CALIFORNIA STATE SCIENCE FAIR
2015 PROJECT SUMMARY

Name(s)

Neil Movva

Project Number

S0918

Project Title

(In)security Everywhere: Machine Learning Assisted Deep Power Analysis Fundamentally Defeats Software Cryptography

Abstract

Objectives/Goals

Classical computers must use power to perform calculations, and this fundamental fact leaves them vulnerable. Since all data is bound to physical electric charge, a computer#s different inputs and operations leave distinct power signatures, resulting in patterns that can be described and predicted by a Hamming weight model. By monitoring a system's power consumption over time with an oscilloscope, patterns in its power use may be identified and used to infer the contents of #secure# data inside the processor. We present a novel, complete system to automatically monitor a target system and procedurally retrieve randomly generated encryption keys, defeating some of the most common cryptography systems in use today.

Methods/Materials

The use of machine learning (scikit-learn) and other modern compute amenities (simulated annealing) gives our solution unprecedented adaptability and efficiency in defeating security; we limit ourselves to the most basic equipment (50 MHz oscilloscope bandwidth) to demonstrate technique efficiency and the extent of threat potential.

Results

On a 16 MHz AVR microcontroller, we defeat AES-128 security in an average time of 152 seconds. We also demonstrate near-linear time scaling with software complexity, ie. keylengths are directly proportional to solution time. Alternately, increased hardware complexity quickly increases solution time, without a strongly discernible relationship.

Conclusions/Discussion

We discuss the impact of this vulnerability, especially in context of the trend towards ubiquitous embedded processing; finally, we detail potential countermeasures for the techniques presented.

Summary Statement

Modern computers leak sensitive information in their power consumption "signatures;" careful monitoring and analysis of this data with modern machine learning frameworks enables rapid, adaptive defeat of computer security measures.

Help Received

Independent Development