EECE 5698-008: Embedded Security
Special Topics: Cyber-Physical Security of IoT Systems in the Age of AI
Instructor: Prof. Kevin Fu
TAs: Hui Zhuang, Nuntipat Narkthong

Handout 7
September 15, 2025

Essay 1

Fault injection attacks were outside the threat model of early smartcards (think the contactless chip inside the Husky Card). Defining security is difficult because security is a non-functional property, effectively a negative goal that cannot be tested to success. We can only test to find failure. Define the specific security properties that must be maintained, and describe the capabilities of the adversary. Further explain how to manage security risks when a product ages into legacy and the threat model shifts, with new vulnerabilities and threats discovered after deployment. Justify your opinion with technical reasoning.

AI Usage Policy:

- Do not use generative AI for generating core ideas.
- AI may only be used to improve writing.
- If you use AI, you must include the prompts you used.

Submission:
Due **Monday, Sep 29** via Canvas before class. Late submissions receive a zero.