S^3: Side-Channel Attack on Stylus Pencil through Sensors

HABIBA FARRUKH, Purdue University, USA
TINGHAN YANG, Purdue University, USA
HANWEN XU, Tsinghua University, China
YUXUAN YIN, Tsinghua University, China
HE WANG, Purdue University, USA
Z. BERKAY CELIK, Purdue University, USA

With smart devices being an essential part of our everyday lives, unsupervised access to the mobile sensors' data can result in a multitude of side-channel attacks. In this paper, we study potential data leaks from Apple Pencil (2^{nd} generation) supported by the Apple iPad Pro, the latest stylus pen which attaches to the iPad body magnetically for charging. We observe that the Pencil's body affects the magnetic readings sensed by the iPad's magnetometer when a user is using the Pencil. Therefore, we ask: *Can we infer what a user is writing on the iPad screen with the Apple Pencil, given access to only the iPad's motion sensors' data?* To answer this question, we present **S**ide-channel attack on **S**tylus pencil through **S**ensors (S^3), a system that identifies what a user is writing from motion sensor readings. We first use the sharp fluctuations in the motion sensors' data to determine when a user is writing on the iPad. We then introduce a high-dimensional particle filter to track the location and orientation of the Pencil during usage. Lastly, to guide particles, we build the Pencil's magnetic map serving as a bridge between the measured magnetic data and the Pencil location and orientation. We evaluate S^3 with 10 subjects and demonstrate that we correctly identify 93.9%, 96%, 97.9%, and 93.33% of the letters, numbers, shapes, and words by only having access to the motion sensors' data.

CCS Concepts: • **Security and privacy → Access control**.

Additional Key Words and Phrases: side-channel attack, user privacy, stylus pencils

ACM Reference Format:
Habiba Farrukh, Tinghan Yang, Hanwen Xu, Yuxuan Yin, He Wang, and Z. Berkay Celik. 2021. S^3: Side-Channel Attack on Stylus Pencil through Sensors. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 5, 1, Article 8 (March 2021), 25 pages. https://doi.org/10.1145/3448085

1 INTRODUCTION

Modern-day smart devices come embedded with various sensors, enabling a vast range of applications in activity recognition, context awareness, mobile health, and productivity. Unfortunately, these sensors are also gateways for unintended information leakage about users' activities. Unauthorized access to users' personal information, habits, behaviors, and preferences through sensor data has long been a major security and privacy concern.

Authors' addresses: Habiba Farrukh, hfarrukh@purdue.edu, Purdue University, 305 N. University St, West Lafayette, IN, USA, 47907; Tinghan Yang, yang1683@mpurdue.edu, Purdue University, 305 N. University St, West Lafayette, IN, USA, 47907; Hanwen Xu, xuhw20@mails.tsinghua.edu.cn, Tsinghua University, Beijing, China; Yuxuan Yin, yin-yx16@tsinghua.org.cn, Tsinghua University, Beijing, China; He Wang, hw@purdue.edu, Purdue University, 305 N. University St, West Lafayette, IN, USA, 47907; Z. Berkay Celik, zcelik@purdue.edu, Purdue University, 305 N. University St, West Lafayette, IN, USA, 47907.

2474-9567/2021/3-ART8 $15.00
https://doi.org/10.1145/3448085