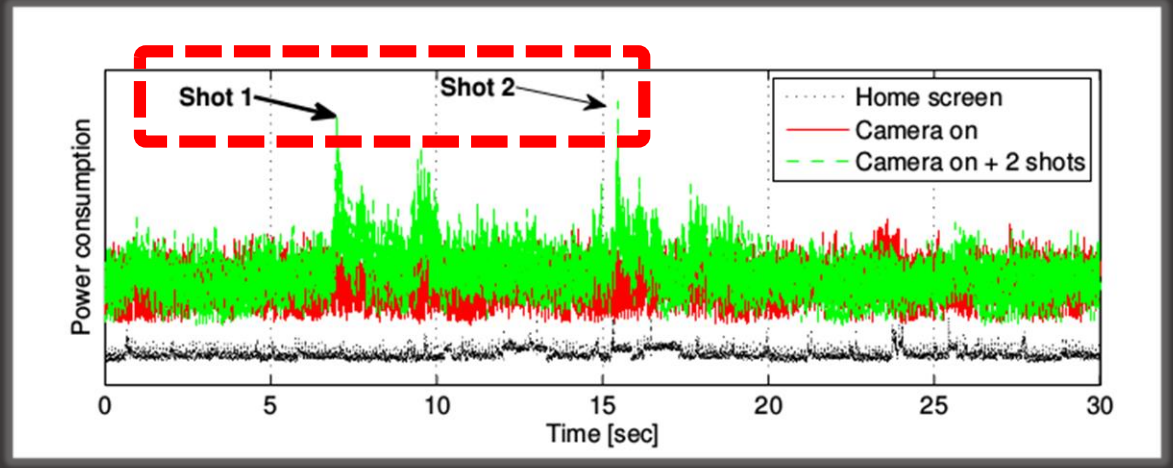
IF THE ATTACKER GETS ON YOUR BATTERY

- Browsing History
- Applications
- Typing



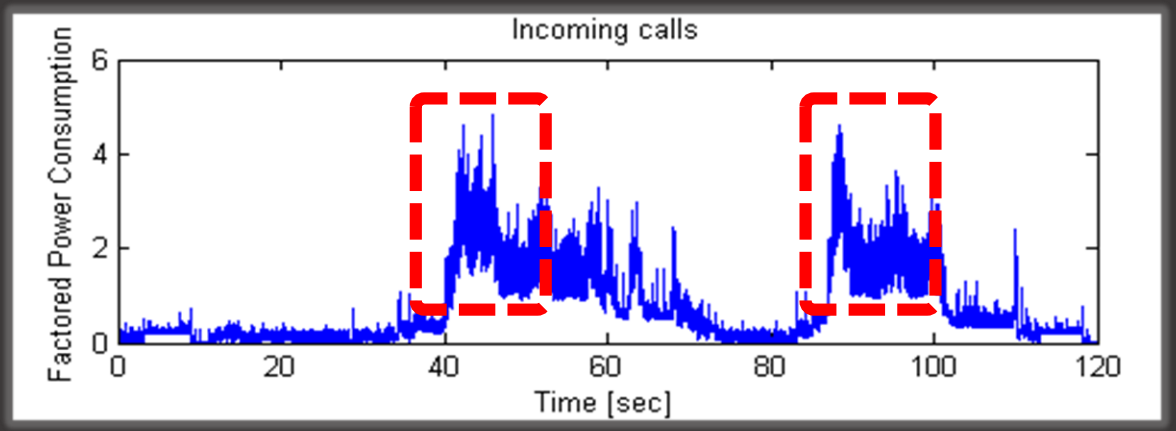
IF THE ATTACKER GETS ON YOUR BATTERY

- Browsing History
- Applications
- Typing
- Photo shot



IF THE ATTACKER GETS ON YOUR BATTERY

- Browsing History
- Applications
- Typing
- Photo shot
- Communication profile –Phone calls



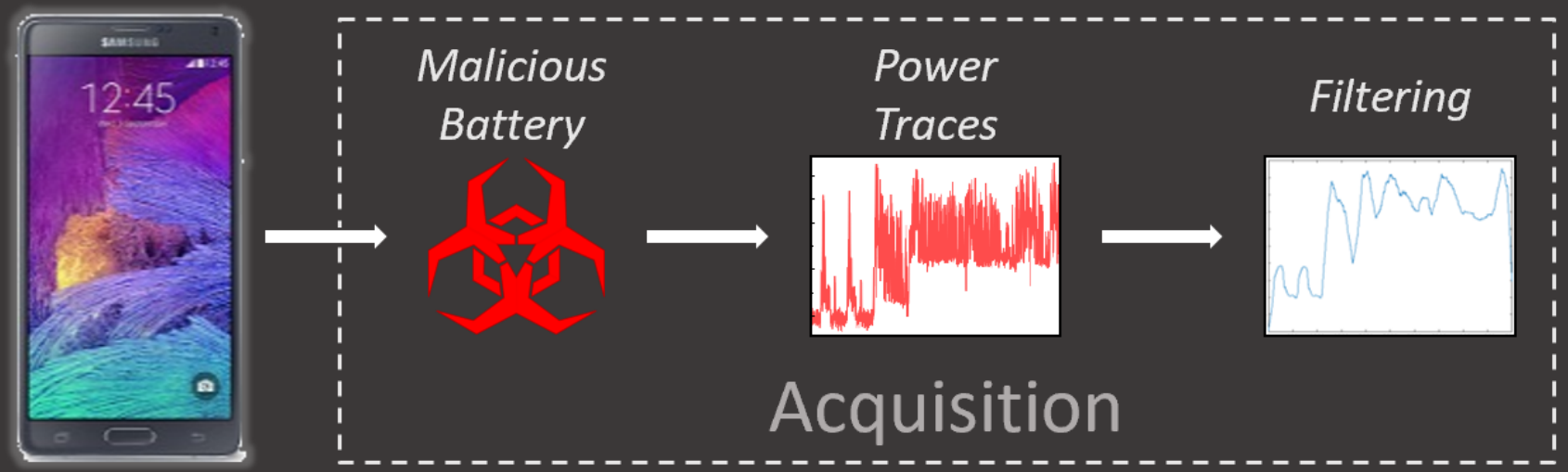
AGENDA

- General scheme for malicious battery attacks
- Examples:

