Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage

Patrick Cronin*, Xing Gao*, Chengmo Yang*, Haining Wang+

University of Delaware*, Virginia Tech+

30th USENIX Security Symposium (USENIX Security 21), 2021

汇报人：蒋嘉欣

Patrick T Cronin

University of Delaware
在 udel.edu 的电子邮件经过验证
Computer Engineering

A mutual auditing framework to protect IoT against hardware Trojans C Liu, P Cronin, C Yang 2016 21st Asia and South Pacific design automation conference (ASP-DAC), 69-74	41	2016
{Charger-Surfing}: Exploiting a power line {Side-Channel} for smartphone information leakage P Cronin, X Gao, C Yang, H Wang 30th USENIX Security Symposium (USENIX Security 21), 681-698	39	2021
A fetching tale: Covert communication with the hardware prefetcher P Cronin, C Yang 2019 IEEE International Symposium on Hardware Oriented Security and Trust ...	22	2019
Fine-tuning CLB placement to speed up reconfigurations in NVM-based FPGAs Y Xue, P Cronin, C Yang, J Hu 2015 25th International Conference on Field Programmable Logic and ...	19	2015
Routing path reuse maximization for efficient NV-FPGA reconfiguration Y Xue, P Cronin, C Yang, J Hu 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 360-365	16	2016
An exploration of ARM system-level cache and GPU side channels P Cronin, X Gao, H Wang, C Cotton Proceedings of the 37th Annual Computer Security Applications Conference ...	15	2021
Securing cyber-physical systems from hardware trojan collusion C Liu, P Cronin, C Yang IEEE Transactions on Emerging Topics in Computing 8 (3), 655-667	11	2017
Lowering the barrier to online malware detection through low frequency sampling of HPCs P Cronin, C Yang 2018 IEEE International Symposium on Hardware Oriented Security and Trust ...	9	2018
'The danger of sleeping', an exploration of security in non-volatile processors P Cronin, C Yang, D Zhou, K Qiu, X Shi, Y Liu 2017 Asian Hardware Oriented Security and Trust Symposium (AsianHOST), 121-126	9	2017
Time-print: Authenticating USB flash drives with novel timing fingerprints P Cronin, X Gao, H Wang, C Cotton 2022 IEEE Symposium on Security and Privacy (SP), 1002-1017	8	2022
A crowd-based explosive detection system with two-level feedback sensor calibration C Yang, P Cronin, A Agambayev, S Ozev, AE Cetin, A Orailoglu Proceedings of the 39th International Conference on Computer-Aided Design, 1-9	8	2020
Reliability and security in non-volatile processors, two sides of the same coin P Cronin, C Yang, Y Liu 2018 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 112-117	7	2018
A collaborative defense against wear out attacks in non-volatile processors P Cronin, C Yang, Y Liu Proceedings of the 55th Annual Design Automation Conference, 1-6	7	2018
Covert data exfiltration using light and power channels P Cronin, C Gouert, D Mouris, NG Tsoutsos, C Yang 2019 IEEE 37th International Conference on Computer Design (ICCD), 301-304	5	2019
Non-volatile memories in FPGAs: Exploiting logic similarity to accelerate reconfiguration and increase programming cycles Y Xue, P Cronin, C Yang, J Hu 2015 IFIP/IEEE International Conference on Very Large Scale Integration ...	5	2015
A low overhead solution to resilient assembly lines built from legacy controllers P Cronin, FS Hosseini, C Yang IEEE Embedded Systems Letters 10 (3), 103-106	4	2018
Investigating mobile and peripheral side channels for attack and defense PT Cronin University of Delaware		2021

Xing Gao

Assistant Professor, University of Delaware
在 udel.edu 的电子邮件经过验证 - 首页

Security Mobile Computing Cloud Computing

Containerleaks: Emerging security threats of information leakages in container clouds X Gao, Z Gu, M Kayaalp, D Pendarakis, H Wang 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems ...	165	2017
Packet injection attack and its defense in software-defined networks S Deng, X Gao, Z Lu, X Gao IEEE Transactions on Information Forensics and Security 13 (3), 695-705	97	2017
Exploiting eye tracking for smartphone authentication D Liu, B Dong, X Gao, H Wang Applied Cryptography and Network Security: 13th International Conference ...	66	2015
Houdini's escape: Breaking the resource rein of linux control groups X Gao, Z Gu, Z Li, H Jamjoom, C Wang Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications ...	60	2019
A study on the security implications of information leakages in container clouds X Gao, B Steenkamer, Z Gu, M Kayaalp, D Pendarakis, H Wang IEEE Transactions on Dependable and Secure Computing 18 (1), 174-191	53	2018
DoS vulnerabilities and mitigation strategies in software-defined networks S Deng, X Gao, Z Lu, Z Li, X Gao Journal of Network and Computer Applications 125, 209-219	51	2019
{Charger-Surfing}: Exploiting a Power Line {Side-Channel} for Smartphone Information Leakage P Cronin, X Gao, C Yang, H Wang 30th USENIX Security Symposium (USENIX Security 21), 681-698	39	2021
Reduced Cooling Redundancy: A New Security Vulnerability in a Hot Data Center. X Gao, Z Xu, H Wang, L Li, X Wang NDSS	37	2018
E-android: A new energy profiling tool for smartphones X Gao, D Liu, D Liu, H Wang, A Stavrou 2017 IEEE 37th international conference on distributed computing systems ...	31	2017
Pmdroid: Permission supervision for android advertising X Gao, D Liu, H Wang, K Sun 2015 IEEE 34th Symposium on Reliable Distributed Systems (SRDS), 120-129	25	2015
A framework for behavioral biometric authentication using deep metric learning on mobile devices C Wang, Y Xiao, X Gao, L Li, J Wang IEEE Transactions on Mobile Computing 22 (1), 19-36	24	2021
Location privacy breach: Apps are watching you in background D Liu, X Gao, H Wang 2017 IEEE 37th international conference on distributed computing systems ...	20	2017
Detecting passive cheats in online games via performance-skillfulness inconsistency D Liu, X Gao, M Zhang, H Wang, A Stavrou 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems ...	18	2017
Red alert for power leakage: Exploiting intel rapl-induced side channels Z Zhang, S Liang, F Yao, X Gao Proceedings of the 2021 ACM Asia Conference on Computer and Communications ...	17	2021
Evade deep image retrieval by stashing private images in the hash space Y Xiao, C Wang, X Gao Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern ...	17	2020
An Exploration of ARM System-Level Cache and GPU Side Channels P Cronin, X Gao, H Wang, C Cotton Annual Computer Security Applications Conference, 784-795	15	2021
Exploring the Unchartered Space of Container Registry Typosquatting G Liu, X Gao, H Wang, K Sun 31st USENIX Security Symposium (USENIX Security 22), 35-51	14	2022
Why" Some" Like It Hot Too: Thermal Attack on Data Centers X Gao, Z Xu, H Wang, L Li, X Wang Proceedings of the 2017 ACM SIGMETRICS/International Conference on ...	14	2017
Investigating Package Related Security Threats in Software Registries Y Gu, L Ying, Y Pu, X Hu, H Chai, R Wang, X Gao, H Duan 2023 IEEE Symposium on Security and Privacy (SP), 1578-1595	10	2023
Investigating security vulnerabilities in a hot data center with reduced cooling redundancy X Gao, G Liu, Z Xu, H Wang, L Li, X Wang IEEE Transactions on Dependable and Secure Computing 19 (1), 208-226	10	2020

