CS 491/591
Intro to Computer Security

Dr. Charles V. Wright
cvwright@cs.pdx.edu

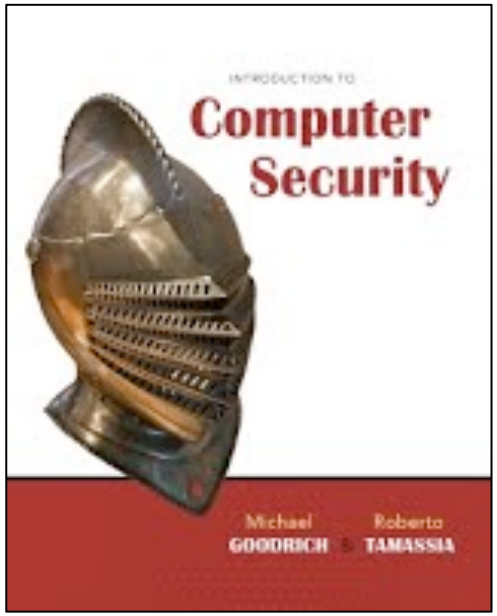
Introduction

- Course title
  - CS 491/591 Introduction to Computer Security
- Time & Location
  - Tues & Thurs 10am-Noon, FAB 40-06
- Instructor
  - Dr. Charles V. Wright <cvwright@cs.pdx.edu>
- Web page
  - http://www.cs.pdx.edu/~cvwright/courses/introsec/

Textbooks

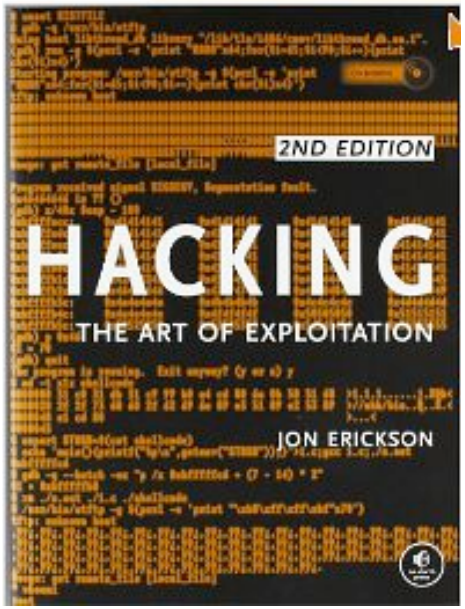
Defense

- **Introduction to Computer Security**
- By Goodrich and Tamassia



Offense

- **Hacking: The Art of Exploitation** (2nd edition)
- By Jon Erickson



Prerequisites

- Essential for success in the course
  - Programming in C (or C++)
  - Basics of computer architecture (CS 201)
  - Operating systems (CS 333)
- Good to know
  - Unix / Linux scripting
  - Some x86 assembly

Grading

	491	**591**
• Homework	40%	40%
• Class Participation	10%	10%
• Term Paper	n/a	10%
• Midterm 1	25%	20%
• Final Exam	25%	20%

Academic Honesty

- All submissions must represent represent the work of the submitting team. It is permissible to discuss the assignment with students on other teams, but you must develop the answers yourselves.

- Do not, under any circumstances, copy another persons work and submit it as your own. Writing material (whether it be code, English text, or other) for use by another or using another's work in any form (even with their permission) will be considered cheating.

- Cheating on an assignment or exam will result in an **automatic zero grade** for that piece of work, and the initiation of disciplinary action at the University level.

A Note on Ethics and Security

- Some of the technical material studied in this course might be useful for doing things that violate university regulations, laws, or common standards of ethical behavior.

- Any such behavior that comes to the instructors attention will be reported to appropriate authorities.

- In particular, note that use of university computing resources is governed by the Office of Information Technology‘s Acceptable Use Policy, which may be found at http://oit.pdx.edu/aup/

Computer Security

What is it?

