CSci 4271W
Development of Secure Software Systems
Day 1: What's Your Threat Model?

Stephen McCamant (he/him)
University of Minnesota, Computer Science & Engineering

Outline

Key course logistics

Discussion group greetings

Intro to security assessment

Instructor information

- Stephen McCamant
- Office: 4-225E Keller (most days)
- Office hours: Monday 9/27 4-5pm, future weeks TBA
- Email: `smccaman@umn.edu`

Teaching assistants

- (Sheikh) Mostofa Amir Foisol
- Office hours: TBA

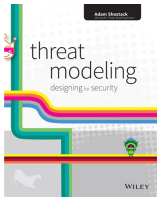
Course content

- Describe a software system
- Identify potential threats
- Detect (and maybe exploit) vulnerabilities
- Mitigate vulnerabilities
- Prevent vulnerabilities
- At design, coding, application, compiler, OS, network and user interface layers

Course outline

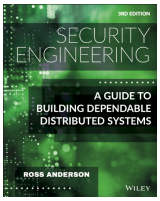
- Threat Modeling
- Secure Coding
- OS Security
- Network Security
- Cryptography
- Web/Mobile Security and Privacy
- Usability and Human Factors

Most important textbook



Particularly relevant for the first part of the course

Next most useful book



Third edition is now free online

Coursework and grading

Category	#	Weight
Labs	13	5%
Homework	6	10%
Projects	3	45%
Midterms	2	20%
Final Exam	1	20%

Coursework and grading

Category	#	Weight	Every week
Labs	13	5%	Tool overviews
Homework	6	10%	Short writeup,
Projects	3	45%	score $\in \{0, \frac{1}{2}, 1\}$
Midterms	2	20%	Groups of up to 3
Final Exam	1	20%	Total score out of 10

Coursework and grading

Category	#	Weight	Every 2–3 weeks
Labs	13	5%	Written work, short coding
Homework	6	10%	Groups of up to 3
Projects	3	45%	Drop one homework
Midterms	2	20%	Late submissions
Final Exam	1	20%	−10%/day up to 3 days

Coursework and grading

Category	#	Weight
Labs	13	5%
Homework	6	10%
Projects	3	45%
Midterms	2	20%
Final Exam	1	20%

Dates: 3/18, 4/15, 5/5

Evolving 10–12 page report:

- Design
- Threat Model
- Vulnerabilities

Groups of up to 3

One extension (to Friday)

Coursework and grading

Category	#	Weight	In-class exams:
Labs	13	5%	Thursday, February 20th
Homework	6	10%	Thursday, March 27th
Projects	3	45%	Final:
Midterms	2	20%	Saturday, May 10th, 4–6pm
Final Exam	1	20%	Open-book, open-notes
			Short answer, exercise-like

Security ethics

- Don't use techniques discussed in class to attack the security of other people's computers!
- If we find you do, you will fail, along with other applicable penalties

Outline

Key course logistics

Discussion group greetings

Intro to security assessment

Say hello to your neighbors

- From time to time I'll ask you to do discussions or exercises in groups with people sitting near you
- For today, just introduce yourself to the folks sitting nearby

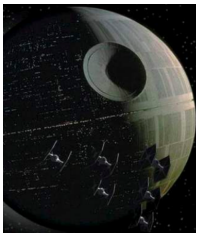
Outline

Key course logistics

Discussion group greetings

Intro to security assessment

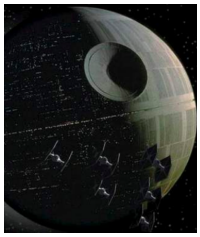
Security assessment



Star Wars TM and (C) Lucasfilm, Ltd.

- "Is it secure?"

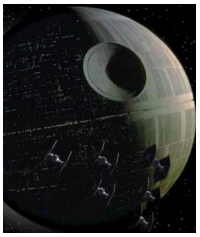
Security assessment



Star Wars TM and (C) Lucasfilm, Ltd.

- "Is it secure?"
- Secure against what?

Security assessment



Star Wars TM and (C) Lucasfilm, Ltd.

- "Is it secure?"
- Secure against what?
- What's your threat model?

Secure against what?

What properties should be preserved, against an attacker with what resources?

Properties	Assets
Confidentiality	Data
Integrity	Memory
Availability	Execution
Accountability	Network
Dependability	Devices

Secure against what? (cont'd)

What properties should be preserved, against an attacker with what resources?

Attacker	Resources
Customer	Computational
Employee	Physical
Competitor	Monetary
Government	Credentials
Nature	

Secure against what? (cont'd)

What properties should be preserved, against an attacker with what resources?

Attacker	Resources	Goal/Motive
Customer	Computational	LOLs
Employee	Physical	. . . Profit!
Competitor	Monetary	Competition
Government	Credentials	Espionage
Nature		

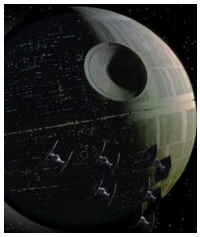
Secure against what? (cont'd)

What properties should be preserved, against an attacker with what resources?

Attacker	Resources	Goal/Motive
Customer	Computational	LOLs
Employee	Physical	. . . Profit!
Competitor	Monetary	Competition
Government	Credentials	Espionage
Nature		

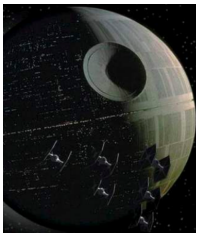
What attacks are out of scope?

Threat modeling



Star Wars TM and (C) Lucasfilm, Ltd.

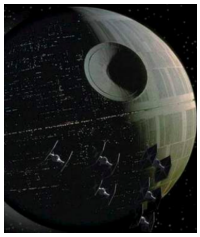
Threat modeling



Star Wars TM and (C) Lucasfilm, Ltd.

- What does/should it do?

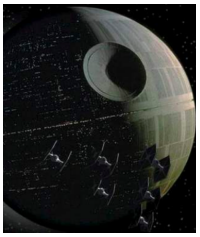
Threat modeling



Star Wars TM and (C) Lucasfilm, Ltd.

- What does/should it do?
- What could go wrong?

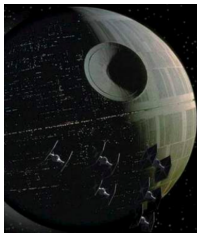
Threat modeling



Star Wars TM and (C) Lucasfilm, Ltd.

- What does/should it do?
- What could go wrong?
- What are you doing about it?

Threat modeling



Star Wars TM and (C) Lucasfilm, Ltd.

- What does/should it do?
- What could go wrong?
- What are you doing about it?
- How did you do?

Risks and costs

- Answering the questions "What are you going to do about it?" and "How did you do?" often involves balancing risk against cost.
- Risk due to a set of attacks is the expected cost per time
- One measure of risk is Annualized Loss Expectancy (ALE):

$$\sum_{\text{attacks } A} (p_A \cdot L_A)$$

p_A is the annualized attack incidence
L_A is the cost (loss) per attack

Risk reduction

- A mitigation or defense D may reduce the ALE of an attack by reducing p_A or L_a.This is the Gross Risk Reduction:

$$GRR_D = \sum_{\text{attacks } A} ((p_A \cdot L_A) - (p'_A \cdot L'_A))$$

- Since the defense also has a cost C_D, the Net Risk Reduction is $NRR_D = GRR_D - C_D$