DATA 599 COMPUTER SECURITY SPRING 2023 MIDTERM I

Instructor Calvin Deutschbein

Roster Name	
Sign here to affirm the Honor Code	

This exam will be timed to take 120 Minutes.

It will be scored out of 200 Points.

It will inform between 20-60% of the final grade, favoring the student.

SECTION I: CRYPTOLOGY 60 Points

Part 1: Terminology: 4 Questions @ 5 Points each = 20 Points

What is the first step of security modeling?

A. Ascertaining Limitations
B. Making a Diagram
C. Mitigating Threats
D. Validation our Assumptions

Signal is a secure messaging app. What does Signal secure?

A. The contents of messages
B. The people using the app
C. The times and dates of when messages are sent
D. More than one of the above

Signal is a secure messaging app. For whom does Signal secure?

A. The contents of messages
B. The people using the app
C. The times and dates of when messages are sent
D. More than one of the above

Signal is a secure messaging app. What are some limitations - things Signal does not keep secure?

A. The contents of messages
B. The people using the app
C. The times and dates of when messages are sent
D. More than one of the above

Part 2: Short Response: 2 Questions @ 10 Points each = 20 Points

Describe in your own words the distinction between safety and liveness, two broad categories of security properties.

Describe in your own words the distinction between sequences and sets. You may wish to use the motivating examples of traces and trace properties in your answer.

Part 3: Written Response: *20 Points*

Security oriented technologies secure both “from” and “for” - but are far from morally neutral. Describe a case in which defining a security policy created “winners” and “losers” and describe whether you consider the aggregate effects to be positive or negative.

SECTION II: LOGIC **90 Points**

Part 4: Multiple Choice: *4 Questions @ 5 Points each =* *20 Points*

Which of the following does not require *a* to hold at some point in the future.

A. **G** *a*
B. **F** *a*
C. **X** *a*
D. True **R** *a*

Which of the following requires *a* to hold at multiple time points in the future.

A. **G** *a*
B. **F** *a*
C. **X** *a*
D. True **R** *a*

Which of the following requires there to be a future time point at which both *a* and *b* hold?

A. b **U** *a*
B. b **R** *a*
C. b **W** *a*
D. b **M** *a*

Which of the following does not require *a* to hold at any point in the future?

A. b **U** *a*
B. b **R** *a*
C. b **W** *a*
D. b **M** *a*

Part 5: Short Response: 2 Questions @ 20 Points each = 40 Points

Select your preferred of the following three specification techniques and briefly argue for its use: (1) linear temporal logic, (2) Kripke Structures, or (3) Büchi Automata.

Propose and briefly argue against your above choice, perhaps address some limitations compared to the other techniques.

Part 6: Threat Modeling Exercise *30 Points*

Recall that threat modeling for some system, including computer systems, proceeds in four steps:

- Diagram. What are we building?
- Identify threats. What could go wrong?
- Mitigate. What are we doing to defend against threats?
- Validate. Have we acted on each of the previous steps?

Consider the development of a computer system to provide legal assistance to individuals who encountered law enforcement during protests that were expressly critical of the institution of law enforcement itself by connecting said individuals with pro bono attorneys. Provide a threat model for this system, minimally including a labeled diagram.

SECTION III: THEORY 50 Points

Part 7: Short Response: 2 Questions @ 25 Points each = 50 Points

Describe what the states of a traffic light are, and what they correspond to in Kripke structure.
Recall a Kripke structure is a a 4-tuple $\{S, I, R, L\}$

Briefly describe a trace and what, under the Büchi Automata framework for traces, is the difference between a letter of a trace, and a full trace.
Recall an automata is a 5-tuple $\{Q, \Sigma, \delta, q_0, \mathbf{F}\}$.