TEMPLATE

Article Name, FirstAuthorLastName et al., 20XX

Being worked on by: Name

Link

* In this paper, the authors…
  + Research question
  + Methodology
  + Key findings
* This will help our project because…
  + Motivations to our study
  + Building upon their findings in this way
  + Ideas for solutions to some problems we have

Why people (don’t) use password managers effectively, Pearman et al, 2019.

Being worked on by: no-one

[Link](https://www.usenix.org/system/files/soups2019-pearman.pdf)

* In this paper, the authors…
  + Research question
  + Methodology
  + Key findings
* This will help our project because…
  + Motivations to our study
  + Building upon their findings in this way
  + Ideas for solutions to some problems we have

Security Evaluation of Password Manager Browser Extensions, Bojan, 2017

Being worked on by: no-one

[Link](https://pdfs.semanticscholar.org/a531/bfae3dc920c41dc9cc3b2d55528257823668.pdf)

* In this paper, the authors…
  + Research question
  + Methodology
  + Key findings
* This will help our project because…
  + Motivations to our study
  + Building upon their findings in this way
  + Ideas for solutions to some problems we have

Password Managers: Attacks and Defenses, Silver et al., 2014

Being worked on by: no-one

[Link](https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-silver.pdf)

* In this paper, the authors…
  + Research question
  + Methodology
  + Key findings
* This will help our project because…
  + Motivations to our study
  + Building upon their findings in this way
  + Ideas for solutions to some problems we have

“Secure Password Managers” and “Military-Grade Encryption” on Smartphones: Oh, Really?, Belenko et al., 2012

Being worked on by: André

[Link](https://www.elcomsoft.com/WP/BH-EU-2012-WP.pdf)

* In this paper, the authors…
  + Reviewed whether password managers on mobile devices make use of the OS security features on the device and whether they provide an improvement over those security features alone
  + Analyzed the encryption methods used and methods of storage for each of the popular password managers, assuming that a copy of the device password database could be acquired by an attacker, but did not consider network attacks
  + Discovered that no third party password manager was better in protecting passwords than the OS built-in features, with a large number not providing any protection whatsoever
* This will help our project because…
  + A couple of the password managers used on mobile have mirrored password managers for desktop, these were among the more effective password managers but still fell significantly short of the OS built-in password protection features
  + We could use this to evaluate how the users feeling of security with regards to a password manager correlate to the actual security offered by the password manager. We could also ask users that make use of LastPass and 1Password if they have a different feeling toward the mobile and desktop variants with regards to utility and security
  + The issue with some of the managers with available desktop variants was in storage of passwords once downloaded, reviewing if browser based managers store passwords locally on a mobile device may highlight differences between security of browser and third party with regards to mobile devices. Asking users of both desktop and mobile variants whether they download the passwords could highlight utility features that degrade security

An investigation into users’ considerations towards using password managers, Fagan et al., 2017

Being worked on by: Sithara

[Link](https://hcis-journal.springeropen.com/articles/10.1186/s13673-017-0093-6)

* In this paper, the authors…
  + give an insight into why some people use password managers and others do not.
* This will help our project because…
  + This paper will be important for our project as it helps us determine what is the ultimate motive of the people who use password managers and why the other side don’t even feel the need to.
  + This article will help us build the right prototype and give an idea on how can the majority of the users be motivated to use password manager not just for convenience but also for the security gain.

Choosing the Right Password Manager, Gallagher, 2019

Being worked on by: Sithara

[Link](https://www.tandfonline.com/doi/full/10.1080/00987913.2019.1611310)

* In this paper, the authors…
  + This article mainly compares 3 different third-party tools (1Password, KeePass, LastPass) and briefs on the pros and cons of each tool
* This will help our project because…
  + It gives a very important piece of information about how the budget can affect people using third-party tools. As in, people or company might not prefer a password manager which is pretty expensive if does not fit their budget.
  + It also helps users determine what do different 3rd party tools offer and helps us answer questions like why users prefer one third party tool over the other and what do the majority of the users look for when they choose a password manager.

Password-manager friendly (PMF): Semantic annotations to improve the effectiveness of password managers, Stajano et al., 2014

Being worked on by: Sithara

[Link](https://www.repository.cam.ac.uk/bitstream/handle/1810/279242/2015-StajanoSpeJenSta-pmf.pdf?sequence=1&isAllowed=y)

* In this paper, the authors…
  + This article explains why people refuse to use password managers owing to their complexity and what can be done to improve usability.
* This will help our project because…
  + This article helps us understand that password managers often fail to be used as they employ complex heuristics.
  + This article might help us building our prototype as it strategizes on how can a password manager be designed that is user-friendly and yet effective.

