WILLIAM & MARY

CHARTERED 1693

CSCI 445:
Mobile Application Security

Lecture 23

Prof. Adwait Nadkarni

Understanding vulnerabilities through mutants – Tutorial and Hackathon!

Key Task: Identify *flaws* in security tools by observing what mutants they don't detect

Goal

To help you *understand* vulnerabilities through observation and practice

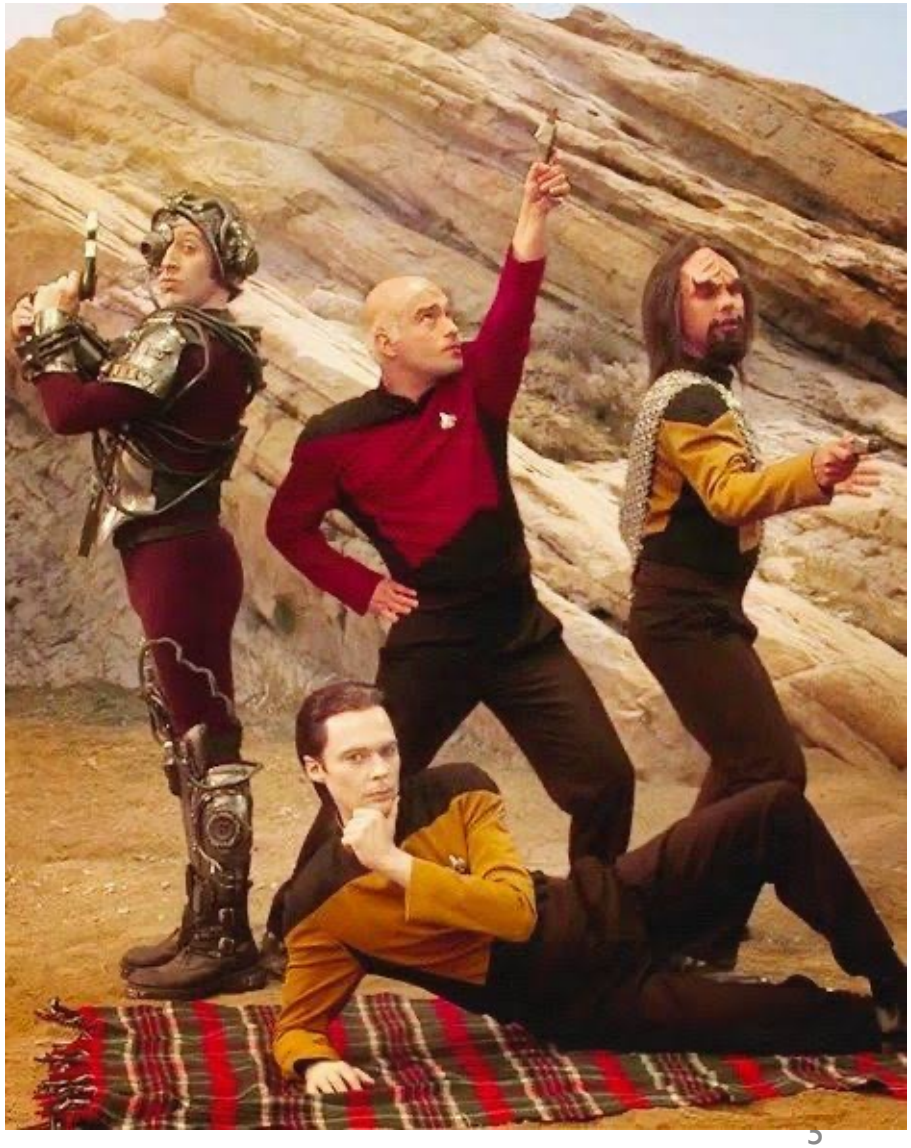
- Go through many diverse vulnerabilities → *learn to recognize them in practice*
- Observe the failure of a tool to detect a vulnerability → *learn about the latent aspects of vulnerabilities*
- Identify *flaws* in tools (i.e., failures to detect a particular type/variant of a vulnerability) → *learn about the practical limitations of analyses*

The task

- Examine *mutants, i.e., vulnerability instances* (crypto API misuse), using 3 artifacts:
  - *Mutation logs*, i.e., logs from MASC on where mutants were placed
  - *Tool logs*, i.e., logs from a security tool (e.g., CryptoGuard) describing where it has detected *what kind* of vulnerability
  - *Vulnerable app source code*, i.e., the source code of apps containing the mutants
- *First*, identify a mismatch between the mutation log and tool log, which will represent a vulnerability MASC inserted but the tool did not catch, i.e., *a potential flaw*
- *For each potential flaw, check if the tool's documentation claims to detect the vulnerability* represented by the mutant (look at the vulnerable app's source code). *Does it claim to detect it (but obviously does not)?* Congratulations! You found a flaw in a tool!

Team Assignment!

- Teams of 3
- Relocate!



Prizes! (for the entire group)

- **Winner**
  - *The first* to report 5 valid flaws (report more, just in case some are not valid)
  - *+5 bonus points on the class grade*
- ***One Runner* up (>1)**
  - Reports 3 or more valid flaws, but not the first to report 5
  - *+3 bonus points on the class grade*
- **Participation bonus (>1)**
  - Reports *at least one valid flaw*
  - +1 bonus point on the class grade

Submit a PDF report to **BlackBoard** ("Vulnerability Detection Hackathon"), latest by EOD today, with the names of Zoom breakout team members