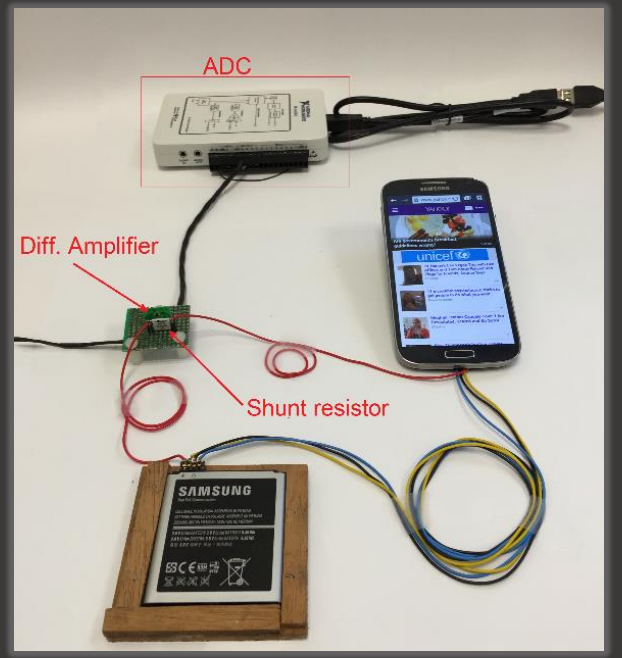
  Keystroke inference

  Combination of multiple attacks
- Data exfiltration mechanism via browser

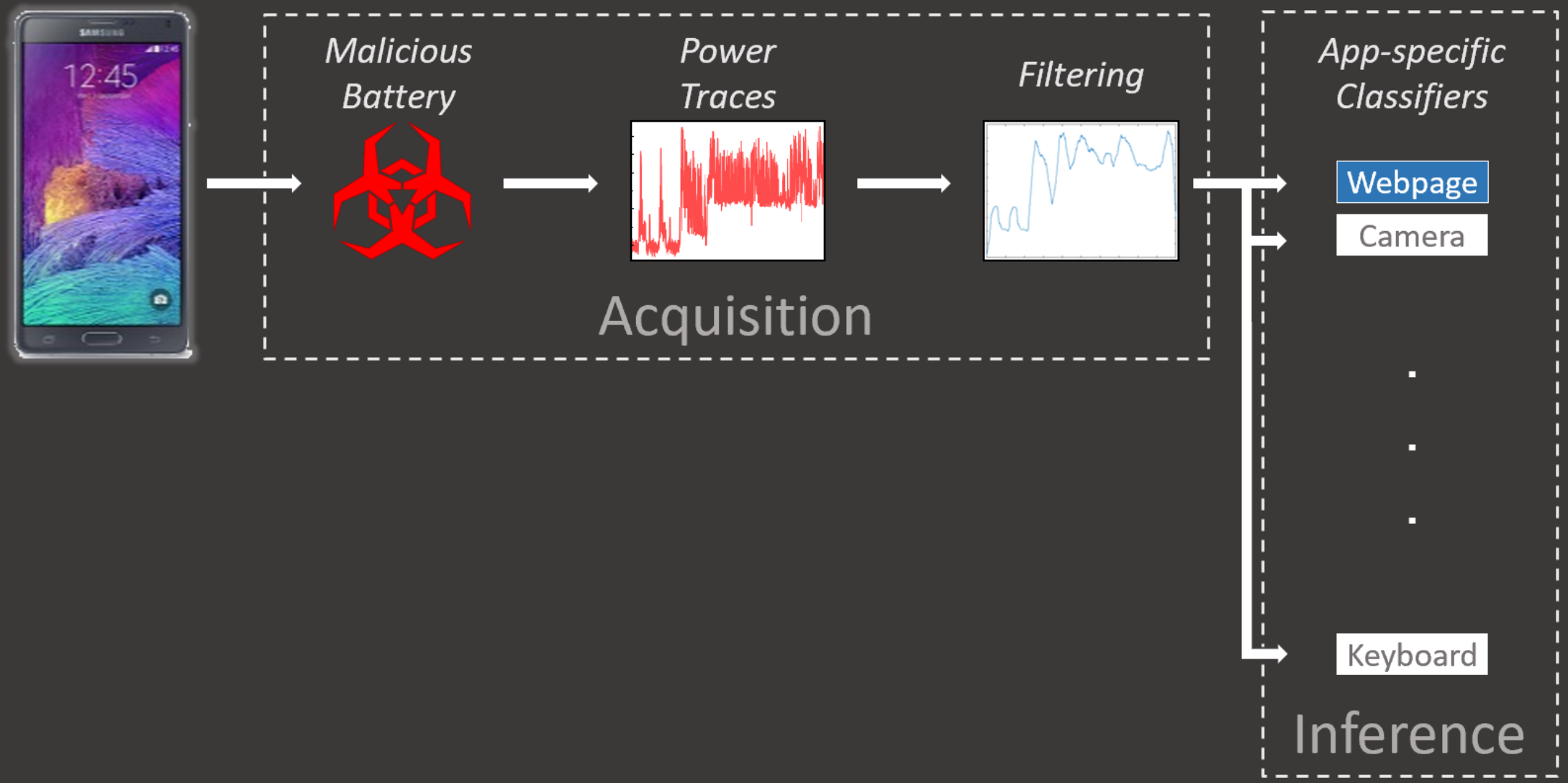
METHODOLOGY



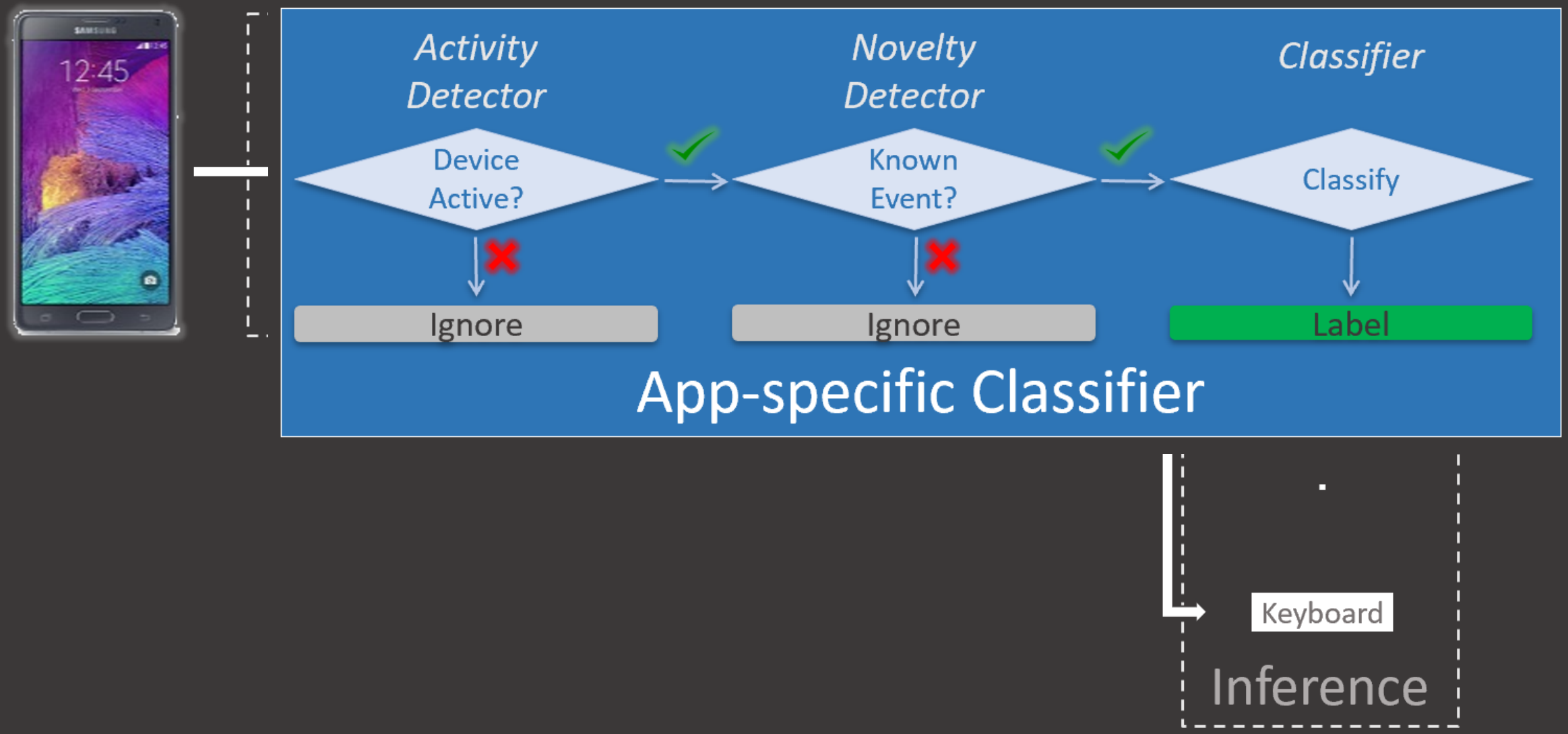
METHODOLOGY



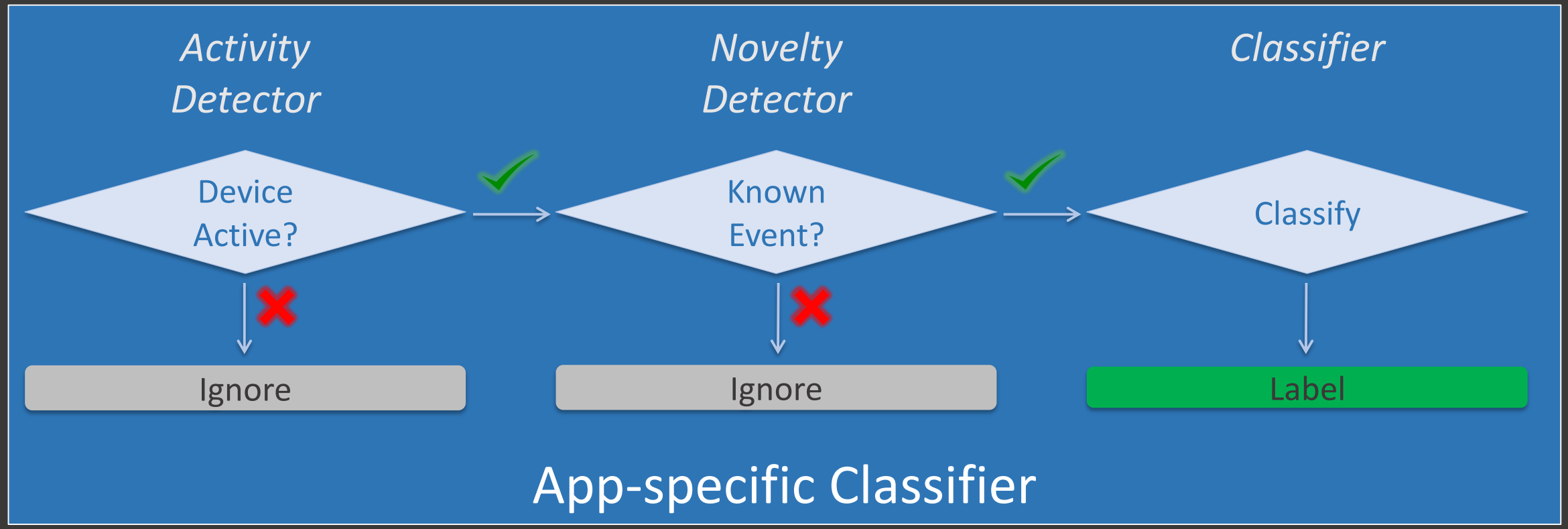
METHODOLOGY



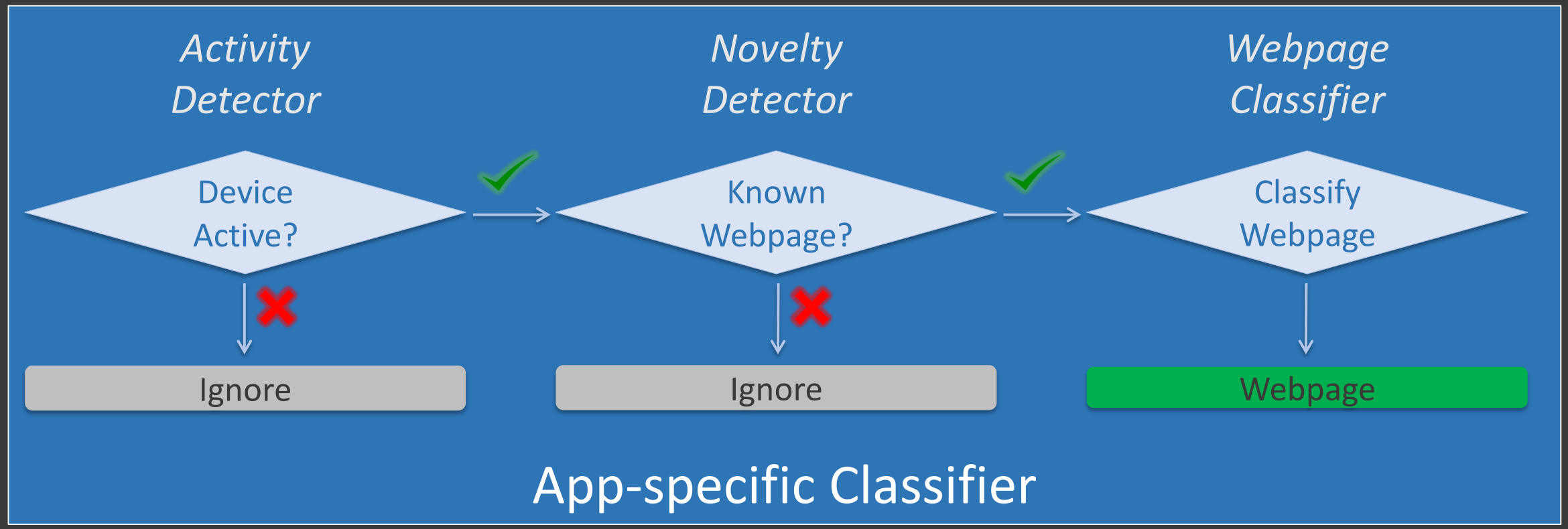
