ECE 443/518 Fall 2022 - Project 2

Security in the Wild

Report Due: 10/30 (Sun.), by the end of the day (Chicago time)
Late submissions will NOT be graded

I. Objective

A lot of software and hardware products that one may use everyday contain solutions to protect certain aspects of security. In this project, you will study one topic based on published papers and reports to understand the technical details of its security solution and possible issues.

For your convenience, here is a list of papers and reports, each corresponding to a possible topic. Please choose one for your project.

- Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0
- got HW crypto? On the (in)security of a Self-Encrypting Drive series
- Github Gentoo organization hacked: incident report
- The Sorry State of TLS Security in Enterprise Interception Appliances
- The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli
- Smart Home - Smart Hack and TUYA-CONVERT
- Smart Spies: Alexa and Google Home expose users to vishing and eavesdropping
- Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem

If you would like to work on your own choice of topic out of my list, please email me your choice before end of 10/16. Your choice should be based on papers and reports providing similar level of technical details, or I may refuse your choice and direct you to one from my list.

There is no need to email me if your choice is within my list.

II. Deliverables

Submit the following to Blackboard for this project.

1. A project report of no less than 500 words. In particular, please address the items below (you may need to perform additional research online).
    - The threat and the security policy, i.e. what should be protected?
    - Technical details of the security solution or issues with it.
    - Is the security solution effective? Why or why not? If yes, will there be any new threats? If no, how to improve the security solution?

The project should be done individually. You can discuss the project with other students but all the source code and writings should be your OWN. PLAGIARISM and called for DISCIPLINARY ACTION. NEVER share your source code and reports with others.