A Comparative Usability Evaluation of Traditional Password Managers, Karole et al., 2010

Being worked on by: Sunny

[Link](https://link.springer.com/chapter/10.1007/978-3-642-24209-0_16)

* In this paper, the authors…
  + The authors compare online Password Managers (Lastpass) to portable Password Manager on the basis of usability via assessing the pre-test and post-test results.
  + Compare the sample based on pre-test usability factors (Toughness, Satisfaction) and post-test usability factors (Control,Perceived Ease, Perceived Necessity and Perceived Security).
  + The key findings were that most of the users preferred portable Password managers over online Password Managers, with sense of security being the most important factor for not picking online PM.
* This will help our project because…
  + May be able to use the factors for understanding usability
  + May help reference the factors further broken into the type of occupation in understanding usability preference.

A Usability Study and Critique of Two Password Managers, Chiasson et al., 2005

Being worked on by: Sunny

Link

* In this paper, the authors…
  + The study performs a usability study and compares 2 Password Managers (PwD Hash and Password Multiplier)
  + Participants were asked to use both the password managers and were asked to fill a survey. Furthermore, an examiner also examined how users interacted with both the managers.
* This will help our project because…
  + Helps understand that understanding a users mental model is necessary for providing them with a usable interface. The interface must support the users mental model and fit into its work patterns to be useful.
  + Designing interface that have better feedback, which in turn helps reduce the Gulf of Evaluation.

Toward a secure and usable cloud-based password manager for web browsers, Zhao et al., 2014

Being worked on by: Zachary

[Link](https://novanet-primo.hosted.exlibrisgroup.com/permalink/f/ljnbc9/TN_sciversesciencedirect_elsevierS0167-4048(14)00105-9)

* In this paper, the authors…
  + Look at shortcomings of existing browser-based password managers (BPMs) before implementing their own cloud storage BPM, as well as accompanying design
  + Compare BPMs, look at security holes, propose a design, implement/evaluate it
  + Show that BPMs can be vulnerable to attack, and that their framework is positively received by test users
* This will help our project because…
  + We also wish to look at BPMs before implementing our own
  + We may be able to use/modify their CSF-BPM design in our own extension
  + They define activities for users to perform as part of their analysis, which we could use/modify for our own purposes

Amnesia: A Bilateral Generative Password Manager, Wang et al., 2016

Being worked on by: Zachary

[Link](https://novanet-primo.hosted.exlibrisgroup.com/permalink/f/ljnbc9/TN_ieee_s7536530)

* In this paper, the authors…
  + Create a new cloud-based, bilateral, password manager that is generates passwords as they are needed, instead of storing/retrieving them
  + Create the framework, and then conduct a user study to gauge success
  + Find that their framework allows for a heightened level of password security and does not significantly impact user convenience
* This will help our project because…
  + We are also building a framework/evaluating it, so can look to this article as an example
  + Their questions/findings on user feedback for the framework may be good questions to ask when evaluating our own framework
  + We may be able to use some of their suggested development tools when we go to build our own framework

User Password Generation Practices and Strong Password Guideline Compliance, Riley et al., 2006

Being worked on by: Zachary

[Link](https://novanet-primo.hosted.exlibrisgroup.com/permalink/f/ljnbc9/TN_sage_s10_1177_154193120605001720)

* In this paper, the authors…
  + Discover the prevailing password practices of college students
  + Conduct a questionnaire into internet usage, password-protected accounts, password generation, user beliefs, and demographics
  + Determine that, in general, users make bad passwords and don’t change them unless they have to. They also highlight characteristics of human-generated passwords
* This will help our project because…
  + We will need to ask similar password generation and password-protected account information (# of accts, differences in passwords, etc.)
  + The dichotomy between what users *know* that should do and what they *actually* do (they know they should change/vary their passwords but don’t) is supportive of a convenient tool to do such actions. That is: users are bad at making passwords!
  + It confirms one idea that is central to all password managers: remembering the passwords is the most important factor in choosing a password. If you take away the remembrance, then security can take a more dominant role

Stronger password authentication using browser extensions, Ross et al.,2005

Being worked on by: Shehzeen

[Link](http://crypto.stanford.edu/~jcm/papers/pwdhash.pdf)

* In this paper, the authors
  + Discusses a PwdHash which is a browser extension used for generating unique passwords for different sites as required by the user.
  + The framework is suggested to overcome the challenges of hashed user passwords in browser extension and discusses the limitations of the framework.
* This will help our project because…
  + it discusses the problems and challenges when the user password is hashed in browsers extension We can face similar problems while building a framework such as JavaScript attack, salting , encoding , autocomplete, password reset and dictionary attack are the few problems which needs to be address in order to maintain password security.