ILLINOIS TECH

College of Computing

Course Overview

CS 558 Advanced Computer Security

Yue Duan

CS 558: Advanced Computer Security

- Instructor:
  - Yue Duan, Assistant Professor
    - https://yueduan.github.io/
    - yduan12@iit.edu
  - PhD in Computer Science from UC Riverside
  - Postdoctoral training at Cornell University and University of Utah
  - Specialized in software security, AI security and blockchain security.

CS 558: Advanced Computer Security

- Lecture Hours
  - Mon/Wed, 8:35am - 9:50am
- Lecture location
  - Stuart Building 111

Due to my visa issue, classes in the first few weeks will be offered online via Blackboard Collaborate Ultra.

CS 558: Advanced Computer Security

- Office hour:
  - SB 209C, Thursday 9AM-11AM
- Course webpage:
  - https://yueduan.github.io/cs558.html
- piazza signup link:
  - https://piazza.com/iit/spring2023/cs558
  - We will use piazza for paper summary submission and other discussion

CS 558: Advanced Computer Security

- Computer security literature: real-world issues and techniques
  - The classics
  - The challenges
  - The state-of-the-art
- Contents:
  - network security
  - IoT security
  - software & hardware security
  - Hot topics: blockchain security, AI security

CS 558: Advanced Computer Security

- Textbook
  - No textbook needed
  - Focus on research papers from top venues in computer security
- Prerequisite
  - Basic knowledge about system and network
  - Programming skills
  - No prior security knowledge required

CS 558: Advanced Computer Security

- Goal
  - Explore a range of problems modern network and computer security
  - Understand basic concepts, threats, and mechanisms in cyber-security
  - Understand how to engage in networking and security research
  - Investigate novel ideas in cybersecurity through a semester-long research project

CS 558: Advanced Computer Security

- Course format and gradings
  - Paper presentation: 20%
  - Paper summary: 10%
  - Discussion participation: 10%
  - Project: 60%
    - Proposal presentation: 5%
    - Mid-term report: 15%
    - Final presentation: 20%
    - Final report: 20%

CS 558: Advanced Computer Security

- All late submissions (but still within one day after the deadline) will automatically lose half points.
- Submissions one day after the deadline will NOT be accepted (unless you get permission from the instructor).
- There will be bonus points for
  - (1) EXCELLENT research projects
  - (2) good discussion participation (paper presentation and project presentation).

CS 558: Advanced Computer Security

- Students are expected to write a paper summary and further present it
- Paper can be from the reading list or from other top conferences
- Each paper summary:
  - no less than 400 words
  - Content: What's this paper about?
  - Motivation: Why do the authors want to conduct this research?
  - Contribution: How is the paper different from its peers?
  - Technique: How do the authors achieve their goal?
  - Evaluation: How is the work evaluated?

CS 558: Advanced Computer Security

- Paper summary (cont.):
  - post it on piazza
  - with the title “Summary - paper name - student name” and the corresponding piazza folder
    - e.g., “Summary - Adaptive selective verification - Yue Duan” with the folder “paper_summary”

CS 558: Advanced Computer Security

- Paper presentation
  - Each student needs to present one paper in the class
    - 15 mins (12 mins presentation + 3 mins discussion)
      - Hint: google the slides of the paper
    - Lead the discussion
      - What are the pros and cons?
      - Why the authors do research the way it is?
      - Any thought for improvement?
      - potential discussion participation credit

CS 558: Advanced Computer Security

- Research Project
  - Aim high!
    - A good project could become
      - publication
      - master/PhD thesis
  - Focus on novelty and impact

CS 558: Advanced Computer Security

- Research Project
  - Students can form groups (no more than 3 students)
    - hint: try finding your collaborators asap
  - Some topics will be provided soon
  - explore new topics encouraged!
  - Talk to me before finalizing your projects

CS 558: Advanced Computer Security

- Research Project (cont.)
  - Four milestones:
    - Proposal presentation: 5-10 min
    - Mid-term report: report progress
    - Final presentation: 15 min
    - Final report: research paper format
  - Example : conduct research on upgradeable smart contracts in blockchain

CS 558: Advanced Computer Security

- Research Project (cont.)
  - Mid-term report
    - Abstract
    - Introduction
    - Problem Statement
    - Motivation
    - Prior Work
    - Your Approach
    - Preliminary Results

CS 558: Advanced Computer Security

- Research Project (cont.)
  - Final presentation assessment
    - Presentation clearness
    - Slides quality
    - Results and Discussion (progress from mid-term)
    - Demo is strongly encouraged
    - Q&A

