

Gossamer: Securely Measuring Password-based Logins ...

Author: Marina Sanusi Bohuk
Mazharul Islam
Suleman Ahmad
Michael Swift
Thomas Ristenpart
Rahul Chatterjee

Final Report

Team member: Xing Chen
Dian Chen

Special thanks to Prof. Sven Dietrich !!!

Project Summary

- Creation of login system and login page.
- Based on sensitivity of monitoring submitted passwords rather than creation process.
- Make observations based on login behaviour and statistics:
 - percentage of user passwords recorded in breaches
 - percentage of users that may be using a password manager

	Univ. 1	Univ. 2
Session Statistics (with a 360s threshold)		
Avg. session size	2.25	2.21
99th percentile session size	10	6
% abandoned sessions	5.47%	1.96%
User Statistics		
# of unique usernames seen	196,424	309,801
# of valid users	177,286	169,774
# of active users	130,695	110,476
% valid users w/ weak passwords	0.03%	0.06%
% valid users w/ username in breach [†]	5.79%	3.27%
% valid users w/ passwords in breach [†]	2.92%	9.34%
% valid users w/ user-pw pair in breach [†]	0.01%	0.15%
% valid users w/ tweaked password	1.22%	0.66%
% valid users who may be using password managers	24.76%	27.34%
Avg. devices per user per day	1.51	1.91
Avg. devices per user (over whole time period)	14.51	14.97
Avg. num unique passwords per user	1.96	9.59
Login Statistics		
Avg. Login requests per day	49,302	246,274
Avg. # of submitted usernames per day	24,822	61,798
% of requests succeeded	94.99%	92.35%
Avg. # requests per day per user	1.99	2.05
% of requests from mobile device	31.00%	35.57%
% IPs from VPNs, proxies, or Tor nodes	22.08%	4.91%
Submitted password statistics		
% req. w/ password in breach [†]	2.71%	0.10%
% req. w/ user-pwd pair in breach [†]	0.07%	0.01%
% failed req. containing a typo	29.67%	12.04%
% failed req. (with edit dist msmt) containing a typo	62.39%	58.37%
% failed req. from mobile device containing a typo	38.63%	38.36%
% failed req. (with edit dist msmt) from mobile device containing a typo	72.69%	81.87%
% pwds tweaked	0.92%	0.34%

Figure 1: (Bohuk et al , 2022)

Understanding Gossamer

Core Components -

- Measurement Service
- Ephemeral Database
- Persistent Database
- Analysis service

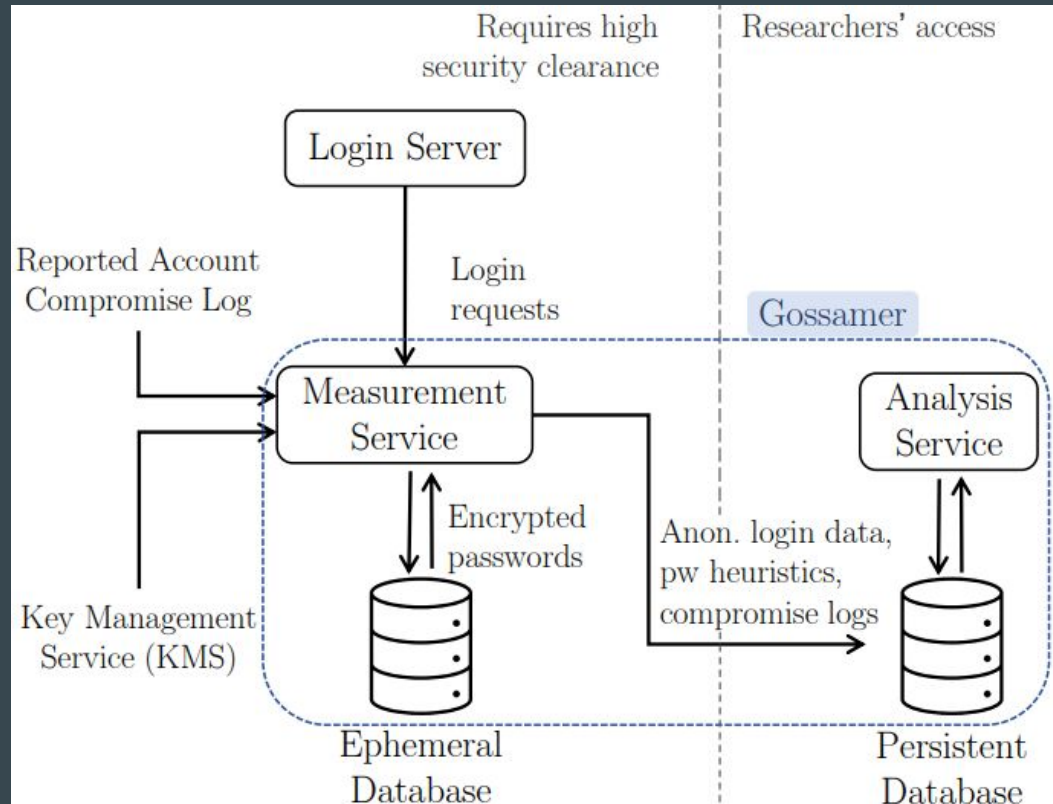


Figure 2: (Bohuk et al , 2022)

How is it secure?

