CS 563 - Advanced Computer Security: Upcoming Project Milestones

Professor Adam Bates
Fall 2018
Throughout the remainder of the semester you will be incrementally building conference-style papers and presentations:

- **Oct. 26**: Abstract, Background, Related Work
- **Nov. 2**: Experimental Proposal
- **Nov 16**: Status Slides
- **Dec 7/12**: Project Presentation (In-Class)
- **Dec 18**: Term Paper
Based on your project choice that has been approved by the teaching staff, prepare the following:

- Abstract
- Background
- Related Work

Format: LaTeX Two Column ACM

- Viable template: https://github.com/acmccs/format

Submission: Submit before class on Compass.
HOW DO I ABSTRACT?

• One (maybe two) paragraphs

• The “Elevator Pitch” of your paper, should cover:

  1. Area
  2. Problem
  3. Solution
  4. Methodology
  5. Results
  6. Takeaway
WHY START WITH BG + RW?

1. Be smart and conduct a literature survey so that you can understand the space before committing to a research direction.

2. Easiest part of the paper to write. Once they’re ‘locked in’ there is no need to change them, so it’s best to get them out of the way.
HOW DO I BACKGROUND?

• What knowledge does a reviewer need to possess before they can evaluate your work?

• Concept-driven, not paper-driven

• Specifications, RFCs, Schematics, Workflows

• Citation Density: Low - Medium

• Examples from our class:
  • A Placement Vulnerability Study -> Public Clouds, Placement Policies, Launch Strategies Co-Residency Detection
  • Draco -> WebView Implementation, WebView API, Javascript and HTML5
How do I relwork?

• Goals:
  • Demonstrate understanding of area
  • Distill prior work into easily understood taxonomy
  • Identify gaps in the literature, differentiate your idea
  • Appease your reviewers by citing their work

• Citation Density: High

• **Requirement for your submission:** 25 peer-reviewed citations
  • Quantity != Quality, but it’s a start
RELWORK EXAMPLE

• DRACO -> “Vulnerability of WebViews has been extensively discussed by previous work [7, 8, 1, 9, 10]. In [7], the authors present several classes of attacks that can be launched against apps that use WebViews. Chin et al. present a static analysis tool that can identify whether an app is vulnerable to WebView attacks [8]. Mutchler et al. present a large-scale analysis on mobile web applications, and present the trend of vulnerabilities in these applications. None of these work implement any defense mechanism targeting WebViews [1]. In [27], the authors present an access control mechanism for WebViews. Their approach uses static analysis to identify the use of security-sensitive APIs in the exposed Java class, and notifies the user if any such use is found. The user is then prompted to allow or completely block the binding of the Java object. The main drawback of this approach is that after the user allows the binding, they do not provide any origin-based access control, so all the origins still have the same access rights. Additionally, their focus is only on the permission-protected resources.”
Milestone #2 (Nov 2)

• Last submission we “locked in” the background and related work sections of our paper. This submission will be a living document as you begin to do the real work.

• Purpose: Tell me specifically what are you doing to DO in your project

• Format: Add a new section called “Experimental Proposal” to your LaTeX document from Milestone #1.

• Submission: **Submit before class** on Compass.
Be sure to include:

• Hypothesis: Based on what you’ve learned so far, “commit” to a prediction that is the basis of your paper.
  • What does a hypothesis in a defensive paper look like?

• Methodology and/or Design: What techniques are you going to use? How are you going to use them? Will you leverage existing tools? Convince me that you will succeed in executing your methodology.

• Evaluation and/or Analysis: How will you determine the extent to which you have succeeded in your goal?