Cybersecurity analysis of password managers

Project owner/sponsor(s) and contact information

- Mr. Donald Privitera

Project overview

- Password managers have proliferated as a vital means of storing and managing many usernames and complex passwords. The concept of centralizing this vital data represents a treasure trove of valuable information that bad actors would likely be motivated to work on complex attacks to compromise. A key component of many password managers is browser integration. It is my hypothesis that this interface represents a logical vector of attack. This project involves analyzing popular commercially available password managers and popular browsers to assess possible weaknesses and if possible, to demonstrate vulnerabilities. Plan for Windows 10 OS as the platform with Windows Security-Device Security-Core Isolation-Memory Integrity should be turned off.

Major expected outcomes

- Identify universe of password managers and narrow to top 5 (based on number of users if possible).
- Identify universe of browsers and narrow to top 3.
- Focus on at least 1 browser with reputation for most security vulnerabilities.
- Research browser add-on technology understanding how it works and how to make an add-on, analyze for possible attack vectors, create an add-on with the intent of attacking a password manager add on.
- Install, run, test, and attack password managers attempting to identify vulnerabilities and to create exploits.
- If possible, demonstrate compromise of passwords from one of more password managers.
- Bitwarden on Windows 10 using Firefox must be included as a part of the final selection. Attacks should be made on both the browser add-on component and the stand-alone application.
- If accepted to C-Day, the project team should plan on attending C-Day.
- If a vulnerability and exploit are demonstrated, the project team should plan on submitting their formal paper for publication.

Deliverables

- Milestone 1 – identify all targets (password manager apps, browsers, and plan of attack)
- Milestone 2 – preliminary results of analyzing and ethical hacking
- Final deliverables – final results of analyzing and ethical hacking including a formal paper in a format suitable for possible publishing.

Type of work (estimation)

- Research, analysis, technical, cybersecurity, software development, applications, project management, web development.

Courses/Skills/knowledge involved

- Software development
- Ethical hacking
- Problem solving
- Excel
- Project management
- Written communication

- Verbal communication
- Presentation

Number of teams and students

1 team, 3 to 5 undergraduate students

Other requirements

- The entire team will need to meet with project sponsor virtually for kickoff, milestones, and final deliverables.
- The sponsor is available to meet with the team other times at the team's request.
- Do not attempt to hack into any websites.
- All analysis must focus on the student's local computer browser and local password manager browser add-ons or local EXE's.
- Password managers that use a PIN shortcut may have a special vulnerability since they may keep password's decrypted. Student's should be sure to analyze this scenario. Bitwarden among a few others offer this feature.
- Students should keep all project information confidential and anonymous by using anonymous identifiers to represent the password managers. For example, students should keep a master reference to what password managers are such as "PW1 = Bitwarden, PW2=Lastpass, etcentera" and then students should refer to the password manager by using the abbreviation in all public facing materials such as but not limited to websites. The master reference should be kept confidential and provided to the instructor and sponsor only. This approach will prevent any security vulnerabilities found in specific password managers from becoming public information and possibly being used by malicious hackers before the manufacturer has a chance to make fixes. Good security practice provides notice to manufacturers first so that they have a reasonable amount of time to apply fixes before any specific information is made public. Some manufacturers may wish to keep such information confidential indefinitely and, in such cases, anonymous information may be the only information allowed to be published.
- With permission from KSU's legal department and the Dean of CCSE, after the project has concluded, students optionally may be allowed to sign up to a "bug bounty" site as may be engaged by a Password Manager company (for example, Synack, BugCrowd, HackerOne, etcetera). Bug bounties are outside of the purvey of the university, college, instructor, and sponsor and it would be up to the students to read and comply with all stipulations related to any such bug bounty. If students meet bug bounty stipulations, students may be entitled to receive a bug bounty award which would be split equally among all students who participated in the project. The instructor and sponsor would not be entitled to receive money from a bug bounty.
- If the paper has merit for publication, the instructor and sponsor would be entitled to publish a paper with their name as an author along with all students who participated in the project. Conversely, if students choose to publish a paper, they must include the names of all students who participated in the project along with the instructor and sponsor. Students must get prior written approval by the instructor and sponsor before publishing anywhere.