WILLIAM & MARY

CHARTERED 1693

CSCI 445: Mobile Application Security

Lecture 24

Prof. Adwait Nadkarni

Final Exam!

- **Date: May 14**
- **Time: 2 -- 5pm**
- **Location:** In class

Policies

- **Crib sheet:** *1 page, both sides,* ***handwritten***
- **Calculator:** *Strongly Recommended*
  - *Any scientific/graphing calculator*
    - *Something that does not have a touchscreen*
- **Content:** Everything up to last class is fair game.
  - **Slides/material taught in class**
  - Readings
  - Homeworks
    - Take a look at the word list!

Final Exam

- Exam will test three kinds of things:
  - *knowledge* (do you know terminology/approaches)
  - *synthesis* (can you extrapolate or compare concepts)
  - *application* (can you apply what you learned)

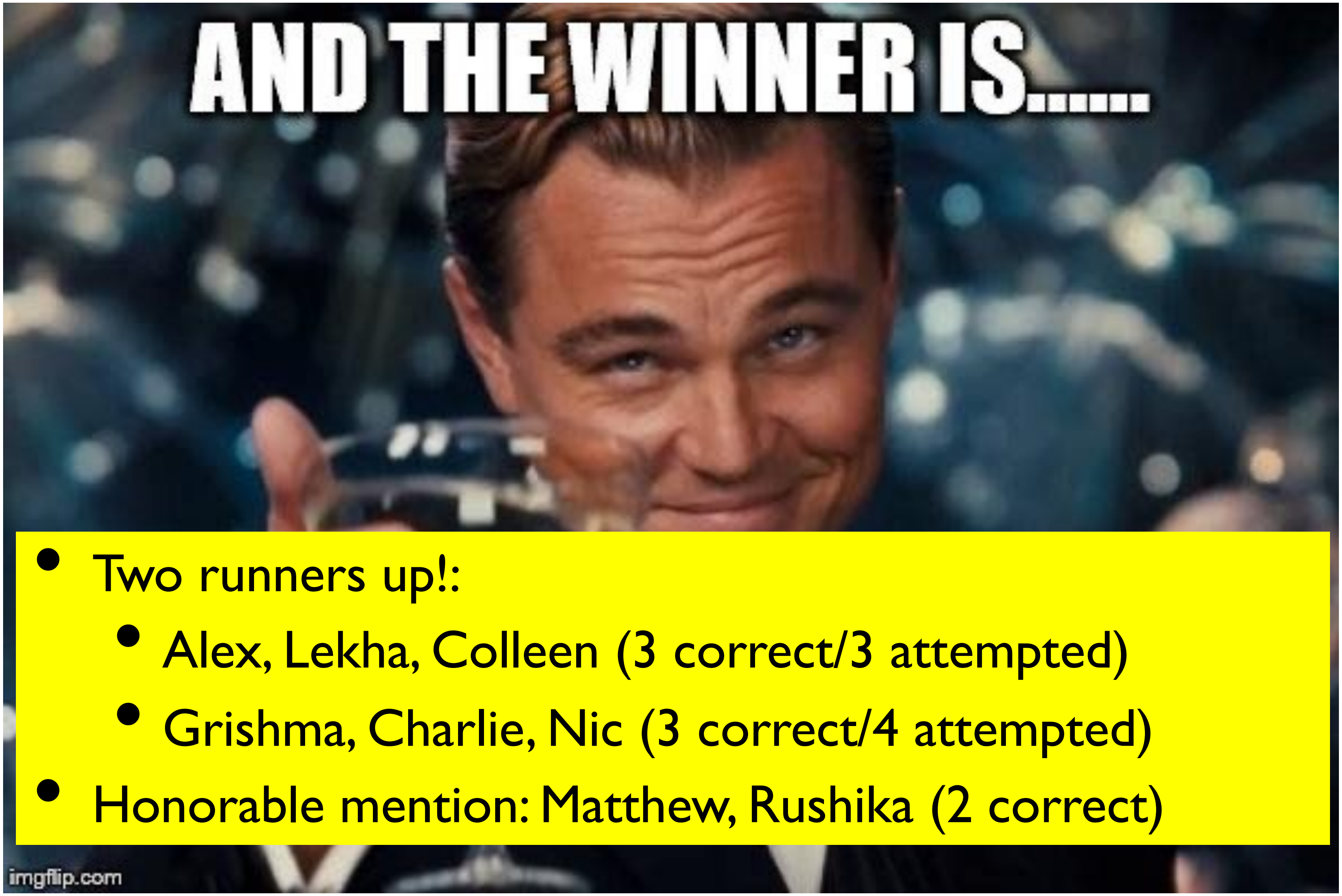
Sample Questions

- Short answer question (3 pts, 1 sentence/word): *Why are active attacks easier to detect than passive attacks?*
- Long answer question (7 pts, 2-3 sentences): *Explain what the safety problem is and how mandatory access control systems deal with it?*
- Problem question (10 pts, show your work): *Acme archival storage systems is a company that promises to securely store customer data. They provide a online system that the customer submits documents for storage which Acme encrypts using AES and a key specific to each request. Acme only accepts requests from 8am to 5pm, Monday through Friday, and they are open on all holidays not falling on a weekend. For the purposes of this exercise, you can assume that Acme has been in operation for exactly 700 days. A customer document di is encrypted as E(di , kr), where the key kr is computed the kr = h(ti) and ti is the timestamp (with millisecond granularity) of the request submission. What is the entropy of the key?*

Announcements

- Project Report deadline extended to May 12, EoD.
  - You can *extend* MalloDroid, Androguard
    - MalloDroid is really basic, you can do more for the same TrustManager and HostnameVerifier checks
    - You can check for more things (permissions, API usage)
- **Finding bugs** (Deadline: May 12 EoD)
  - 2 bugs in readings, *OR*, 4 valid vulnerabilities in the 100 apps
    - Need to be the *first to find*

Security Analysis Hackathon



- Two runners up!:
  - Alex, Lekha, Colleen (3 correct/3 attempted)
  - Grishma, Charlie, Nic (3 correct/4 attempted)
- Honorable mention: Matthew, Rushika (2 correct)

Example questions

- What is the principle of least privilege? (3 pts)
- What is application *collusion*? Provide a short example. (3 pts)
- Define static and dynamic analysis, and compare them, i.e., describe their tradeoffs for analyzing apps (7 pts)

Example questions

- A professor of computer science and engineering at an unnamed university wants to detect students cheating on the final exam by looking at the answers given. He develops an algorithm the data mines the exam responses to detect cheaters. This algorithm correctly accuses cheaters 95% of the time and falsely accuses honest students 4% of the time. I our of every 400 students who takes an exam cheats. Denote the **probability of a cheater to be Pr(C)** and the **probability of accusation as Pr(A)**. Fill out the following values and SHOW YOUR WORK: (10 pts)
- P(!C) = ?
- P(A) = ?
- P(A|C) = ?
- P(A|!C) = ?
- P(C|A) = ?
- ....

Final Review

- Ask away!
- Feel free to make me repeat *anything*