Chengmo Yang

Associate Professor of Electrical and Computer Engineering, University of Delaware
在 udel.edu 的电子邮件经过验证 - 首页

Embedded Systems Fault tolerance Hardware Security Computer Architecture Emerging Memory Technol…

Shielding Heterogeneous MPSoCs From Untrustworthy 3PIPs Through Security- Driven Task Scheduling Chen Liu, Jeyavijayan Rajendran, Chengmo Yang, Ramesh Karri IEEE Transactions on Emerging Topics in Computing 2 (4), 461-472	84	2014
Shielding heterogeneous MPSoCs from untrustworthy 3PIPs through security-driven task scheduling C Liu, J Rajendran, C Yang, R Karri Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), 2013 …	84	2013
A fault-tolerant neural network architecture T Liu, W Wen, L Jiang, Y Wang, C Yang, G Quan Proceedings of the 56th Annual Design Automation Conference 2019, 1-6	68	2019
ExLRU: A unified write buffer cache management for flash memory L Shi, J Li, CJ Xue, C Yang, X Zhou Proceedings of the ninth ACM international conference on Embedded software …	56	2011
Prolonging PCM lifetime through energy-efficient, segment-aware, and wear-resistant page allocation H Aghaei Khouzani, Y Xue, C Yang, A Pandurangi Proceedings of the 2014 international symposium on Low power electronics and …	44	2014
Segment and Conflict Aware Page Allocation and Migration in DRAM-PCM Hybrid Main Memory HA Khouzani, FB Hosseini, C Yang IEEE Transactions on Computer-Aided Design of Integrated Circuits and …	43	2017
A mutual auditing framework to protect IoT against hardware Trojans C Liu, P Cronin, C Yang 2016 21st Asia and South Pacific Design Automation Conference (ASP-DAC), 69-74	41	2016
Exploiting set-level write non-uniformity for energy-efficient NVM-based hybrid cache J Li, L Shi, CJ Xue, C Yang, Y Xu 2011 9th IEEE Symposium on Embedded Systems for Real-Time Multimedia, 19-28	40	2011
Charger-Surfing: Exploiting a Power Line Side-Channel for Smartphone Information Leakage P Cronin, X Gao, C Yang, H Wang 30th USENIX Security Symposium	39	2021
Improving performance and lifetime of DRAM-PCM hybrid main memory through a proactive page allocation strategy HA Khouzani, C Yang, J Hu The 20th Asia and South Pacific Design Automation Conference, 508-513	39	2015
Predictable execution adaptivity through embedding dynamic reconfigurability into static MPSoC schedules C Yang, A Orailoglu Proceedings of the 5th IEEE/ACM international conference on Hardware …	39	2007
Checkpoint-aware instruction scheduling for nonvolatile processor with multiple functional units M Xie, C Pan, J Hu, C Yang, Y Chen The 20th Asia and South Pacific Design Automation Conference, 316-321	34	2015
Toward future systems with nanoscale devices: Overcoming the reliability challenge W Rao, C Yang, R Karri, A Orailoglu Computer 44 (2), 46-53	34	2011
3M-PCM: Exploiting multiple write modes MLC phase change main memory in embedded systems C Pan, M Xie, J Hu, Y Chen, C Yang Proceedings of the 2014 International Conference on Hardware/Software …	30	2014
Minimizing MLC PCM write energy for free through profiling-based state remapping Mengying Zhao, Yuan Xue, Chengmo Yang, Chun Jason Xue Design Automation Conference (ASP-DAC), 2015 20th Asia and South Pacific …	29 *	2015
Leveling to the last mile: Near-zero-cost bit level wear leveling for PCM-based main memory M Zhao, L Shi, C Yang, CJ Xue 2014 IEEE 32nd International Conference on Computer Design (ICCD), 16-21	29	2014
Power efficient branch prediction through early identification of branch addresses C Yang, A Orailoglu Proceedings of the 2006 international conference on Compilers, architecture …	28	2006
A 3.77 TOPS/W convolutional neural network processor with priority-driven kernel optimization J Yue, Y Liu, Z Yuan, Z Wang, Q Guo, J Li, C Yang, H Yang IEEE Transactions on Circuits and Systems II: Express Briefs 66 (2), 277-281	26	2018
Improving MPSoC reliability through adapting runtime task schedule based on time-correlated fault behavior LAR Duque, JMM Diaz, C Yang 2015 Design, Automation & Test in Europe Conference & Exhibition (DATE), 818-823	26	2015
Processor reliability enhancement through compiler-directed register file peak temperature reduction C Yang, A Orailoglu 2009 IEEE/IFIP International Conference on Dependable Systems & Networks …	23	2009