METHODOLOGY



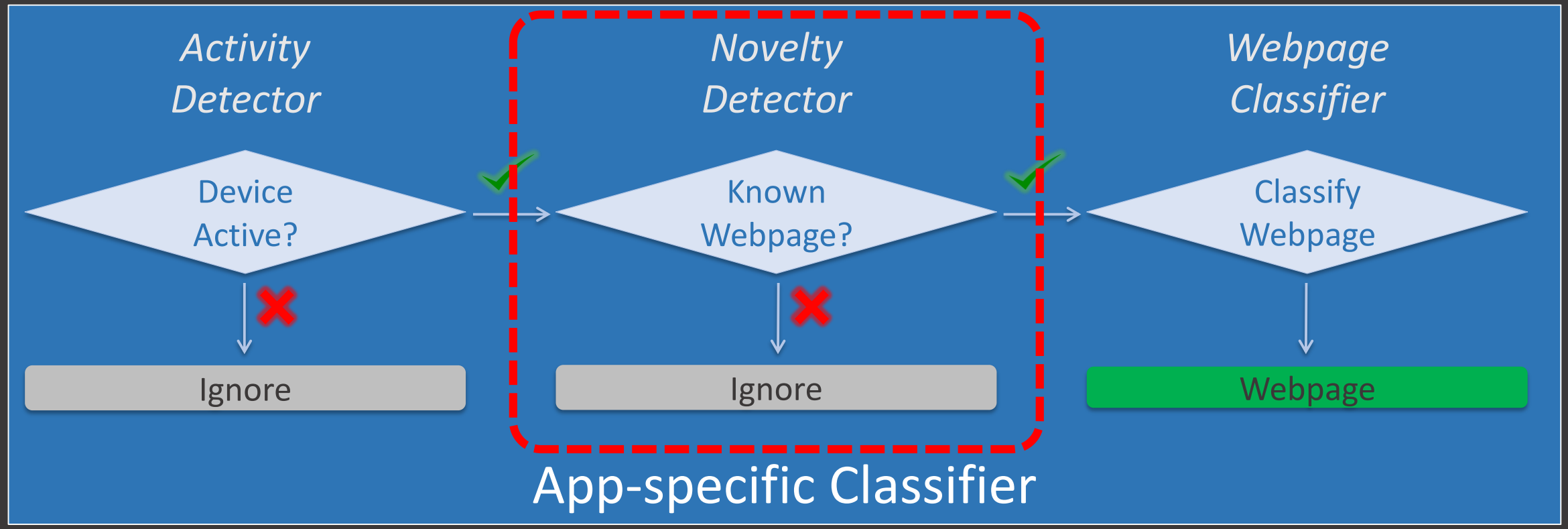
APP SPECIFIC PIPELINE



BROWSING HISTORY ATTACK PIPELINE



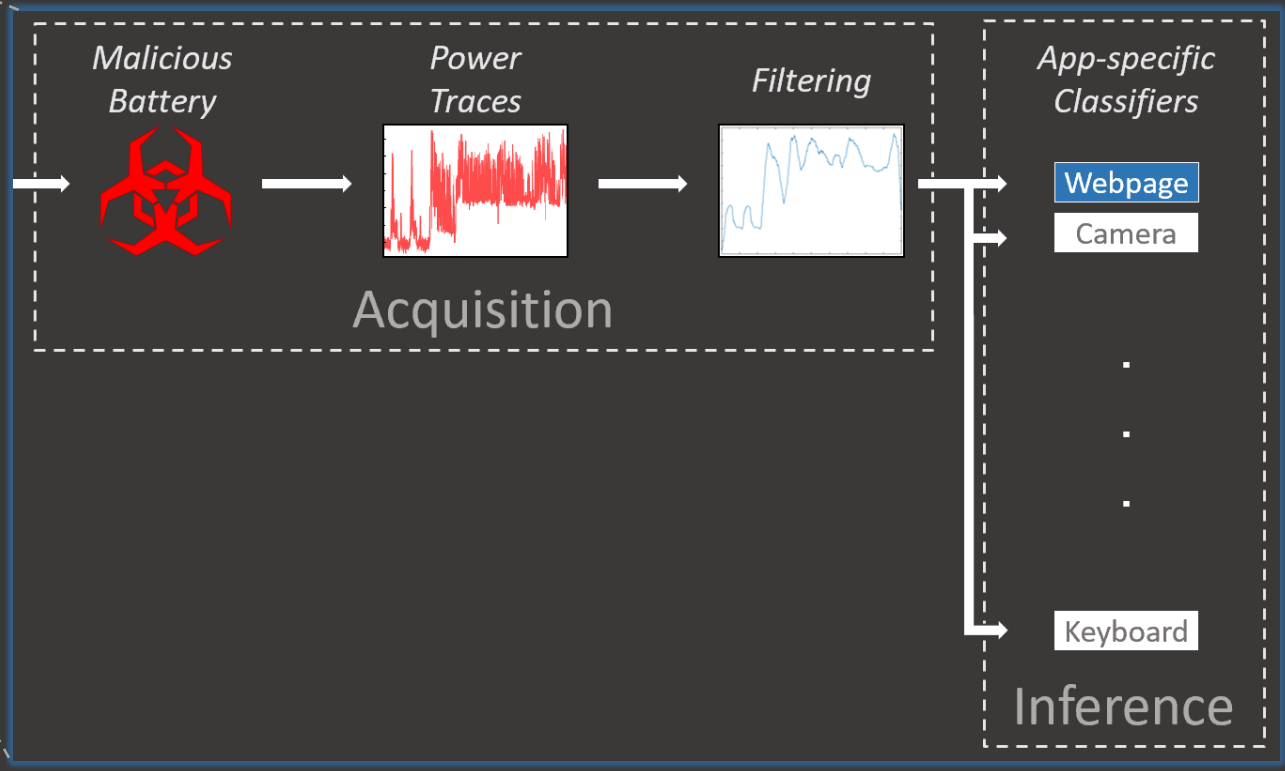
BROWSING HISTORY ATTACK PIPELINE



CONSTRAINT - FIT INSIDE THE BATTERY

Power requirements - <70 mA phone at rest
- *Computational complexity*
- *Signal sample rate*

