Design flaws and implementation bugs are two different types of security defects. Design flaws are errors that occur in the design phase, while implementation bugs are errors that occur in the implementation phase of the product development lifecycle. Unfortunately, the current focus of the security community is more on common implementation bugs than on design flaws even though design flaws constitute 50% of the security defects.

To enhance usability and performance, both application developers and platform vendors are constantly introducing new features (like synchronization features), and often such desires for increased usability/performance results in a violation of secure design principles. This is the reason why most design flaws hide in plain sight as product features. Attackers can take advantage of the unintended consequence of such features to compromise the whole system. This is a different way of exploitation when compared to typical memory corruption bug exploitation. Hence, it is typically difficult to detect, and complex to patch a design flaw compared to an implementation bug — often requiring solutions that are unique to each attack.

This thesis explores design flaws that may occur at the software- and hardware-level of computing systems, and the cyber threats stemming from them. We build novel software-level computer defenses to protect from these identified cyber threats and discuss the cost associated with them. Furthermore, this research is broadened by identifying whether the current set of design principles is comprehensive enough to prevent today’s cyber threats. We achieve this goal by performing an in-depth analysis of a new cyber attack called cryptojacking which does not break today’s widely-accepted security model called CIA triad (standing for Confidentiality, Integrity, and Availability; yet, a very practical and stealthy cyberattack that monetizes a victim’s computational resources. Based on this study, we propose to include least required resource as a new principle to the current set of design principles to offer protection from such futuristic attacks.