Motivating Quote

- ***Bad guys have the time, skills, and motivation*** *to study edge devices for weaknesses,* ***and they are finding as many weaknesses as they need*** *to inject malicious code into our precious devices where they can then copy our data, modify our installed software, spy on us, and steal our identities* ***—75 years of science fiction has not begun to prepare us for how vulnerable we and our livelihoods are****, now that everyone is online. Since the adversaries of freedom and privacy now include nation-states, the extreme vulnerability of edge devices and their software is a fresh new universal human-rights problem for the whole world.*

  -- Paul Vixie

More Pithy Quotes

- "The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."
  – *Gene Spafford*

- "Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."
  – *Kevin Mitnick*

More Pithy Quotes

- "Using SSL on the Internet is like a homeless guy who sleeps on a park bench using an armored car to send a note to his friend who lives under a bridge."
  – *Bill Cheswick*

- "Being able to break security doesn't make you a hacker any more than being able to hotwire cars makes you an automotive engineer."
  – *Eric Raymond*

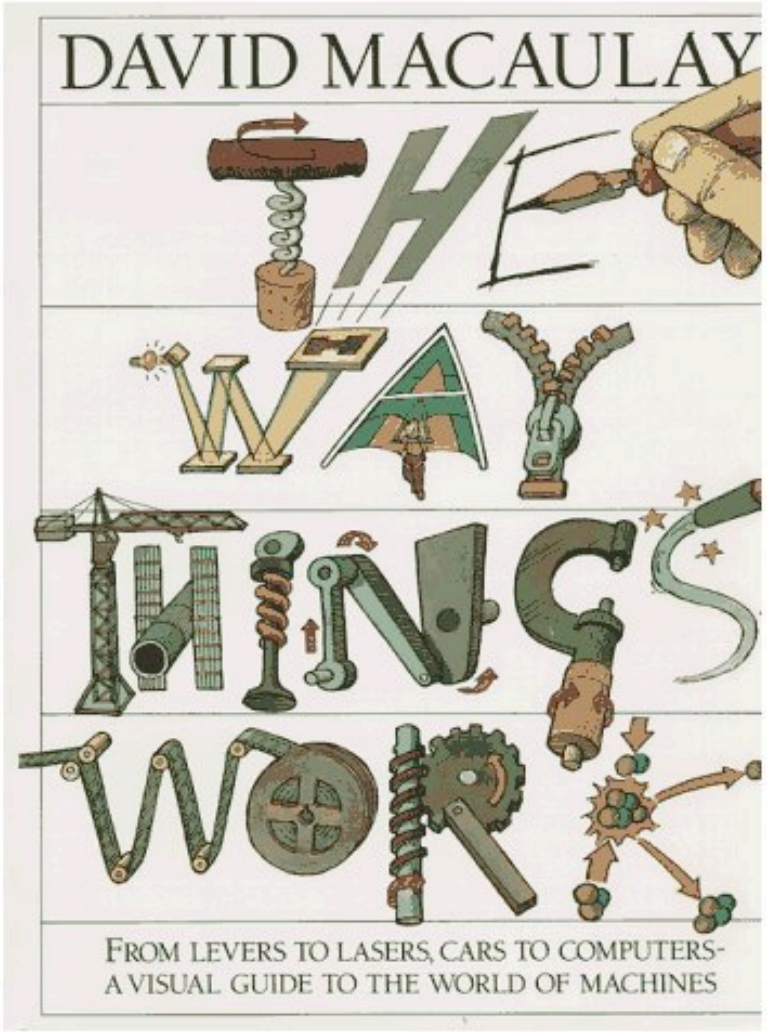
Computer Security: The Study of How S**t Breaks (and how to fix it)

- Computer systems can be made to do things that nobody expected
  - Including the people who designed, built, and operate them
- Attackers exploit this unpredictability to make computers do things that their owners don't want
  - Defenders design systems to make this more difficult
- But HOW??
  - That's the focus of this course