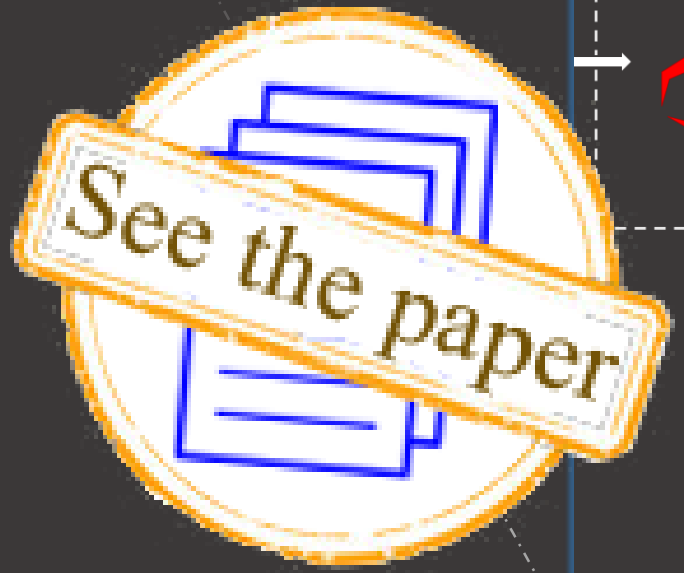
Storage

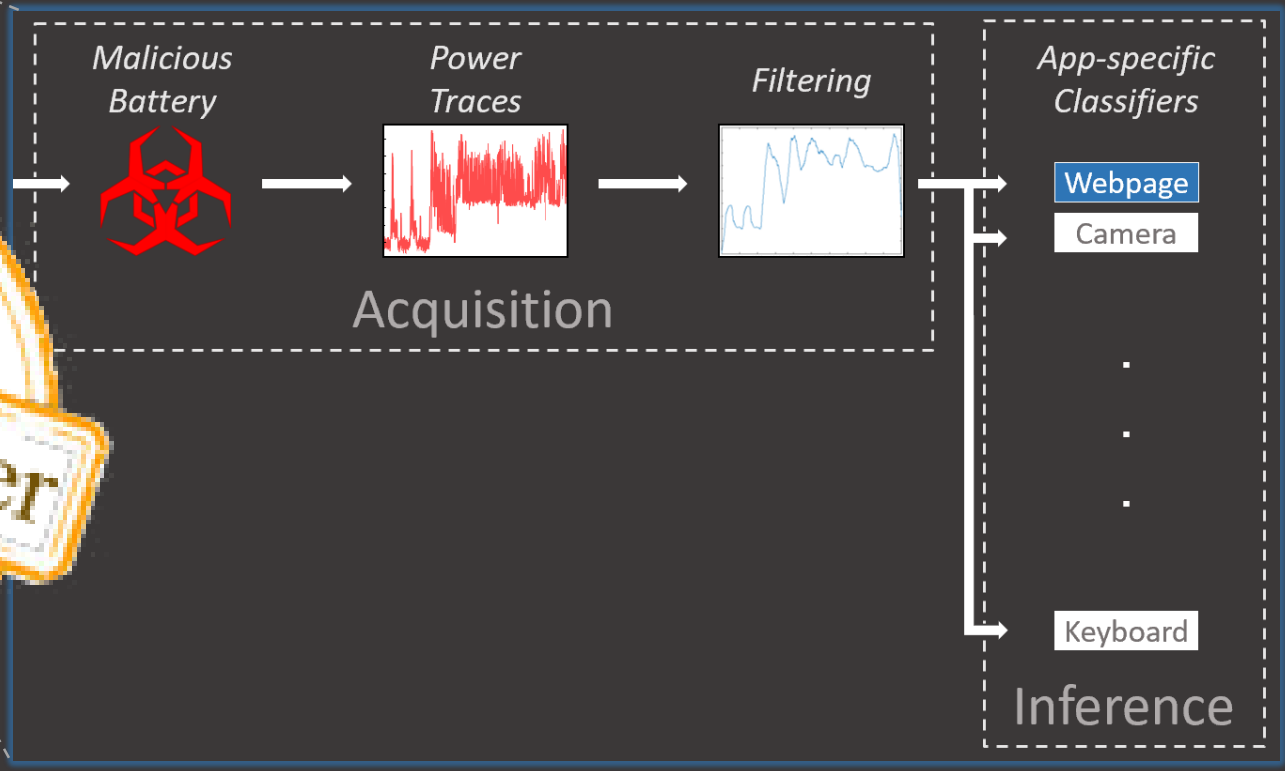


CONSTRAINT - FIT INSIDE THE BATTERY

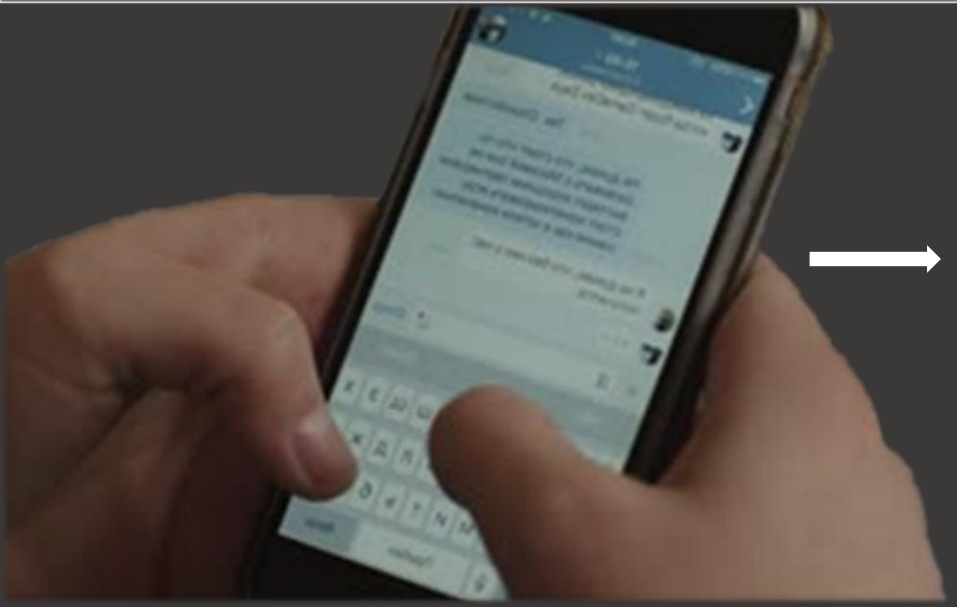
Power requirements - <70 mA phone at rest
- *Computational complexity*
- *Signal sample rate*

