The Internet of Things (IoT) is an increasingly widespread phenomenon involving computing

devices that interact with the real world and also network with other computers. These types of

devices introduce new security risks, such as cyberattacks that impact the physical world. In spite

of these risks, IoT security has remained underdeveloped, leading to the rise of immense botnets

and footholds in household and corporate networks the world over. Meanwhile, researchers often

use IoT security as a trial ground for blockchain and machine learning, rather than tracking the

attacks happening in the world today and figuring out how to stop them in the future.

This dissertation addresses that gap. It begins with a concrete definition of an IoT device,

then exhuastively surveys IoT device vulnerabilities published over an eighteen-month period. A

thorough analysis of those vulnerabilities guides three paths toward IoT security. The first is an

experimental evaluation of static analyzers based on their ability to detect known vulnerabilities

and their usability by software developers. Next is a set of simple but effective guidelines for IoT

device software developers to prevent or mitigate the most common weaknesses. Last is a series of

hands-on IoT security lab exercises for an undergraduate class to train future security

professionals in how to secure networks that include IoT devices.