1 Introduction: Part 1

1.1 Problem Statement

In a technology centric world, cybersecurity is crucial to ensuring consumer privacy of information. Some microarchitecture-based malware attacks cannot be detected using current existing software – causing a breach of security and loss of privacy. Major chip manufacturers and cloud computing providers need a way to identify and differentiate these attacks from benign signals in order to ensure consumer privacy. These attacks can happen at any given time, making it difficult to consistently and accurately identify them. Thus, our team is creating a software tool that can assess the robustness of an AI based detector against microarchitecture attacks. This will allow companies to strengthen and improve their own software to better detect and quarantine said attacks.

1.2 Intended Users and Uses

Researchers

Researchers focusing on microarchitecture attacks will use our tool to test and further research power-anomaly detection systems.

Key Characteristics

Researchers are the leaders in developing and further exploring microarchitecture vulnerabilities and security solutions. They have a vast knowledge of computer engineering and system security. They are more concerned with the pursuit of knowledge and development of theory than they are with implementing solutions for economic reasons.

Needs

Researchers need a better way to test new microarchitecture attacks against their deep learning power-anomaly detection systems. They must validate that their security systems hold up against evasive microarchitecture attacks.

How they will benefit

With the tool our team is developing, researchers can quickly generate new, highly evasive microarchitecture attacks. Saving them a lot of time implementing it themselves and providing them the tools they need to test their systems.

Implementors

Implementors, such as Intel, AMD, Nvidia, and PaaS providers, will use our tool to test their systems against microarchitecture attacks.

Key Characteristics

Implementors are companies that manufacture chipsets or provide access to computer resources. Vulnerabilities in their products can damage their reputation and be very costly, so they tend to invest heavily in cybersecurity.

Needs

Implementors need a tool to test their products and discover potential vulnerabilities.

How they will benefit

Implementors will be able to penetration test their products with evasive microarchitecture attacks and, as a result, discover existing vulnerabilities.

End Users

End users indirectly benefit by trusting their data with systems tested by our tool.

Key Characteristics

End users are typical everyday computer users. They don't have much knowledge of cybersecurity or the inner workings of the system they are using, and they trust the product they use is secure.

Needs

End users need their data to be secure. They need their personal computer or cloud environment not to be vulnerable to microarchitecture attacks.

How they will benefit

End users can be assured that their private information is secured and inaccessible to non-authorized individuals. They can also have better protection on their personal devices and as well as their cloud environments.