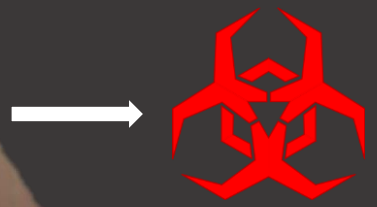
Storage

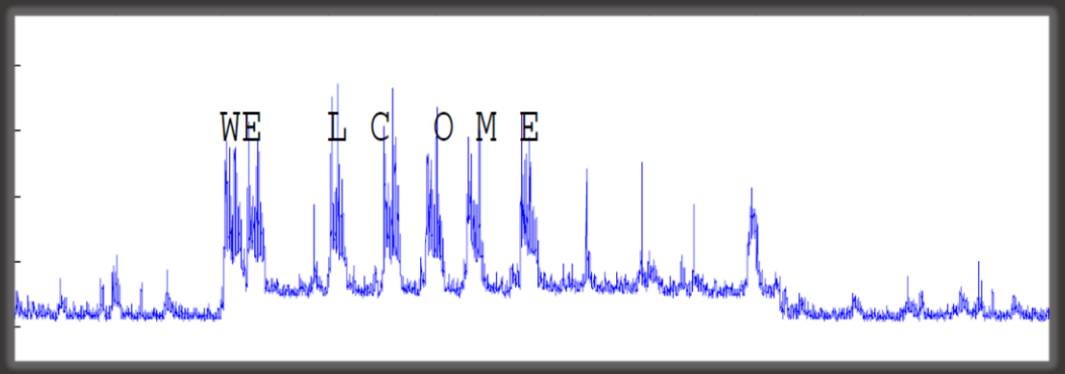




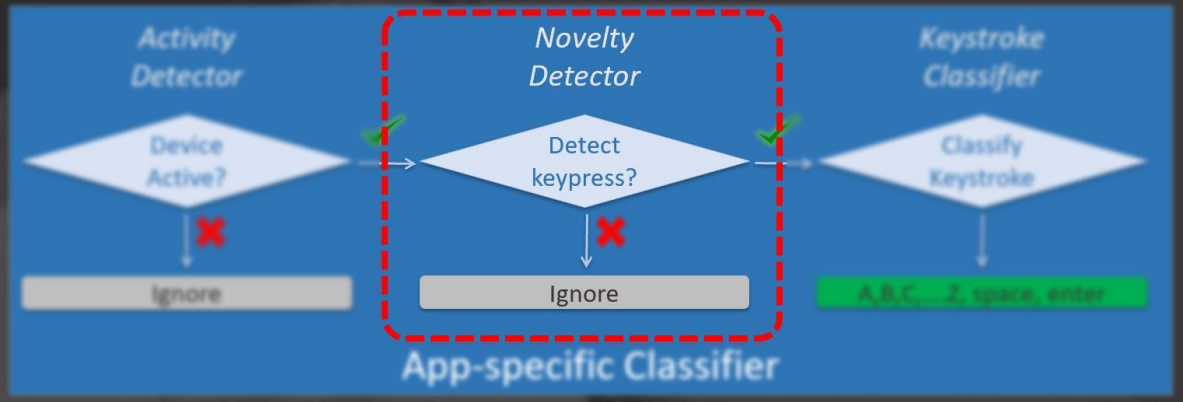
KEYSTROKE INFERENCE

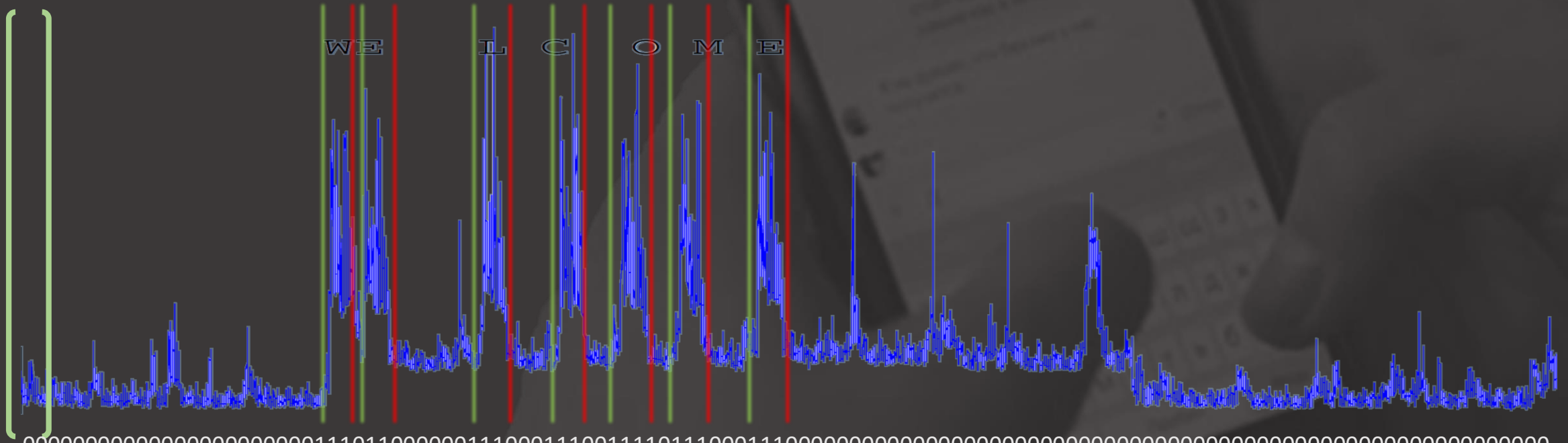




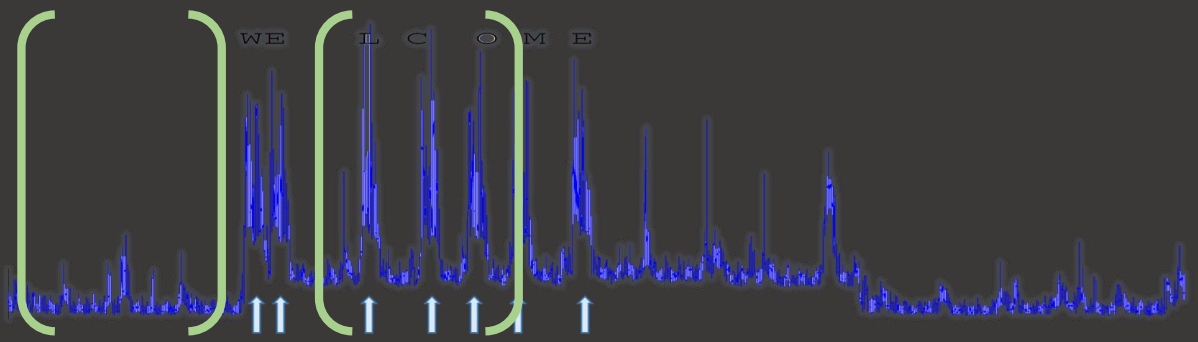


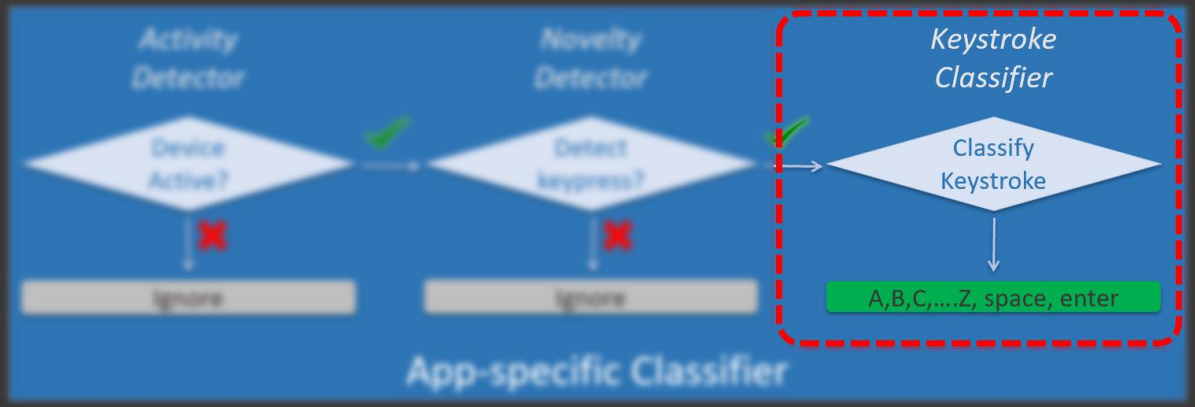
KEYSTROKE INFERENCE

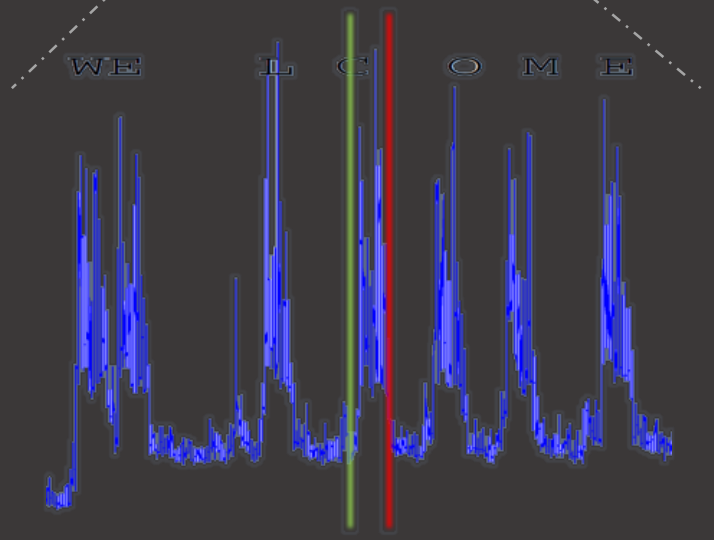