Haining Wang

Professor of ECE, Virginia Tech
在 vt.edu 的电子邮件经过验证

Security Networking Systems Cloud Computing

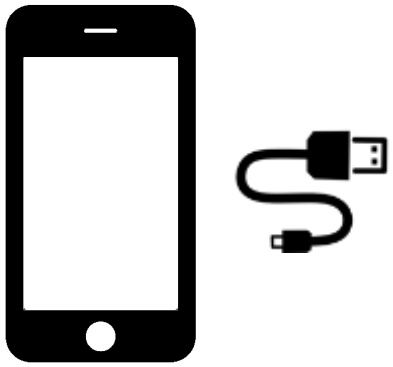
Detecting SYN flooding attacks H Wang, D Zhang, KG Shin Proceedings. Twenty-first annual joint conference of the IEEE computer and …	1023	2002
Detecting automation of twitter accounts: Are you a human, bot, or cyborg? Z Chu, S Gianvecchio, H Wang, S Jajodia IEEE Transactions on dependable and secure computing 9 (6), 811-824	932	2012
Who is tweeting on Twitter: human, bot, or cyborg? Z Chu, S Gianvecchio, H Wang, S Jajodia Proceedings of the 26th annual computer security applications conference, 21-30	772	2010
Hop-count filtering: an effective defense against spoofed DDoS traffic C Jin, H Wang, KG Shin Proceedings of the 10th ACM conference on Computer and communications …	765	2003
Defense against spoofed IP traffic using hop-count filtering H Wang, C Jin, KG Shin IEEE/ACM Transactions on networking 15 (1), 40-53	481	2007
Whispers in the hyper-space: high-bandwidth and reliable covert channel attacks inside the cloud Z Wu, Z Xu, H Wang IEEE/ACM Transactions on Networking 23 (2), 603-615	466	2014
You are how you touch: User verification on smartphones via tapping behaviors N Zheng, K Bai, H Huang, H Wang 2014 IEEE 22nd International Conference on Network Protocols, 221-232	402	2014
Change-point monitoring for the detection of DoS attacks H Wang, D Zhang, KG Shin IEEE Transactions on dependable and secure computing 1 (4), 193-208	359	2004
An efficient user verification system via mouse movements N Zheng, A Paloski, H Wang Proceedings of the 18th ACM conference on Computer and communications …	340	2011
Detecting covert timing channels: an entropy-based approach S Gianvecchio, H Wang Proceedings of the 14th ACM conference on Computer and communications …	262	2007
Enhancing cache robustness for content-centric networking M Xie, I Widjaja, H Wang 2012 Proceedings IEEE INFOCOM, 2426-2434	219	2012
Detecting social spam campaigns on twitter Z Chu, I Widjaja, H Wang Applied Cryptography and Network Security: 10th International Conference …	216	2012
Detecting VoIP floods using the Hellinger distance H Sengar, H Wang, D Wijesekera, S Jajodia IEEE transactions on parallel and distributed systems 19 (6), 794-805	213	2008
Model-based covert timing channels: Automated modeling and evasion S Gianvecchio, H Wang, D Wijesekera, S Jajodia Recent Advances in Intrusion Detection: 11th International Symposium, RAID …	209	2008
Acquisitional rule-based engine for discovering {Internet-of-Things} devices X Feng, Q Li, H Wang, L Sun 27th USENIX security symposium (USENIX Security 18), 327-341	179	2018
High fidelity data reduction for big data security dependency analyses Z Xu, Z Wu, Z Li, K Jee, J Rhee, X Xiao, F Xu, H Wang, G Jiang Proceedings of the 2016 ACM SIGSAC conference on computer and communications …	173	2016
An entropy-based approach to detecting covert timing channels S Gianvecchio, H Wang IEEE Transactions on Dependable and Secure Computing 8 (6), 785-797	166	2010
Characterizing insecure JavaScript practices on the web C Yue, H Wang Proceedings of the 18th international conference on World wide web, 961-970	166	2009
Containerleaks: Emerging security threats of information leakages in container clouds X Gao, Z Gu, M Kayaalp, D Pendarakis, H Wang 2017 47th Annual IEEE/IFIP International Conference on Dependable Systems …	165	2017
VoIP intrusion detection through interacting protocol state machines H Sengar, D Wijesekera, H Wang, S Jajodia International Conference on Dependable Systems and Networks (DSN'06), 393-402	150	2006

Charger-Surfing

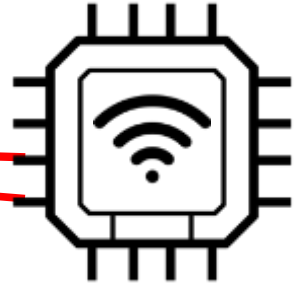
- Shoulder Surfing attack via the charger
- Can we utilize the power signal from a charger to infer what is on the screen?

Attack

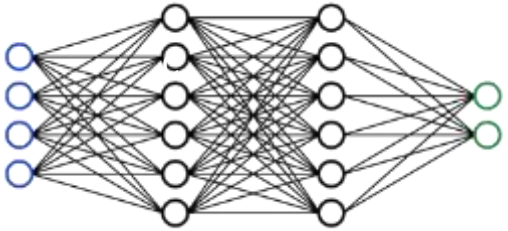
User Plugs Device into Public Charger and Uses as Normal



Attacker Monitors Voltage via hidden probe



Attacker Uses Neural Network to Read User's Presses



1 3 2 7

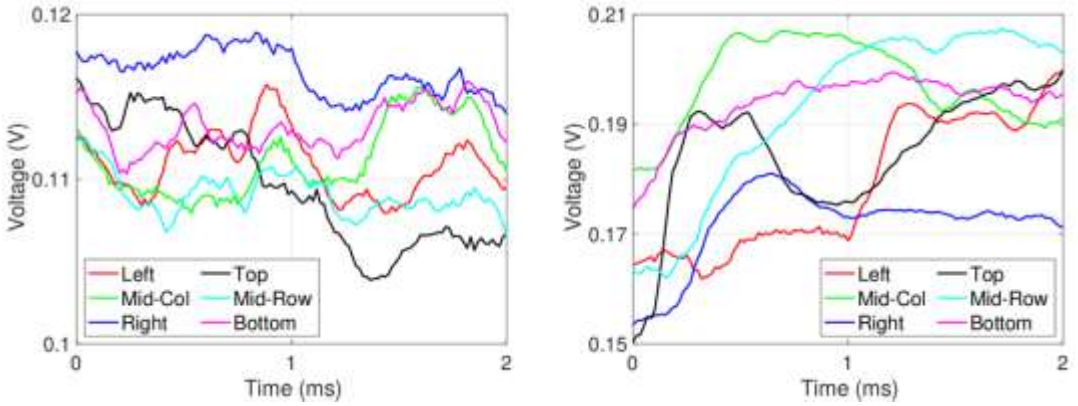
The Threat of Public Charging

- Can an attacker gain any information about the user's activity or private information with just the power trace?
  - Activity/potentially the app [1]
  - Internet browsing [2]

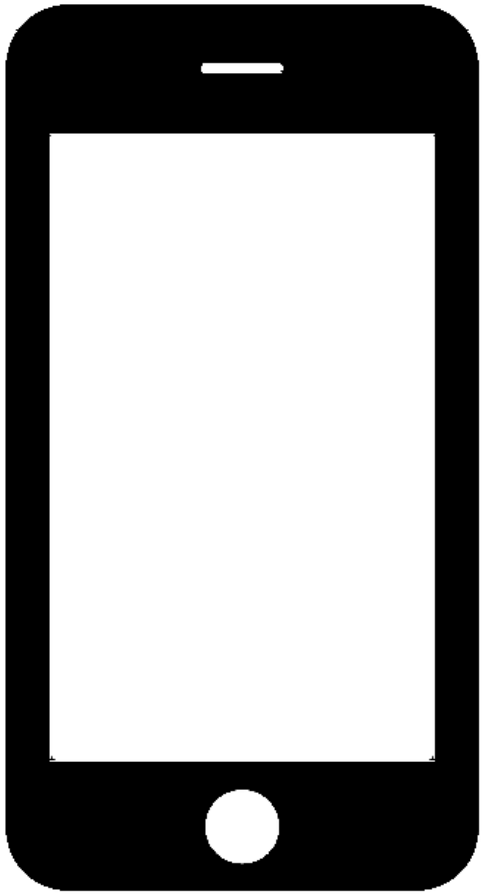
1Yimin Chen, Xiaocong Jin, Jingchao Sun, Rui Zhang, and Yanchao Zhang. POWERFUL: Mobile App Fingerprinting via Power Analysis. In Proceedings of the IEEE Conference on Computer Communications, 2017
2Qing Yang, Paolo Gasti, Gang Zhou, Aydin Farajidavar, and Ki-ran Balagani. On Inferring Browsing Activity on Smartphones via USB Power Analysis Side-Channel. IEEE Transactions on Information Forensics and Security, 2017