CS 558: Advanced Computer Security

- Research Project (cont.)
  - Final report
    - Based on your midterm report
    - at least 5 pages excluding reference and appendix
    - Latex ACM or IEEE template
    - conference paper style

CS 558: Advanced Computer Security

- Tentative course schedule
  - **1.9 - 1.30** Introductions to different topics
  - **2.1 - 2.8** Network security (**2.8** project topic due)
  - **2.13 - 2.20** Proposal presentations
  - **2.27 - 3.6** IoT security
  - **3.8 - 3.27** Software & Hardware security (**3.27** Mid-term report due)
  - **3.29 - 4.3** Hot topics: Blockchain & AI
  - **4.5 - 4.26** Paper & Project presentations
  - **5.4** Final report due

CS 558: Advanced Computer Security

Acknowledgement

Some materials from Prof. Kevin Jin, Prof. Matthew Caesar, Prof. Carl Gunter, Dr. Susan Hinrichs , Prof. Guofei Gu, and Dr. Mark Stamp

Computer Security

- Has be

Network Security

- Internet
  - Global scale, general purpose, heterogeneous technologies, public, computer network
  - Vast distributed system comprising
    - 1602 million hosts (potentially malicious)
    - 26,000 ISPs (potentially competing)

Network Security

- Spam email

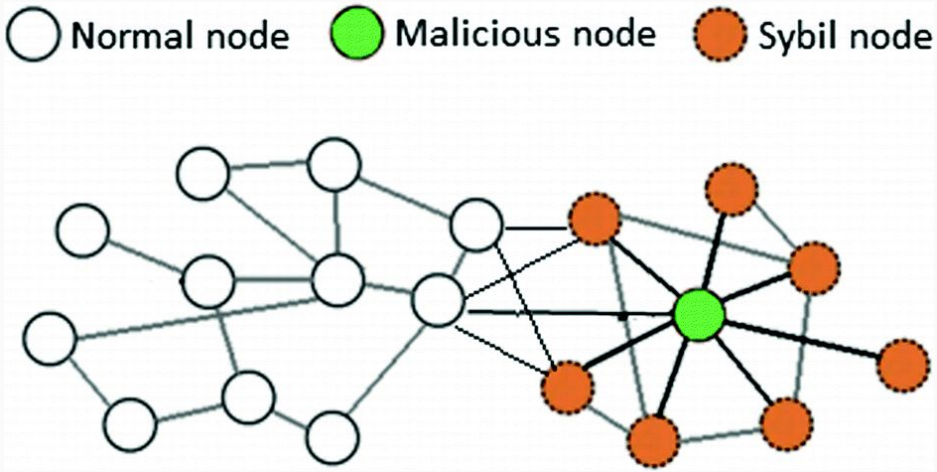
- Denial-of-service attacks

Final Fantasy XIV European Servers Bombarded by DDOS Attack

by Ryan Pearson on August 14, 2021 at 6:05 PM, EDT

Network Security

- Sybil attacks

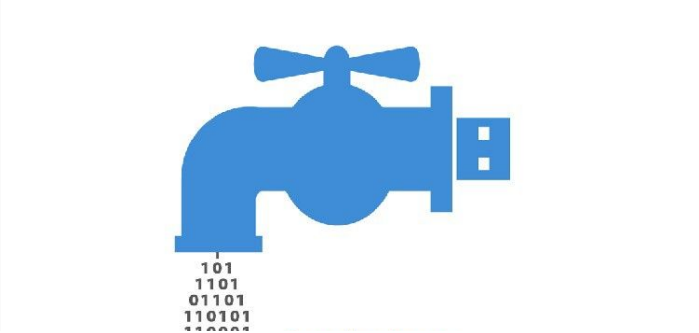


IoT Security

- Cyber-physical system security
  - Internet of things (IOT)
  - smart home
  - smart manufacturing
  - smart agriculture
  - ...

IoT Security

- IoT privacy leakage



- attacks

Cyberattacks on Nuclear Power Plants: How Worried Should We Be?