KEYSTROKE INFERENCE



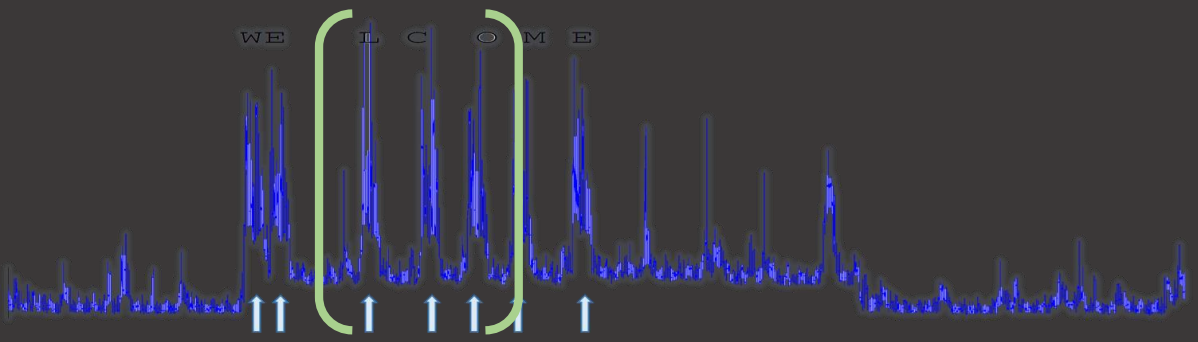


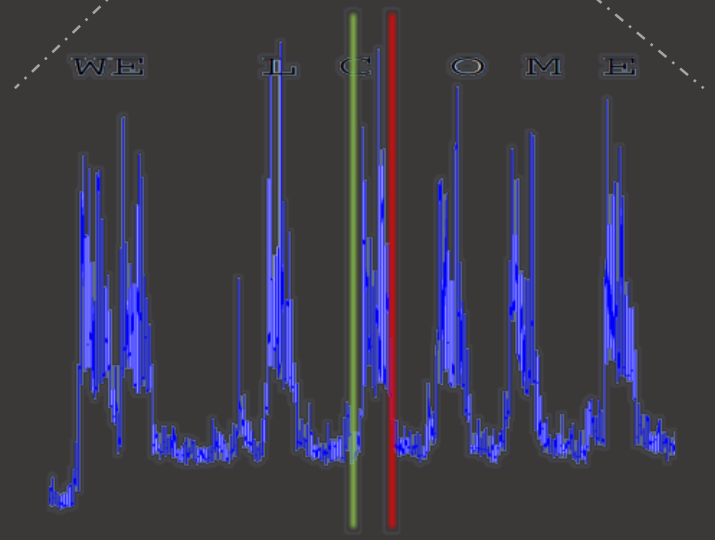


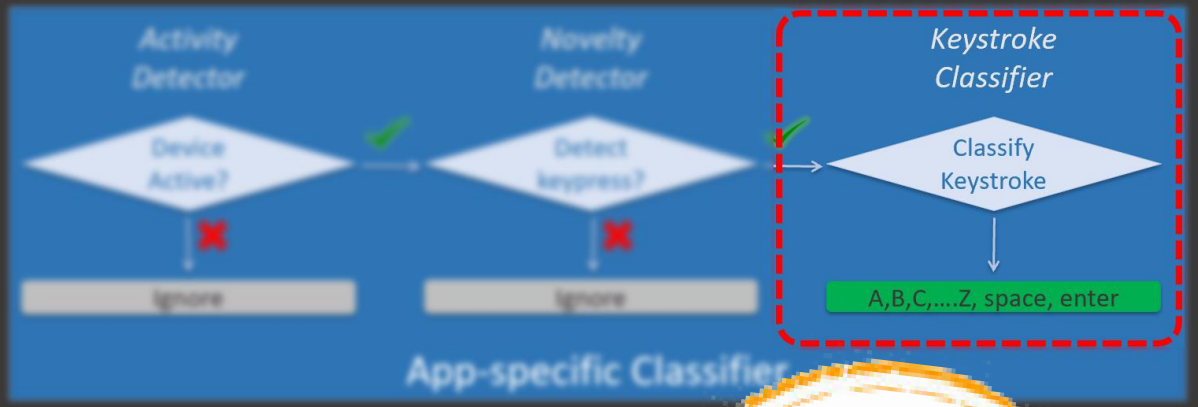
Convolutional Neural Network

'C'

KEYSTROKE INFERENCE



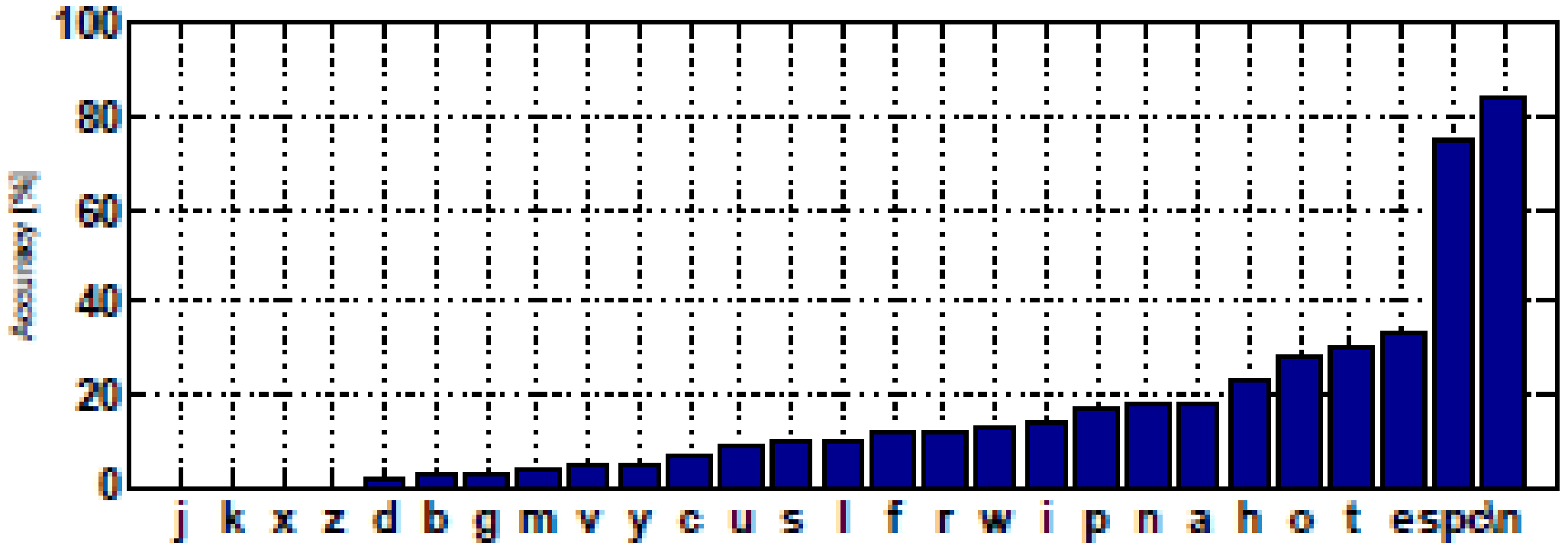




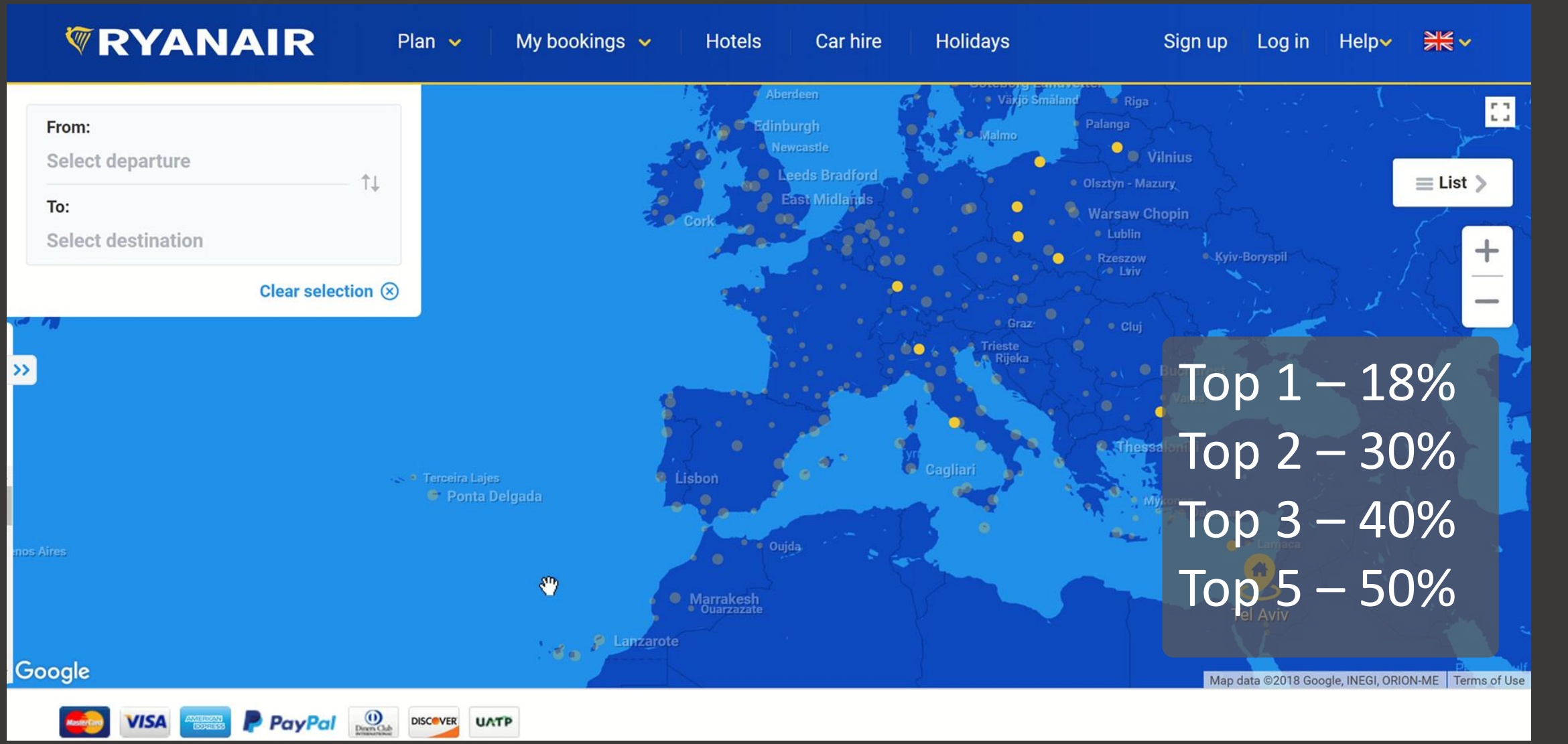
Convolutional Neural Network

'C'