Intuition

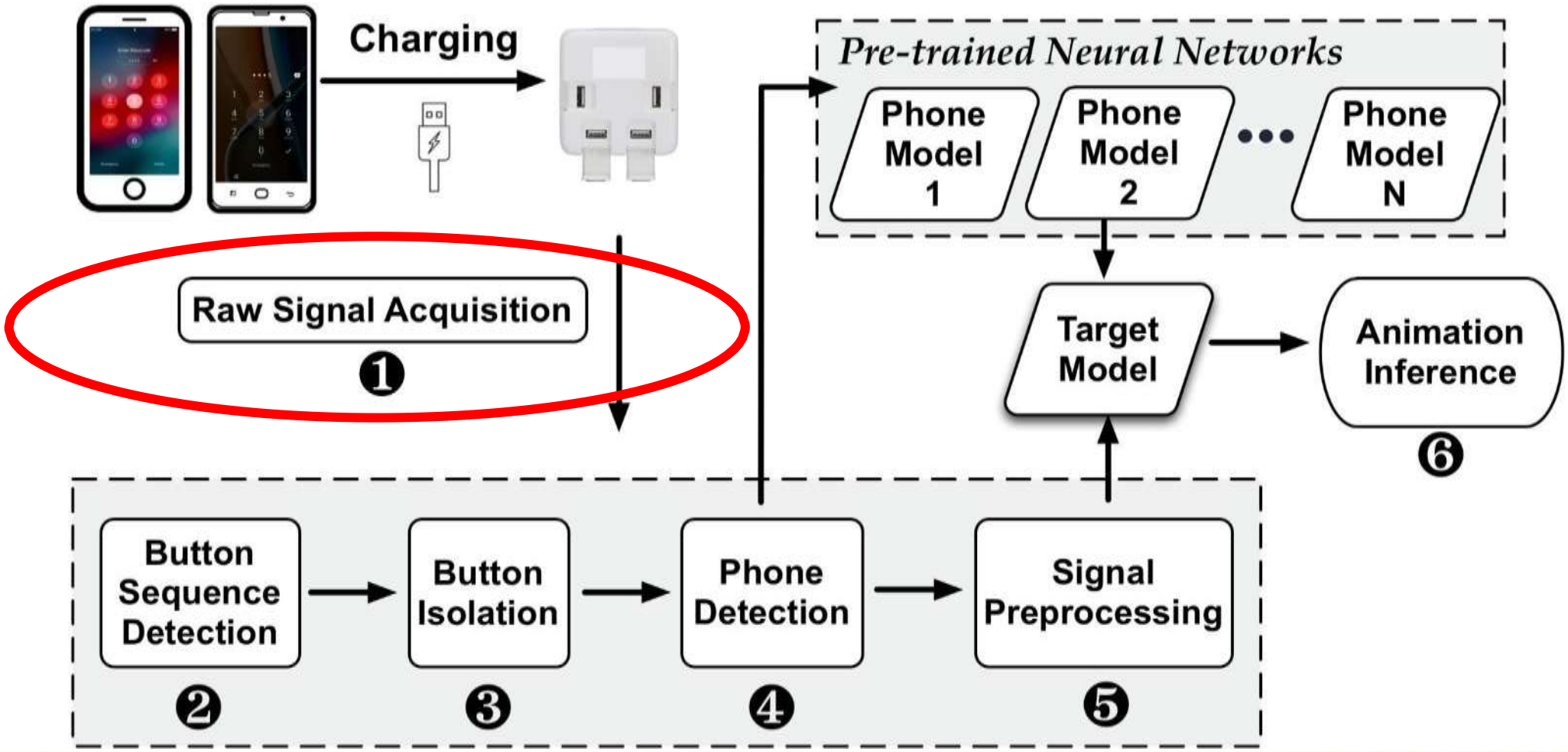
- Phone screen refreshes left to right top to bottom
- Different energy costs to change pixel colors
- Different locations produce different signals