Goals for the Course

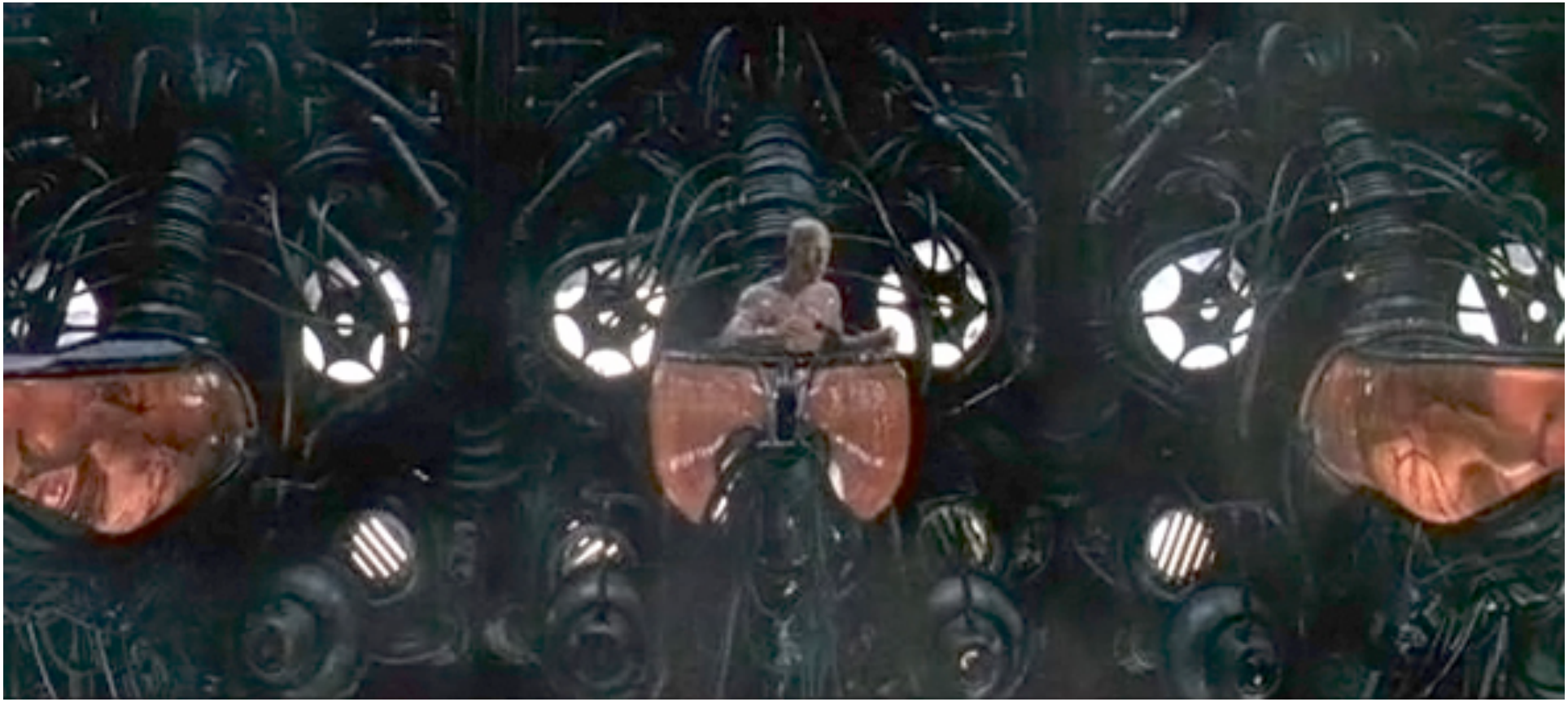
- De-mystify computer security
- Understand current protection mechanisms
  - Strengths
  - Weaknesses
- Learn to think like an attacker
  - Don't fall victim to the same old attacks
- **Build better systems!**

