SC3010
Computer Security

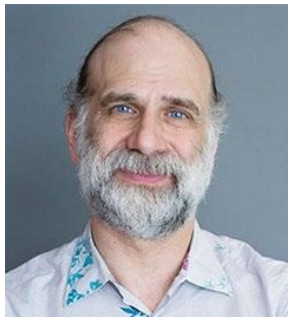
Lecture 1: Introduction

What is Computer Security

Guarantee the correct usage of computer systems and desired properties in the presence of malicious entities

Rose Anderson
Professor, Univ. of Cambridge

"Security engineering is about building systems to remain dependable in the face of malice, error, or mischance."



Bruce Schneier
Adj Lecturer, Harvard Kennedy School

"Security involves making sure things work, not in the presence of random faults, but in the face of an intelligent and malicious adversary trying to ensure that things fail in the worst possible way at the worst possible time … again and again. It is truly programming Satan's computer."

Significance of Computer Security

Critical to physical safety

- Power grid and water systems: blackouts, water contamination or disruption of supply
- Transportation networks and connected vehicles: traffic jam, car collisions or crashes
- Aviation: interfere with navigation and communication, leading to accident
- Factory automation: sabotage industrial processes, leading to equipment failure or explosions
- Medical devices: pose life-threatening risks to patients (e.g., pacemakers)
- Start home systems: compromise devices like thermostats or locks can lead to unsafe temperature levels or unauthorized access to homes
- Electric Vehicle charging stations: overload circuits and cause fire hazards

Case Study: Jeep Hack

Shock at the wheel: your Jeep can be hacked while driving down the road

Taking over a Jeep Cherokee driving at speed 70 mph at a remote highway is quite real.

This hack is even more stunning as the duo found a way to took over a car remotely. Their volunteer victim was driving 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

"As the two hackers remotely toyed with the air-conditioning, radio, and windshield wipers, I mentally congratulated myself on my courage under pressure. That's when they cut the transmission."

Case Study: Throwback Attack

Throwback Attack: An insider releases 265,000 gallons of sewage on the Maroochy Shire

The groundwork for attacks like these was laid back in 2001, when an Australian man became the first known hacker to produce a successful cyberattack against critical infrastructure. Then-49-year-old Vitek Boden launched a sustained cyber assault against the Maroochy Shire, Queensland, Australia, sewage control, a computerized waste management system. He ultimately released 265,000 gallons of untreated sewage into local parks and rivers, causing serious damage to the local environment.

"Marine life died, the creek water turned black and the stench was unbearable for residents," said Janelle Bryant of the Australian Environmental Protection Agency in The Register.

This hack was the first widely recognized example of a threat actor — in this case, an insider — maliciously attacking an industrial control system (ICS). It was also an insider attack, which can be more damaging because the attacker often has specialized knowledge and the ability to manipulate control systems.