Power signal shape for animations in different locations

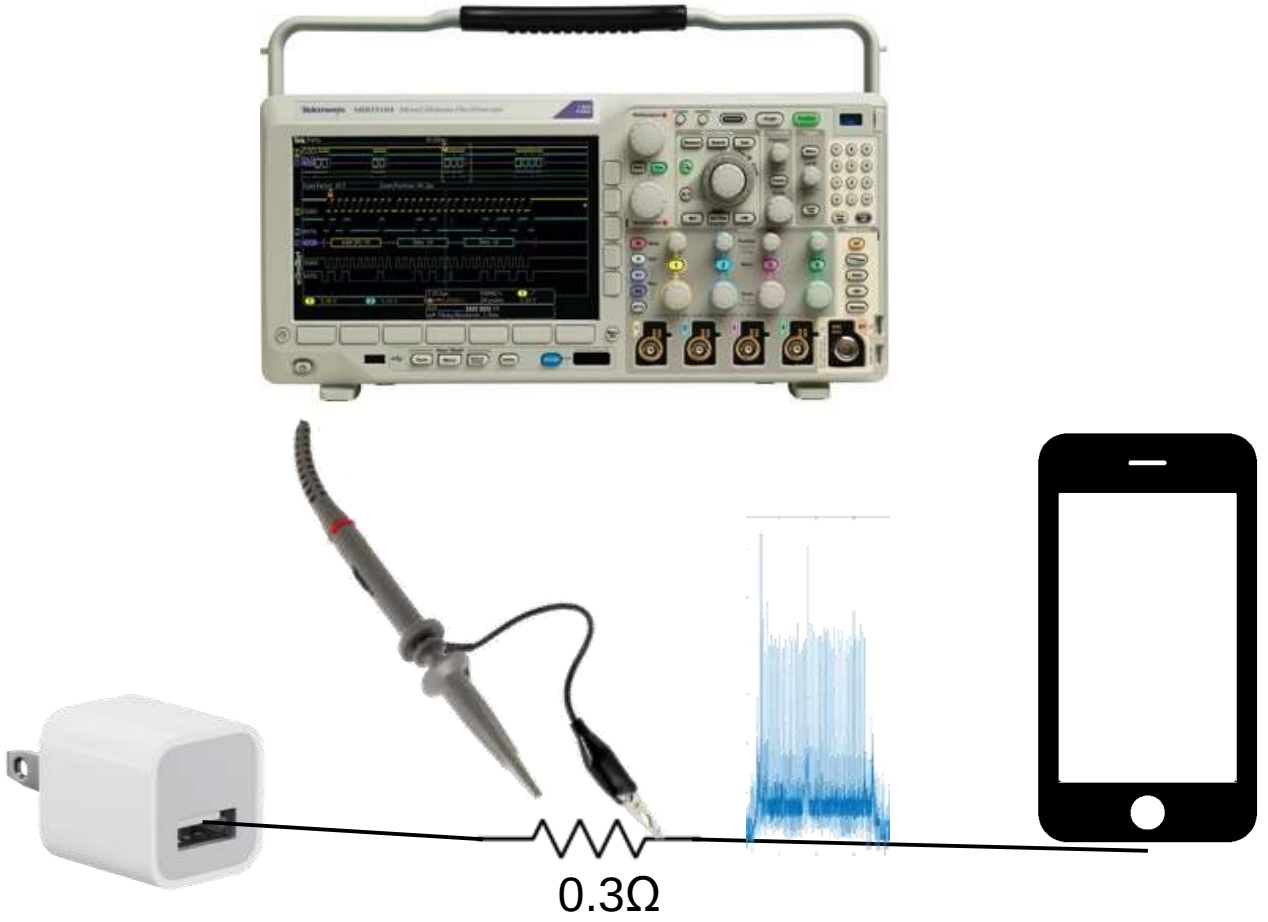


System Design

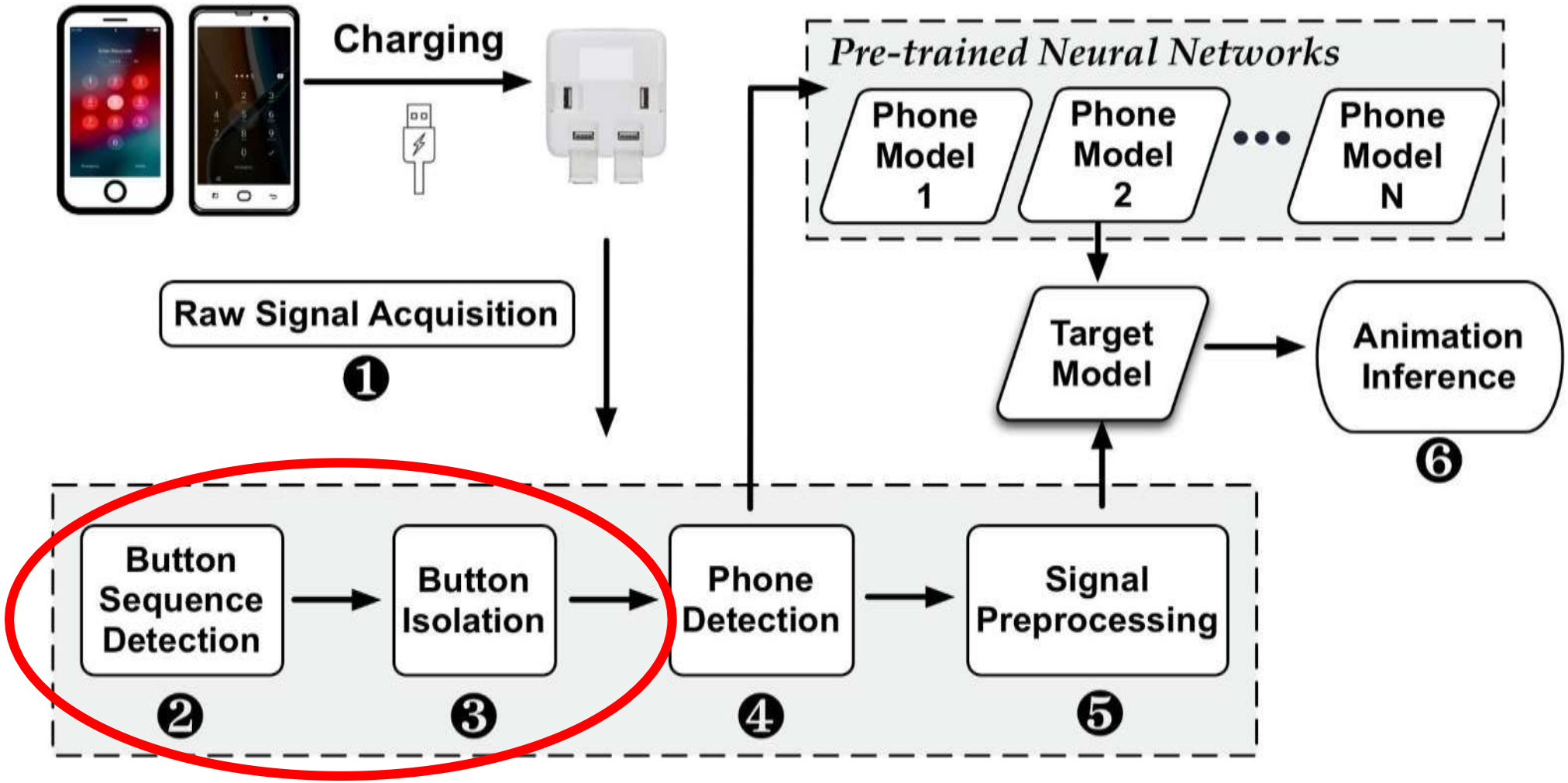


Raw Signal Acquisition

- Oscilloscope / Other Voltage Monitor
- Small resistor inserted into charging cable or circuitry