KEYSTROKE INFERENCE - RESULTS



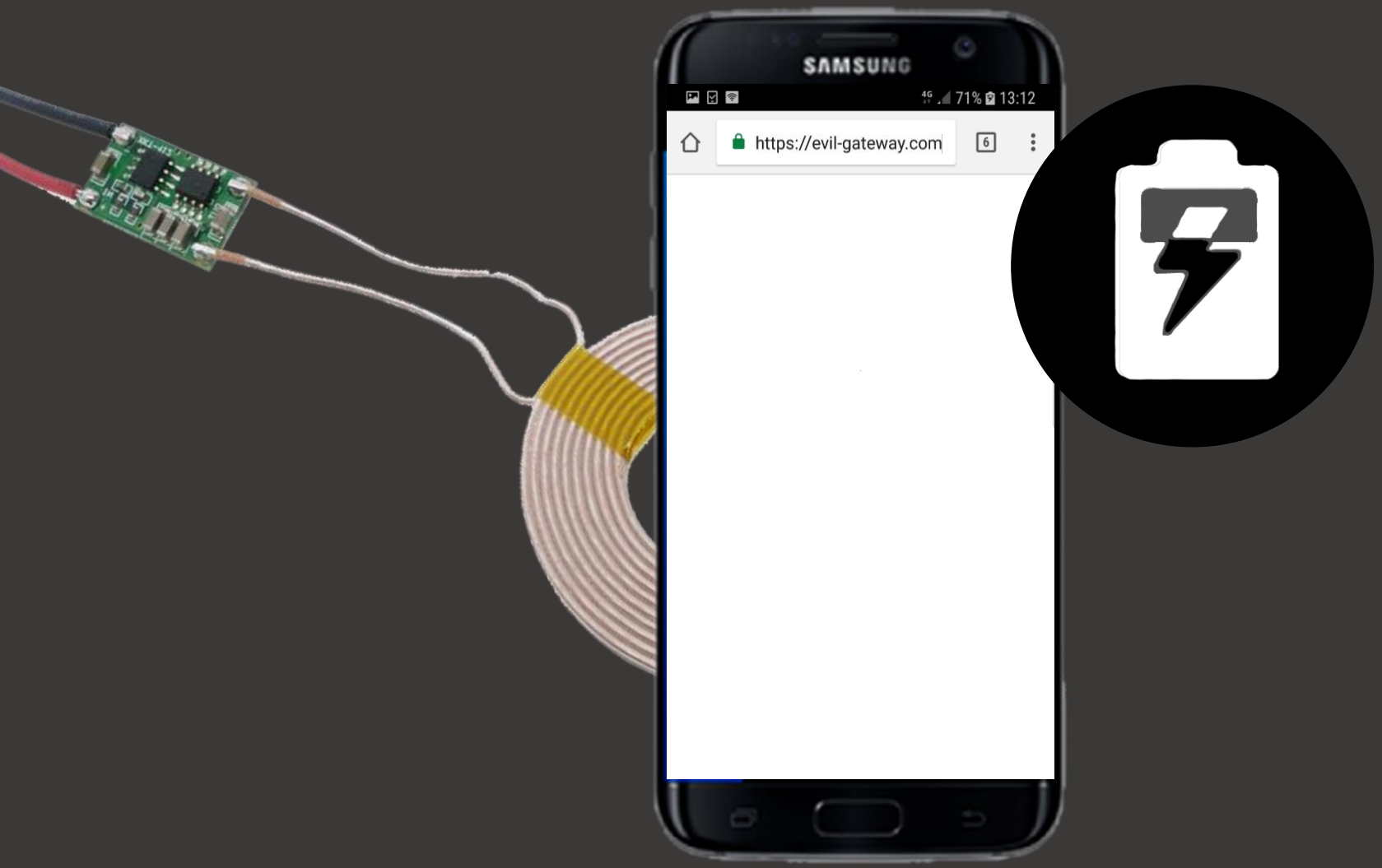
COMBINATION OF ATTACKS



EXFILTRATION

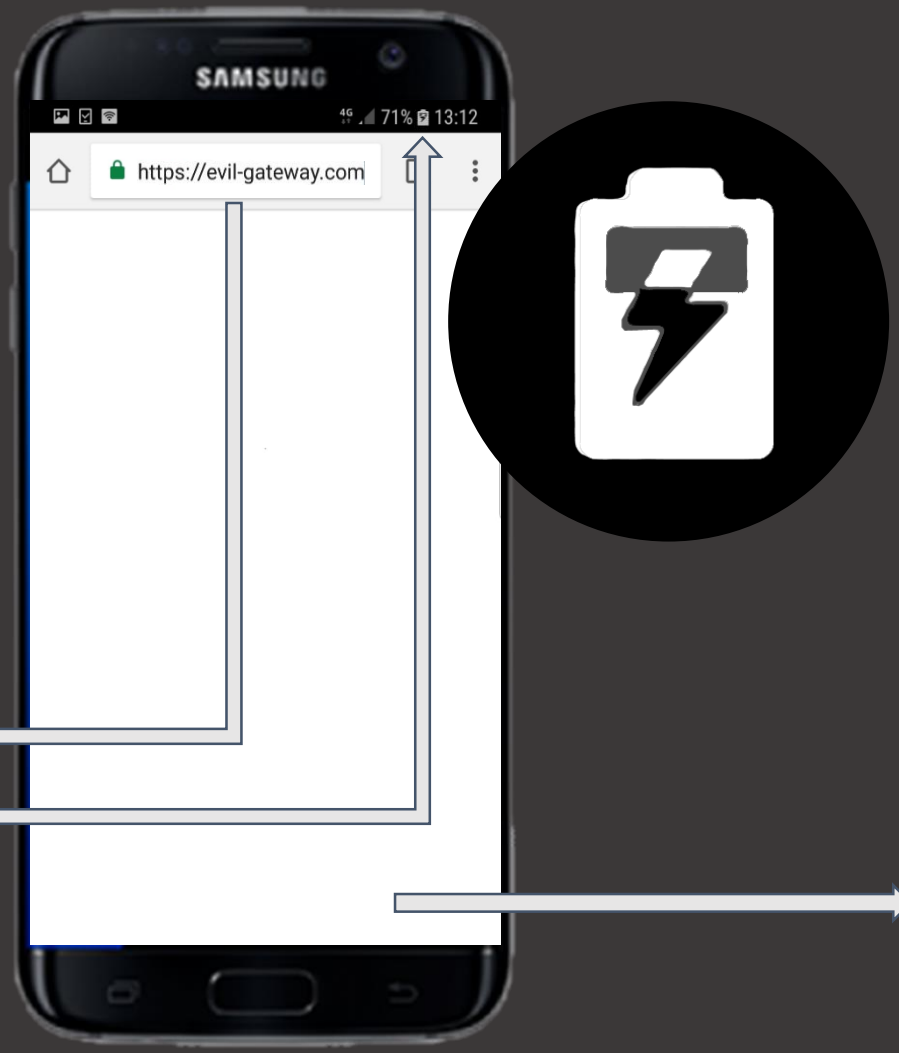
- ✖ Wifi / Bluetooth
- ✖ Manipulate voltage
  - ✖ App
  - ✖ Battery Status API

EXFILTRATION

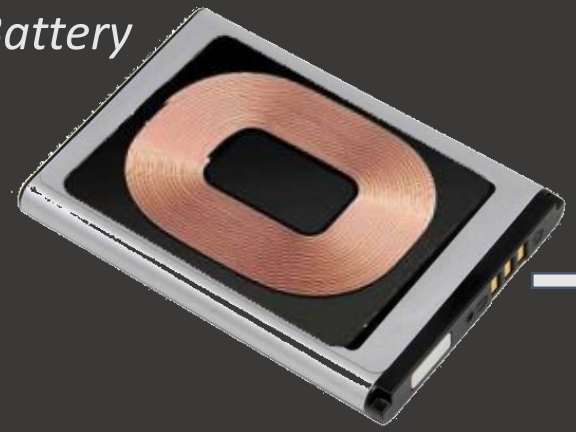


Victim

EXFILTRATION



Malicious Battery



Victim

Attacker

SEE PAPER FOR -

- Attacks – (Sections 6 & 7)
  - Web fingerprinting (open-world, Alexa top 100%)
  - Keystroke
  - Camera
  - Incoming calls
- Robustness analysis - (Section 8)
  - Network conditions
  - Sample rate
  - Browsers
  - Phones
  - Users
- Why Power channel leaks data? (Section 10)
- Defenses & Mitigation (Section 11)

THEORETICAL?!

BUSINESS INSIDER

TECH FINANCE POLITICS STRATEGY LIFE INTELLIGENCE ALL

The companies that make your smartphone batteries say they should barely last a year

Antonio Villas-Boas, Tech Insider Oct. 16, 2015, 1:30 PM

Business Insider

The manufacturers that make your smartphone's lithium-ion battery say it'll have a lifespan of 300-500 charging cycles, according to Battery University, a leading resource for information on batteries.

Every time you plug in your phone to charge when its below 70%, it goes through a "charging cycle."