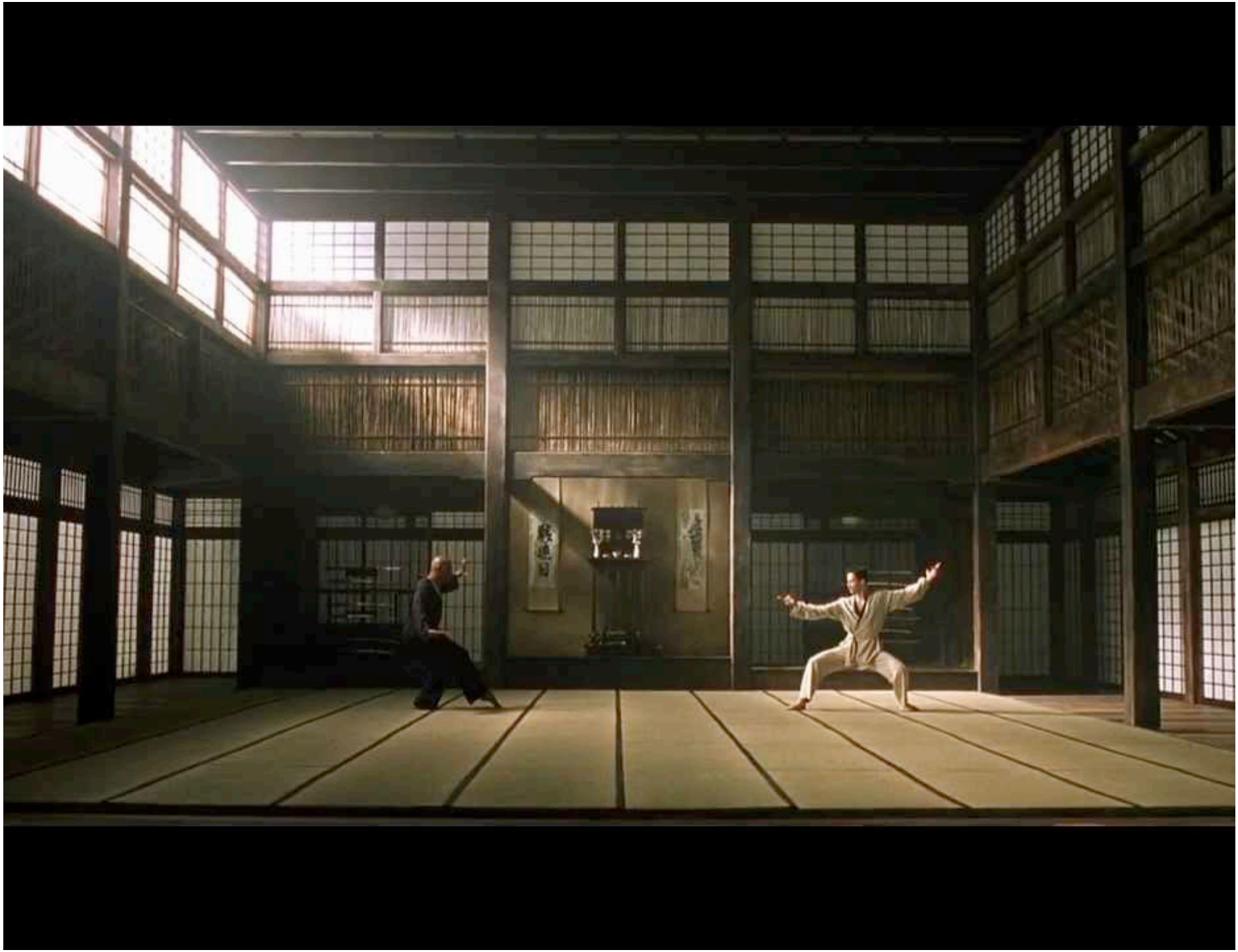
Computer Science and Engineering: How Stuff Works