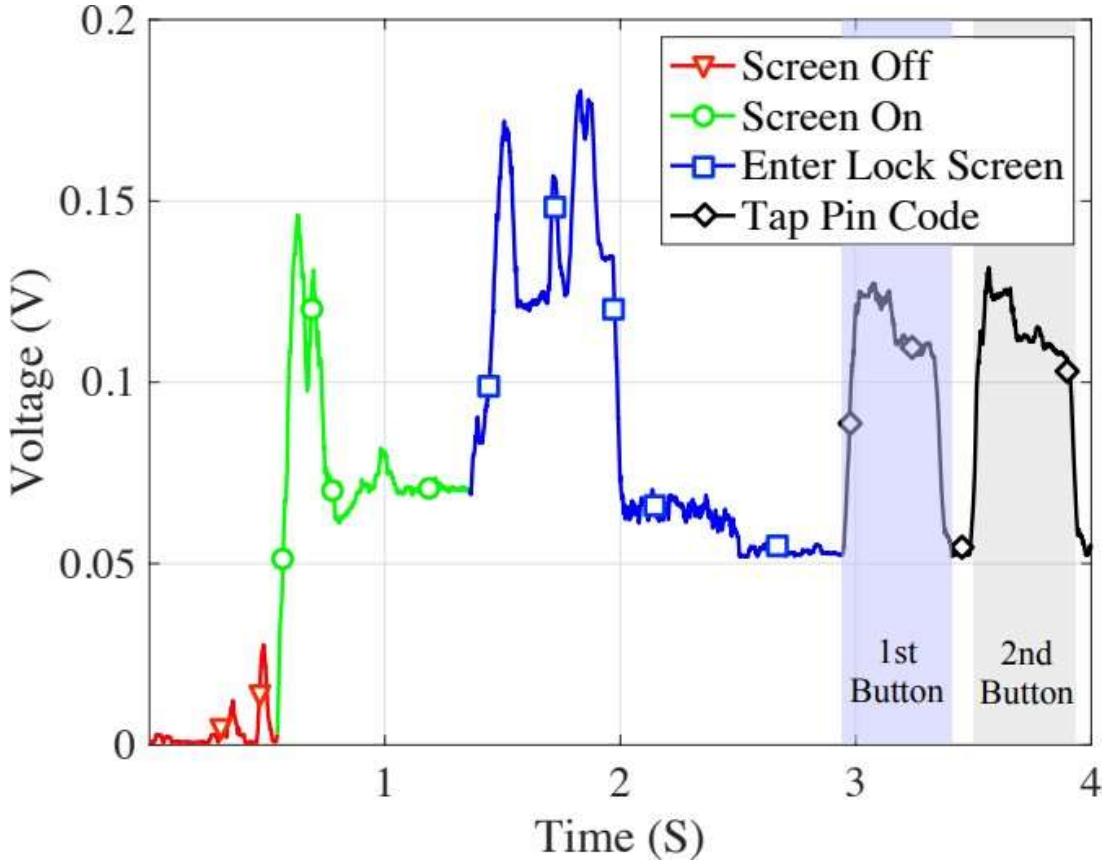


System Design



Detecting Events

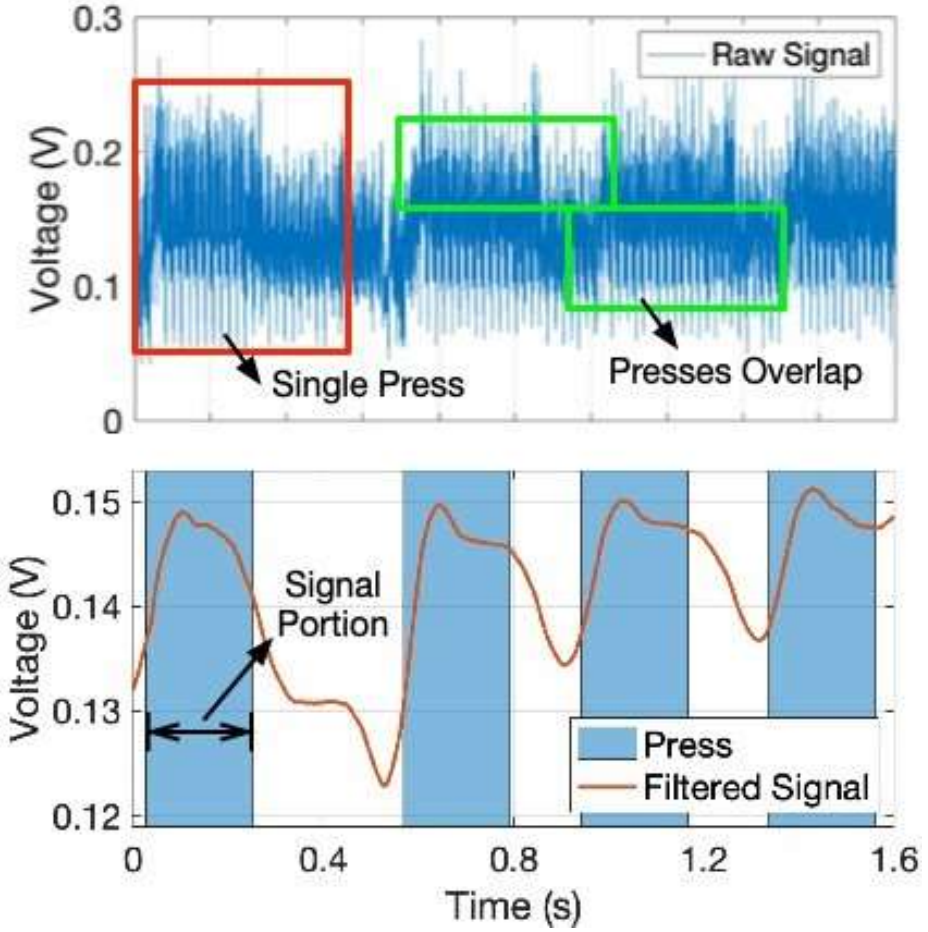
- Different states of the phone screen are observable via just the power trace



