Super-Human Cryptanalysis for Scalable Side-Channel Analysis

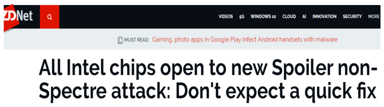
PIs: Berk Sunar (PI), Thomas Eisenbarth (Former Co-PI)

https://www.nsf.gov/awardsearch/showAward?AWD_ID=1814406&HistoricalAwards=false

Proposed Micro-architectural Attacks

New Intel CPU Vulnerabilities Discovered:

- **Spoiler:** Increase the speed of cache attacks by creating eviction sets 256 times faster and conducting Rowhammer attacks much efficiently (CVE-2019-0162)
- **Zombieload:** A novel Meltdown-type attack, which steals sensitive data and encryption keys from buffers while the computer accesses them (CVE-2018-12130)
- **Fallout:** Store buffers leak personal data and ASLR can be bypassed (CVE-2018-12126)
- Micro-architectural attacks are still a huge threat to public security and privacy!



ZDNet VIDEOS 5G WINDOWS 10 CLOUD AI INNOVATION SECURITY MORE

MUST READ: Gaming, photo apps in Google Play infect Android handsets with malware

All Intel chips open to new Spoiler non-Spectre attack: Don't expect a quick fix

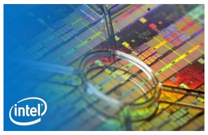
FORTUNE

TECH • CYBERSECURITY

'Zombieload' Flaw Lets Hackers Crack Almost Every Intel Chip Back to 2011. Why's It Being Downplayed?

Challenges

- Side Channel Attacks steal personal information
- The attacks evolve and new attacks are introduced
- It is difficult to patch each leakage in silicon
- A generic approach is required to detect and prevent side-channel attacks



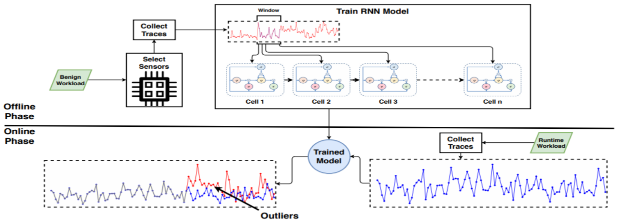
Scientific Impacts

- Side-channel attacks are more efficient when **Deep Learning** is used to analyze the raw traces
- **FortuneTeller** detects the current microarchitectural side-channel attacks and possible future attacks by training **unsupervised LSTM** models
- **Adversarial example techniques** can be used to craft artificial traffic to fool the ML-based classifiers
- **DeepCloak** is a sophisticated countermeasure against micro-architectural attacks

Proposed Countermeasures

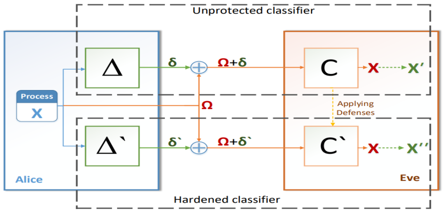
FortuneTeller

- LSTM model is trained with benign execution traces
- Performance counter data from Intel processors
- Micro-architectural attacks detected with F-score 0.99
- Real-time detection with low performance overhead



DeepCloak

- Adversarial traffic crafted to fool ML classifier Adversaries
- Crypto implementations classified by training a CNN model
- DeepCloak is immune to adversarial re-training and defensive distillation



Impact on Society

- Automating the side-channel security analysis using deep learning techniques
- Providing a thorough and scalable solution to perform security reviews without human intervention
- Creating the perfect education environment at the intersection of security and AI

Impact on Education

- Training experts at the intersection of two critical technologies, i.e. cybersecurity and AI
- AI-Cybersecurity integrated courses are given at WPI
- Disseminating our findings in premier AI and Security conferences and research group visits
- New AI techniques are always followed to increase the efficiency of both attacks and detection systems

Potential Impact

- Side-channel analysis researchers would integrate AI to their automations in the industry
- Adversarial learning would be considered deeply in the attack creation
- The proposed dynamic detection techniques would be integrated to real-time systems

The 4th NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting (2019 SaTC PI Meeting)
October 28-29, 2019 I Alexandria, Virginia