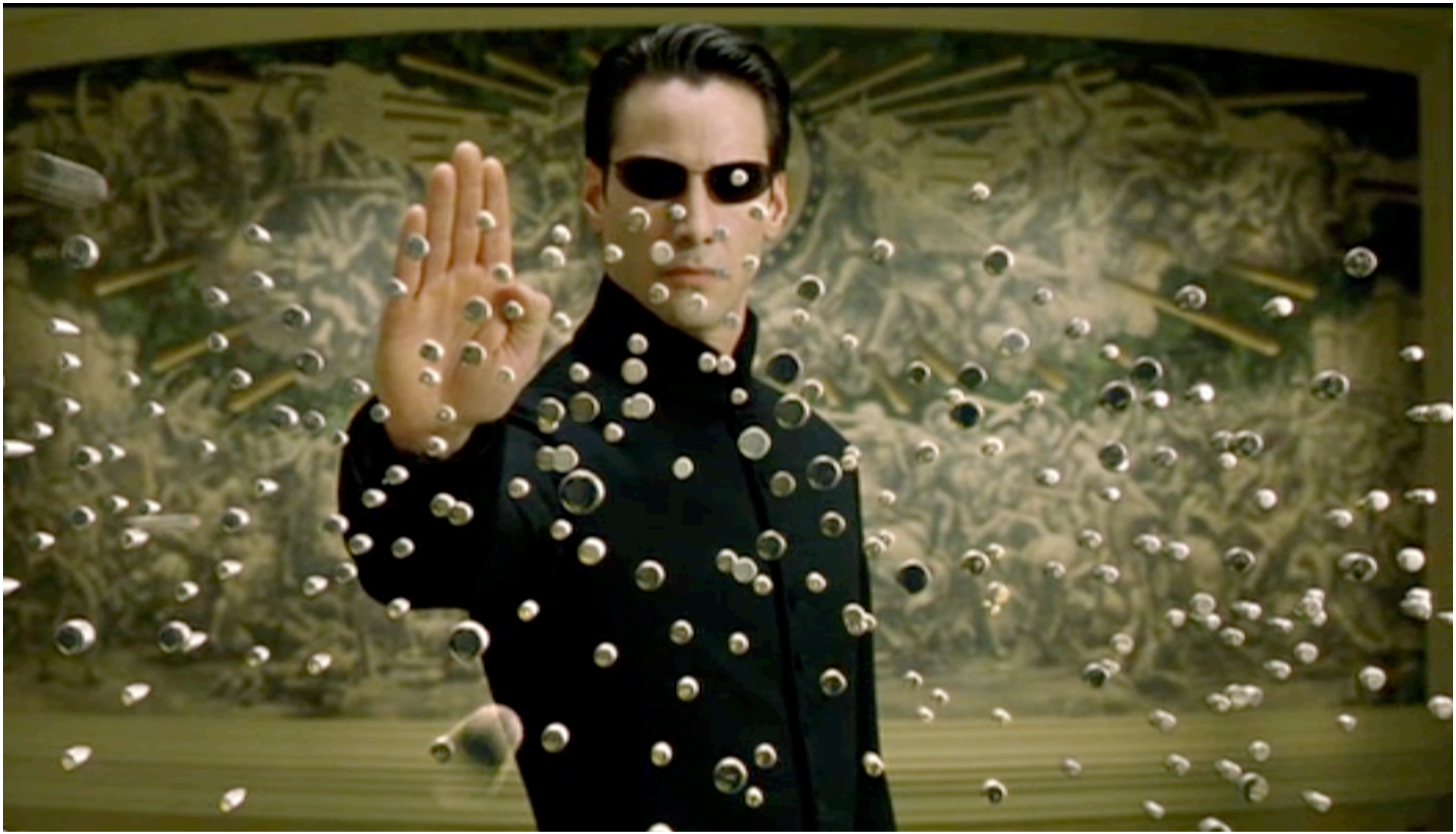


- To understand how a system can be made to fail, we first need a **deep understanding** of **how and WHY it works**
- "The devil is in the details"


TONY
PARK M PARK
RESTAURANT







Why is security so hard?

- Because building good software is difficult
- Because market forces make it even harder
- Because adversaries are clever and motivated
- Because breaking things is easier than building

What is security?

- Typically talk about maintaining three key properties
  - Confidentiality
  - Integrity
  - Availability

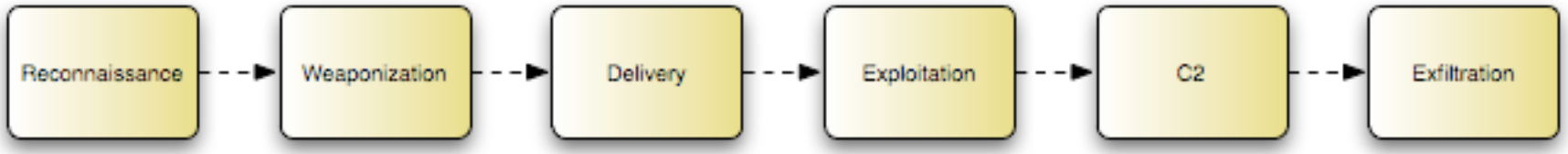
- Despite the best efforts of some adversary

AAA

- Authentication – Who are you?
- Authorization – Who is allowed to do what?
- Audit – Who actually did what?