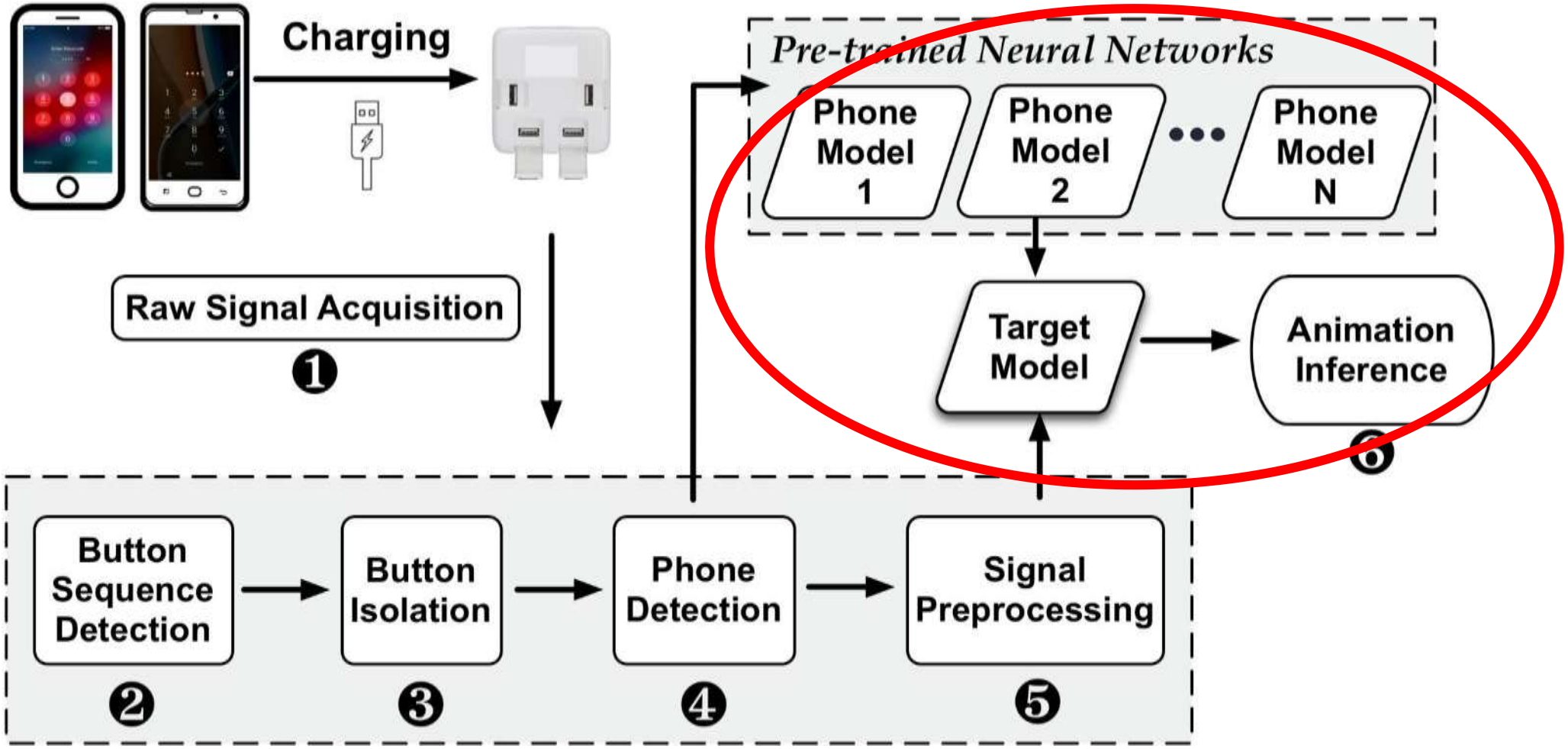
Smoothed Power Trace of Phone Unlock

Preprocessing

- Presses can overlap
- Signal smoothing clearly shows button press actions
- Signal thresholding allows for extraction of each press



System Design



Experimental Goals

- Two goals
  - Demonstrate effectiveness of Charger-Surfing across a wide range of phones with multiple users
  - Demonstrate the transferability of Charger-Surfing across phones of the same model and in a wide range of situations

Broad Analysis
- 4 Different Phones
- Feasibility
- Passcode Inference
- Practicality
- 15 Different Users

Detailed Analysis
- Cross Device Testing
- Configuration Testing
- Defenses
- 33 users

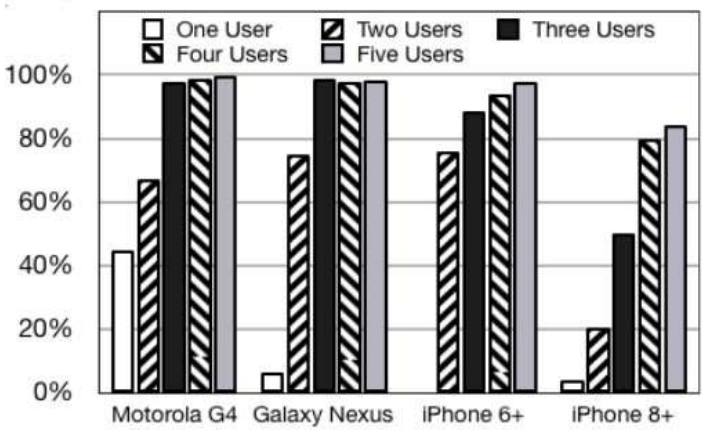
Broad Analysis

- Vary the number of training users
- Diminishing returns as more users are added
- 98.7% accuracy with 5 training users
- Variations in the way users tap the screen lead to the necessity of more training users

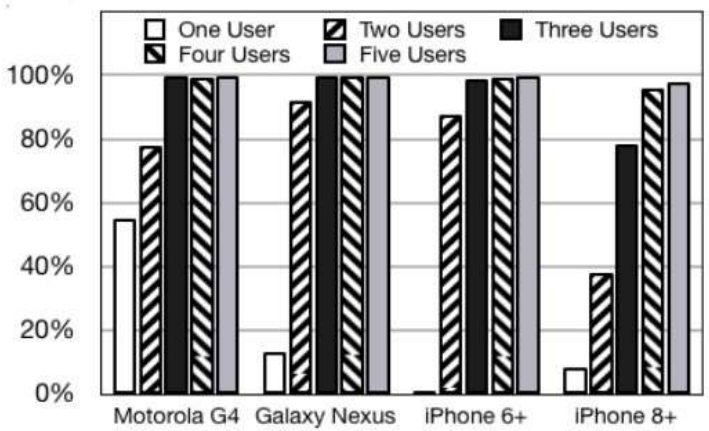
# of Training Users	Phone			
	Motorola G4	Galaxy Nexus	iPhone 6+	iPhone 8+
1	82.0%	50.0%	23.8%	44.6%
2	90.0%	95.0%	93.3%	67.1%
3	99.6%	99.1%	96.9%	88.7%
4	99.7%	99.4%	98.5%	94.5%
5	99.9%	99.6%	99.5%	95.8%

4-Digit Passcode Inference

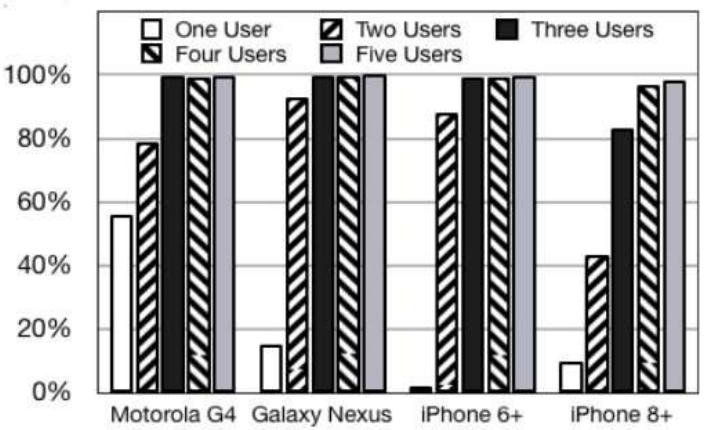
- Examine accuracy across multiple button presses and guesses
- 95.1% success on the first attempt and 99.5% success on the tenth trial with five training users