IoT Security

- attacks

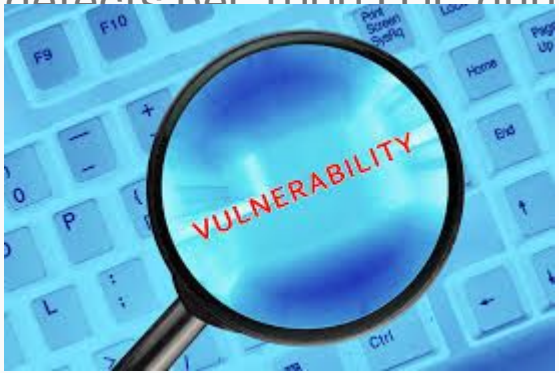
LILY HAY NEWMAN SECURITY 08.09.2018 12:30 PM

A New Pacemaker Hack Puts Malware Directly on the Device

Researchers at the Black Hat security conference will demonstrate a new pacemaker-hacking technique that can add or withhold shocks at will.

Traditional Software Security

- Huge impact
  - Malicious software is designed to cause damages
  - Normal software can and **will** contain vulnerabilities
    - Microsoft Applications: 10 - 20 defects per 1000 LOC during
    - out 15 - 50



Software Security

- Heartblee
  - In pop
  - Resul

Reference: The Heartbleed Bug, explained
https://www.vox.com/2014/6/19/18076318/heartbleed

Software Security

- Malware
  - Marri
  - On M h that impa who used their

Blockchain Security

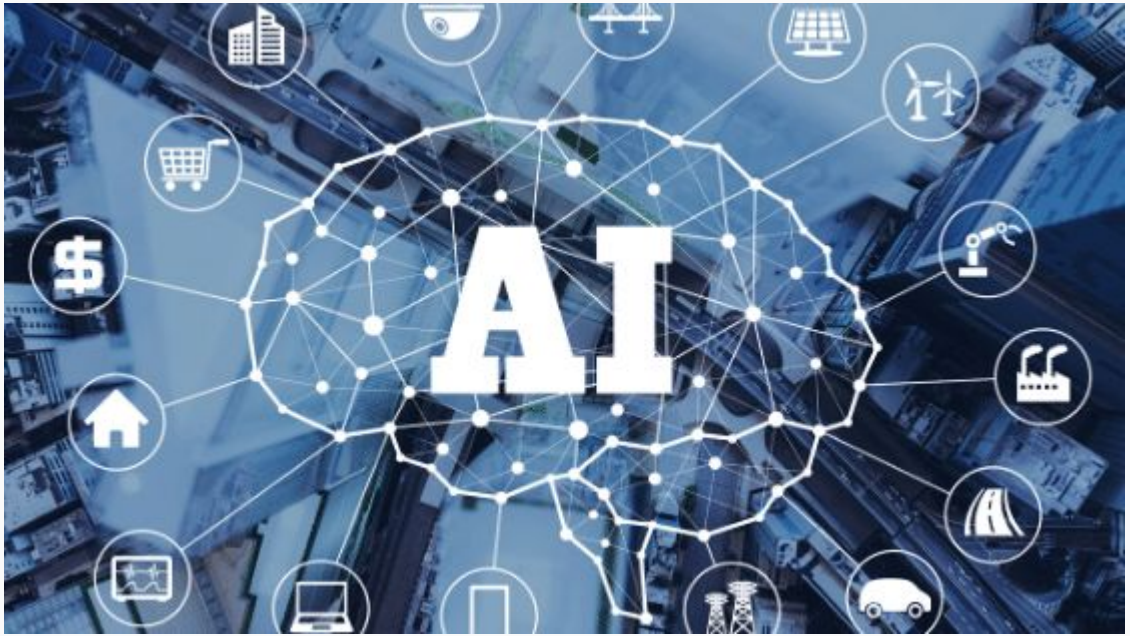
- Blockchain security
  - Smart contracts
    - piece of software running on blockchain
  - Attacks and vulnerabilities
  - Anonymity

Blockchain Security

- The DAO attack
  - On 16 Jun approximately 3.6 million Eth d abusing this loophole.