THEORETICAL?!

Counterfeit Cell Phone & Laptop Batteries

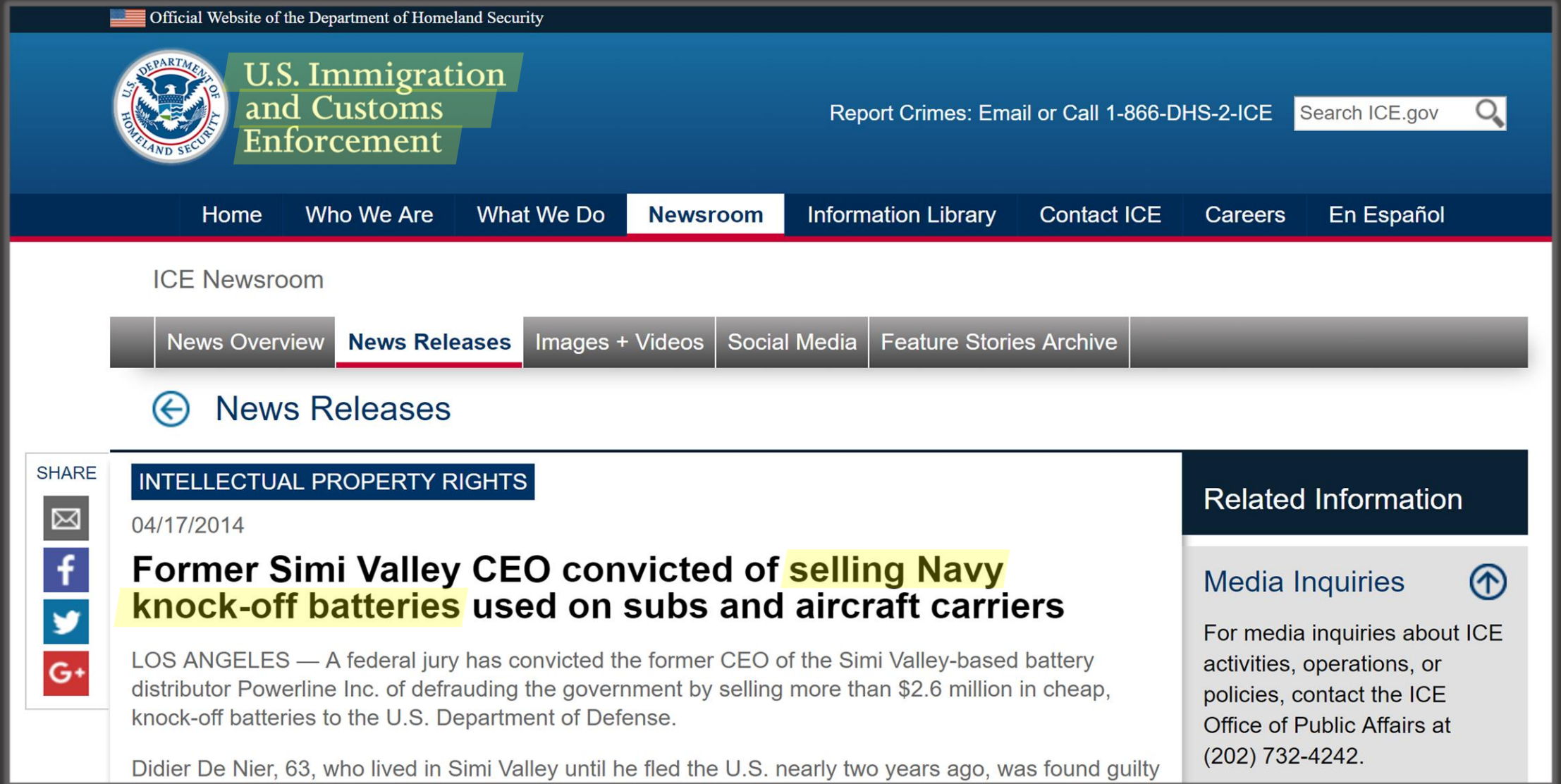
Caution, Credibility, Causes and Cures

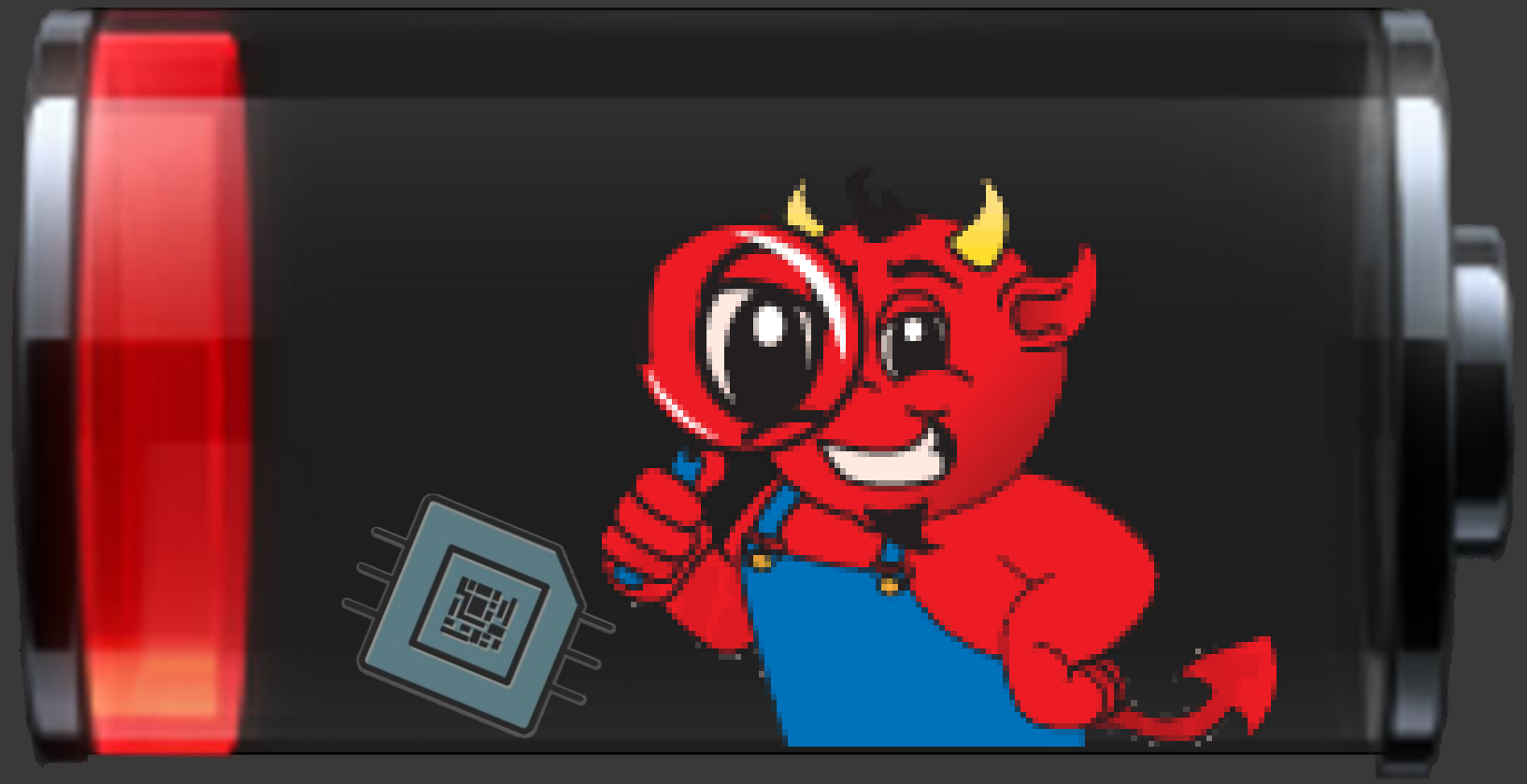
by Shirley Georgi

Examples are shown of the recent Consumer Product Safety Commission (CSPC) battery related safety recalls. Although there is no accurate report of the number of counterfeit/defective batteries that are currently in the U.S., or seized at point of arrival, the CSPC does keep track of the numbers in its recalls. This year a total of 1,190,000 cell phone batteries (Lithium-ion) were in the hands of the consumer before they were recalled as being potentially dangerous, potentially causing injury if overheating, venting and/or exploding. In addition, another 28,000 laptop batteries had to be recalled for the same reasons.+

...re shown of the recent Consumer Product Sa...
...mission (CSPC) battery related safety recalls. Although th...
...ccurate report of the number of counterfeit/defective batteries th...
are currently in the U.S., or seized at point of arrival, the CSPC does
keep track of the numbers in its recalls. This year a total of 1,190,000
cell phone batteries (Lithium-ion) were in the hands of the consumer
before they were recalled as being potentially dangerous, potentially
causing injury if overheating, venting and/or exploding. In additio...
...ther 28,000 laptop batteries had to be recalled for the same

THEORETICAL?!





QUESTIONS?

Pavel Lifshits, *pavell@ef.technion.ac.il*

Mark Silberstein, *mark@ee.technion.ac.il*