(a) 1st Trial



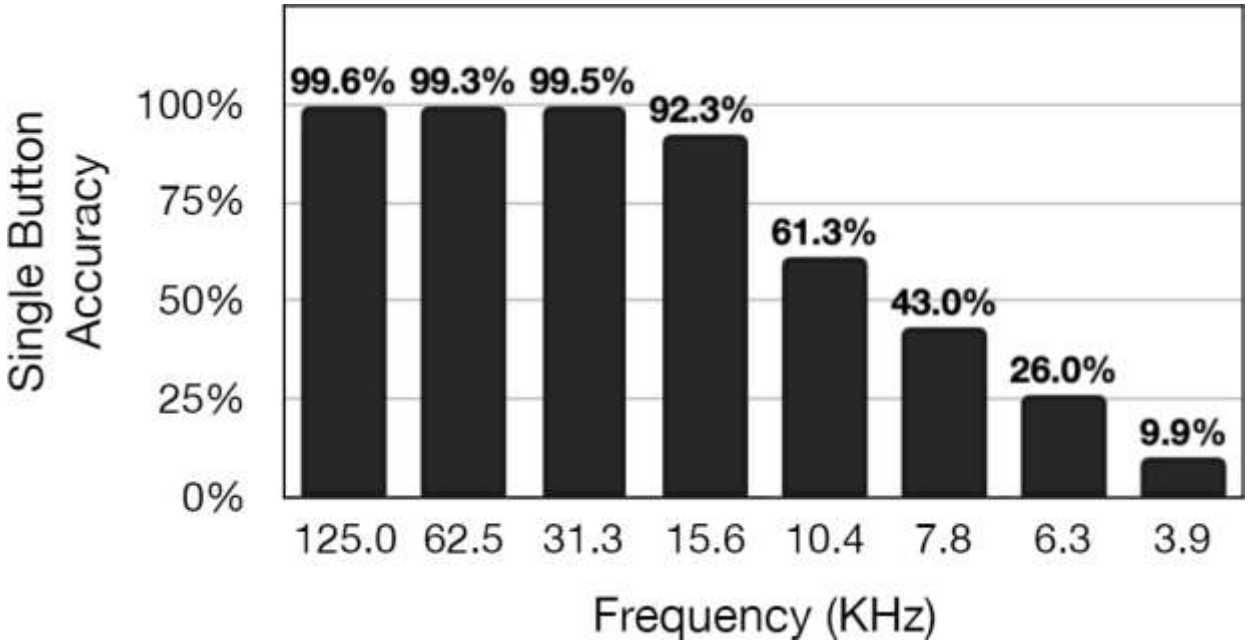
(b) 5th Trial



(c) 10th Trial

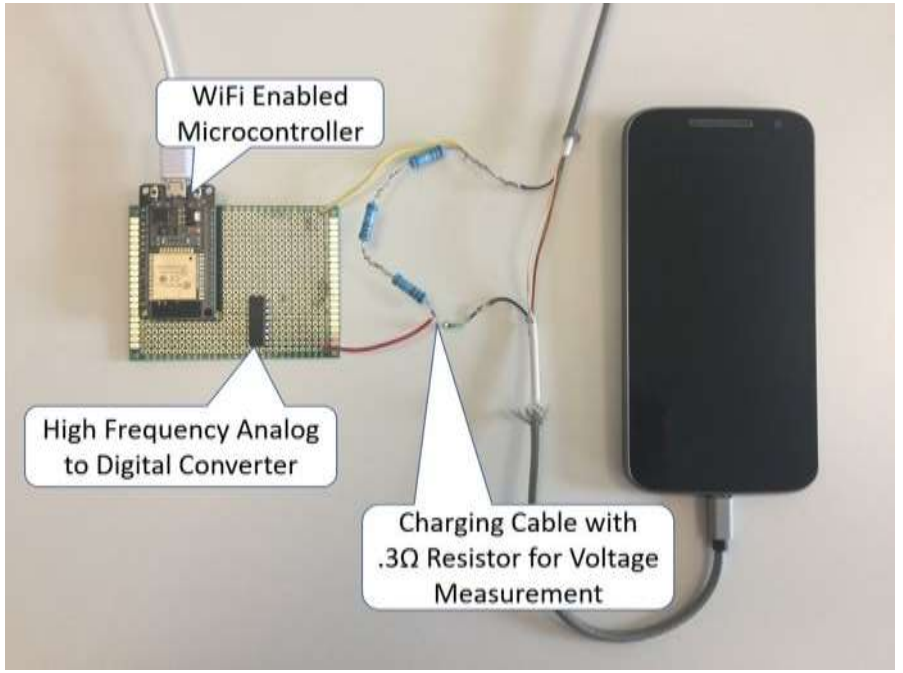
Feasibility Analysis

- Expensive and impractical to use an oscilloscope!
- Sampling frequency can determine practicality of attack
- Minimal accuracy loss with sampling frequency above 31.3KHz



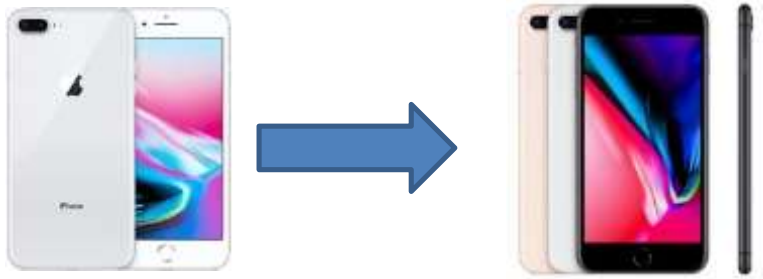
Low Cost Attack

- ESP32 WiFi/Bluetooth enabled Microcontroller
- Analog Devices AD7813 Analog to Digital Converter
- Cost < $20



Detailed Analysis

- Able to attack users on different phones
- Able to attack users with different settings
  - Brightness
  - Wallpaper
  - Haptics
  - Charge levels
- Defenses?



Cross Device Experiments

- Attacker won't have access to victim's phone beforehand!

Train on one phone

Attack different phone?

Cross Device Results

- Minimal accuracy loss when trained on one device and tested on different device

Attempt	Single Button Press
1	99.1%
2	99.4%
3	99.4%

Trial	Passcode	
	4-Digit	6-Digit
1	96.5%	94.6%
5	97.4%	95.6%
10	97.4%	96.2%

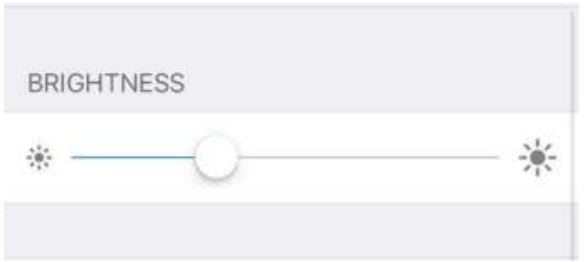
iPhone 6+

Attempt	Single Button Press
1	99.7%
2	99.8%
3	99.8%

Trial	Passcode	
	4-Digit	6-Digit
1	99.0%	98.6%
5	99.1%	98.6%
10	99.1%	98.7%

iPhone 8+

Attack Effectiveness

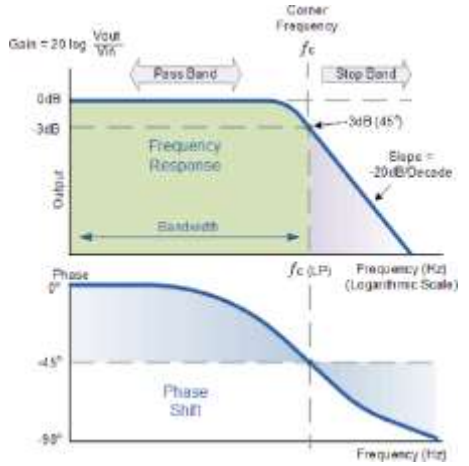


- Minimal impact of differing phone conditions!

Configuration	Static Wallpaper		Brightness			Charge	Haptics
	1	2	0%	50%	100%		
Accuracy (1st Attempt)	99.3%	98.0%	98.0%	97.3%	100%	99.2%	100%

Countermeasures?

- Can Charger-Surfing be defended against?
  - Add noise?
    - Live Wallpaper
  - Filter power output?
    - Power Filter



Thank You!