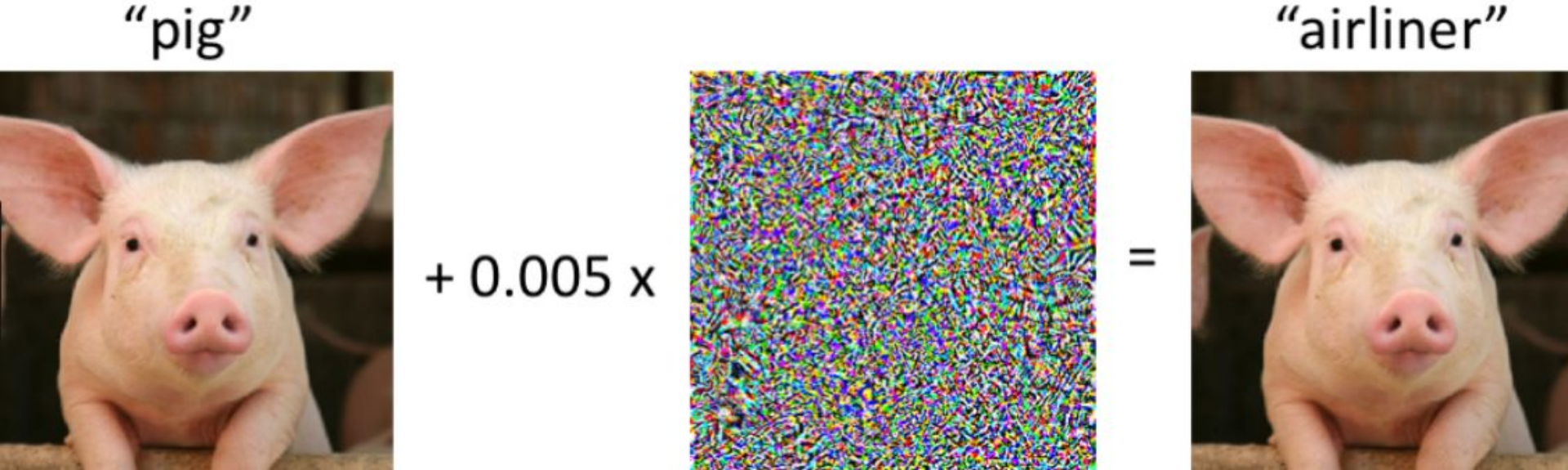
AI Security

- AI is everywhere
  - mobile devices
  - car
  - infrastructure
  - ...



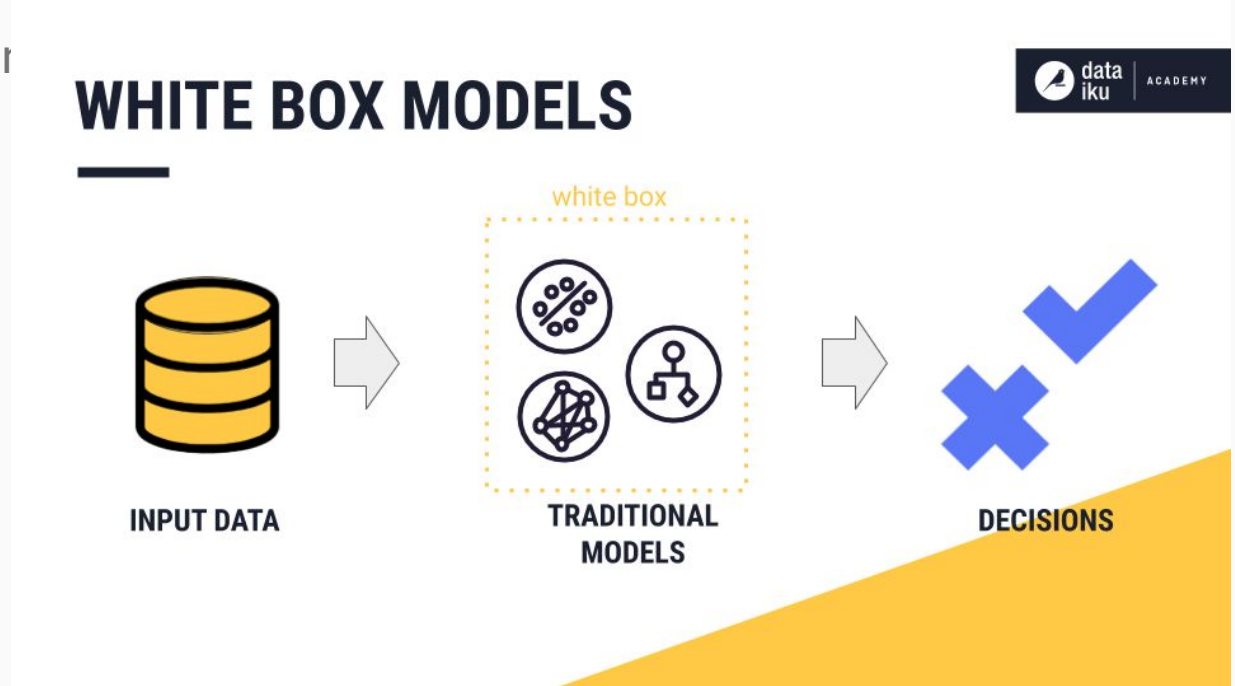
AI Security

- Adversarial ML



AI Security

- Explair



Question?