Lifecycle of an Attack

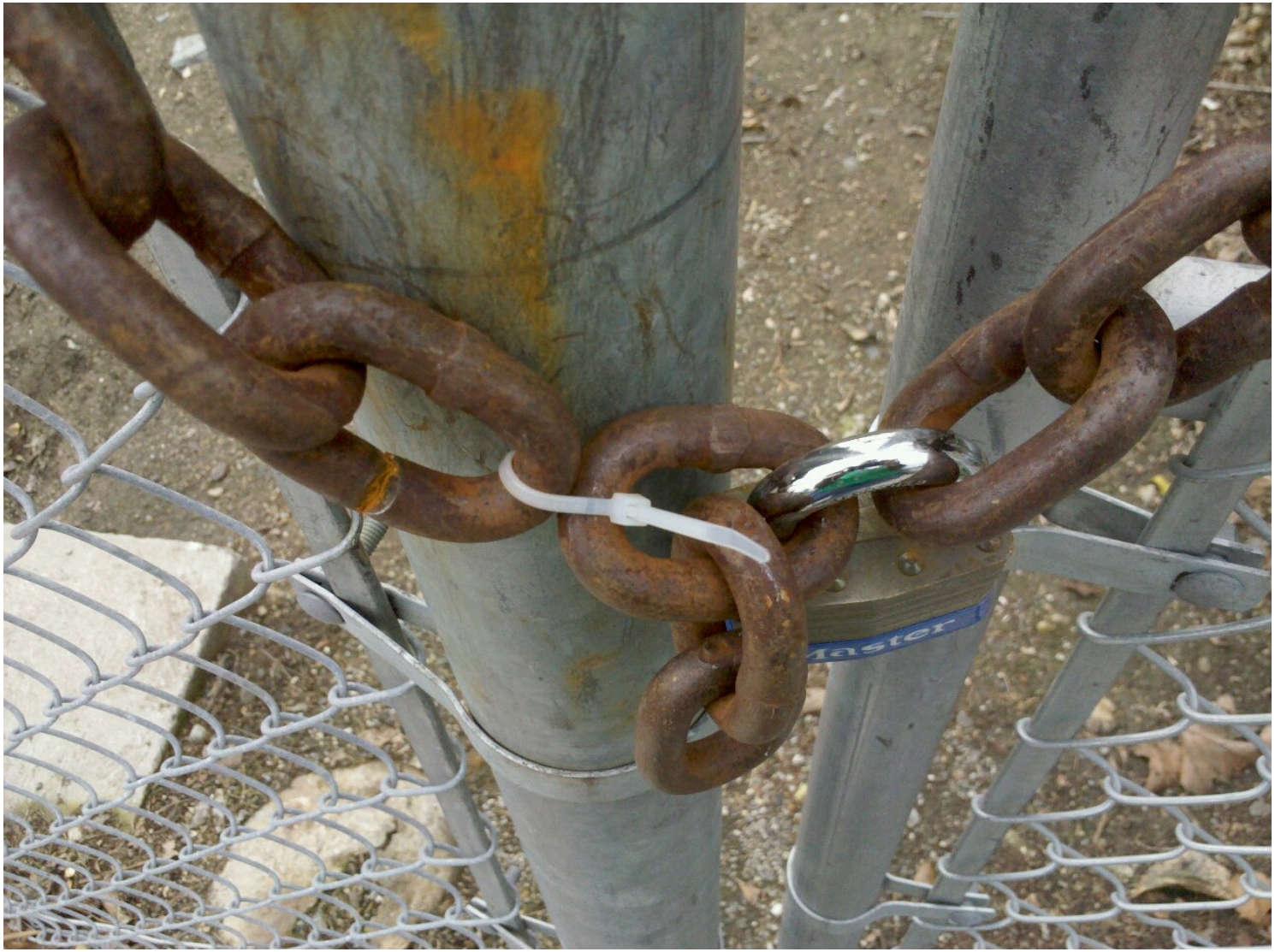
- Attackers carry out a series of steps to achieve their goals
  - Example:
  - http://computer-forensics.sans.org/blog/2009/10/14/security-intelligence-attacking-the-kill-chain



- Defenses aim to halt this process at some point along the chain

Don’t Build Security Like This

Can you spot the flaw here?




Security Fail
failblog.org

Security Camera FAIL

More FAIL

Preliminary Survey

- Goals:
  - Help me target lectures to what you need
  - Get to know each other a little bit

Homework 1

- Due: Tuesday, October 6th, 10:00pm

- Objectives:
  - Create an SSH public/private key pair
  - Log in to the CS Linux machines
  - Write some simple C programs