Quantitative Analysis and Reporting of Electromagnetic Covert and Side Channel Vulnerabilities

Georgia Institute of Technology

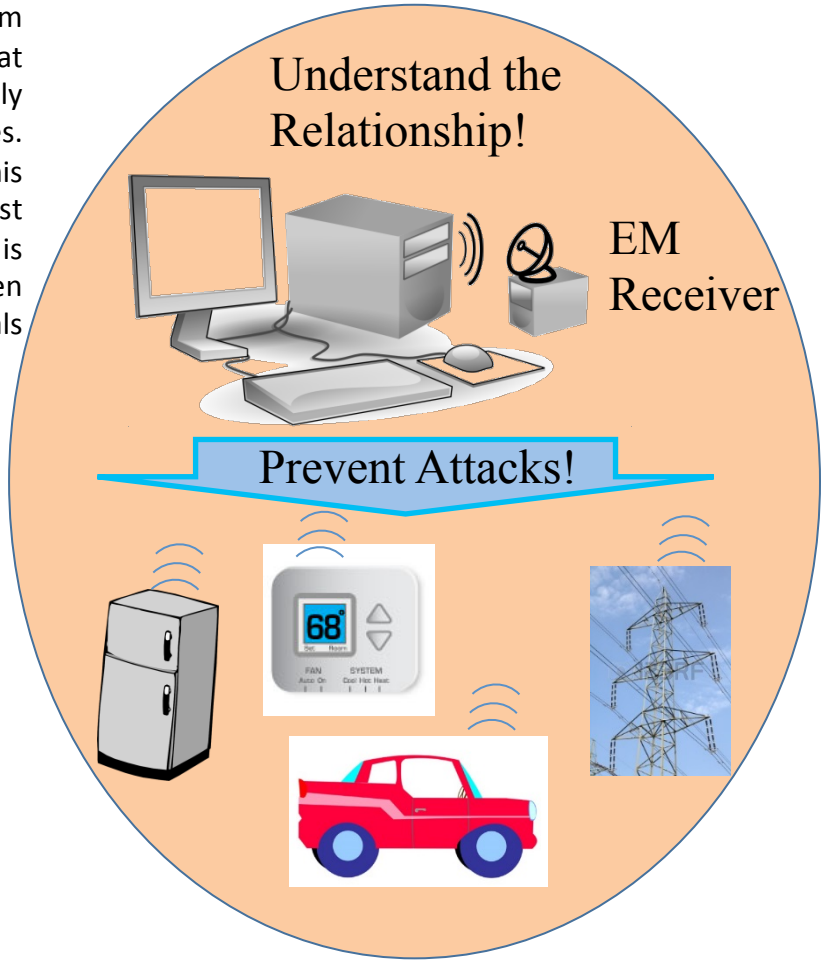
Challenge:

Most approaches to computer system security rely on the assumption that interaction with the system will occur only through one of its explicit I/O interfaces. Covert and side-channel attacks break this assumption, thus circumventing most traditional protection measures. There is not enough knowledge in the open literature on how side-channel signals interact with software.

Solution:

Find relationship between software and emanations

- Method for comparing emanations from individual instructions
- Method for finding where in a spectrum useful signal will appear
- Method for profiling code to verify its execution
- Method for detecting malware in less then 40 ms with accuracy above 90%



Scientific Impact:

This research is the first quantitative and systematic software analysis of EM covert and side channel vulnerabilities. This work will lead to lower risk from future covert- and side-channel attacks, enable management of this risk, and enable future innovation at the intersection of program analysis and design, software/hardware interaction, and computer security. We have already demonstrated some of the benefits of the technology.

Broader Impact:

This research helps increase national security by better understanding covert- and side-channel mechanism of generation and propagation. This understanding as led us to use side-channels to detect malware in IoT devices.

Award 1318934, Georgia Institute of Technology, Alenka Zajic (PI) and Milos Prvulovic (Co-PI)