Ephemeral Database - Any information stored is erased every 24 hours or on reboot

Measurement Service - Stores encrypted passwords on ephemeral database

Adheres to four security principles

- Least privilege
- Bounded-leakage logging
- Periodic deletion
- Safe on reboot

Motivation for the Project

- Compare our finding using Amazon MTurk with Author's work.
- Lead to valuable observations that may improve both password security and usability.
 - Researchers found that there is a massive decrease in locked out accounts simply by detecting the number of entries that were unique passwords.
 - creation of better password policies without much increase in risk for users

Initial Approach

- Create login system using PHP and set up Gossamer in this environment.
- Using Amazon Mechanical Turk to gather enough source of account creation and simulating a base of users with daily logins.
- Attempt to establish communication with users in order to generate returning users.

Expected Outcomes

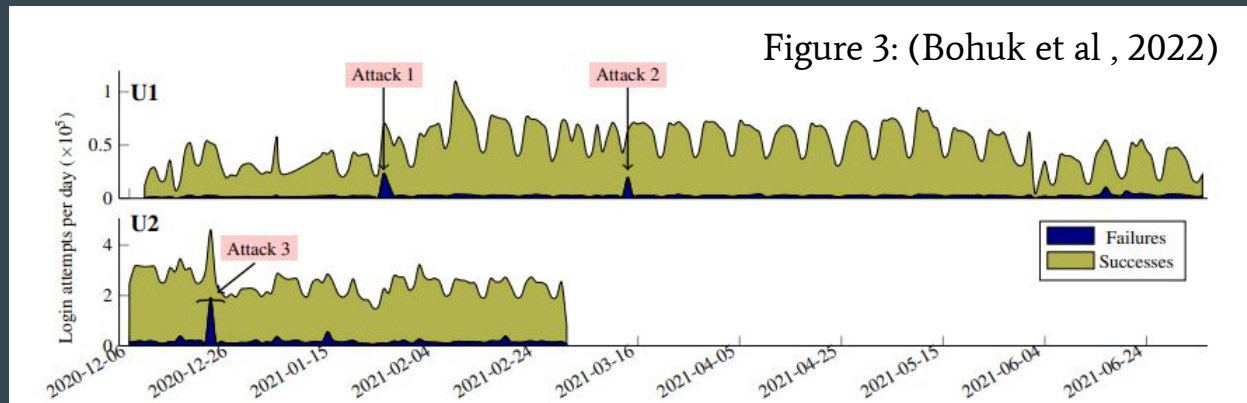
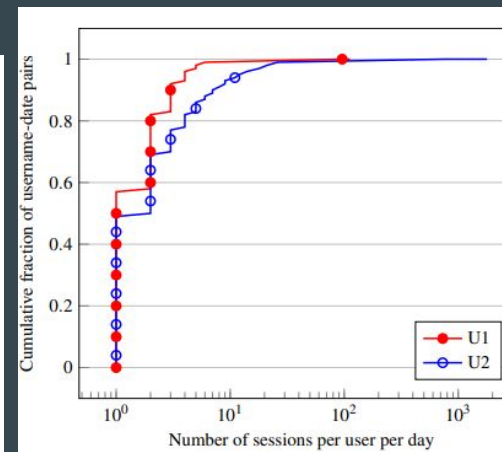


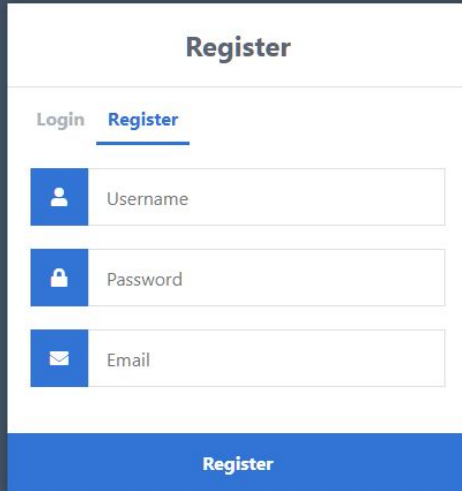
Figure 4: (Bohuk et al ,2022)



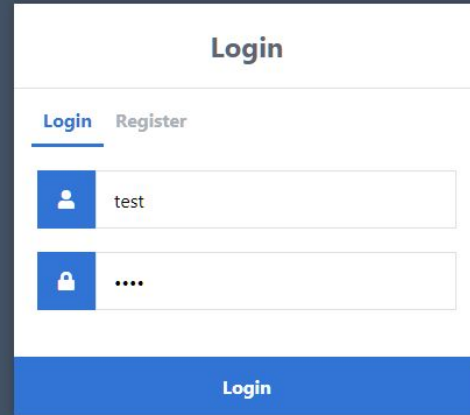
- Showcase Gossamer's ability to identify password characteristics of users in a secure and non-intrusive way.
 - Number of unique users
 - Percentage of users with weak passwords
 - Percentage of passwords in public breaches
 - Percentage of users who may be using password managers
- Compare our finding with author, if differ, analyze the result further.
- Stretch Goal: Run an experiment with zxcvbn as a strength indicator during password creation to monitor any difference in password habits.

Attempt

- Find existing login system that allow us to implement Gossamer tool.
- Create own login page and login system

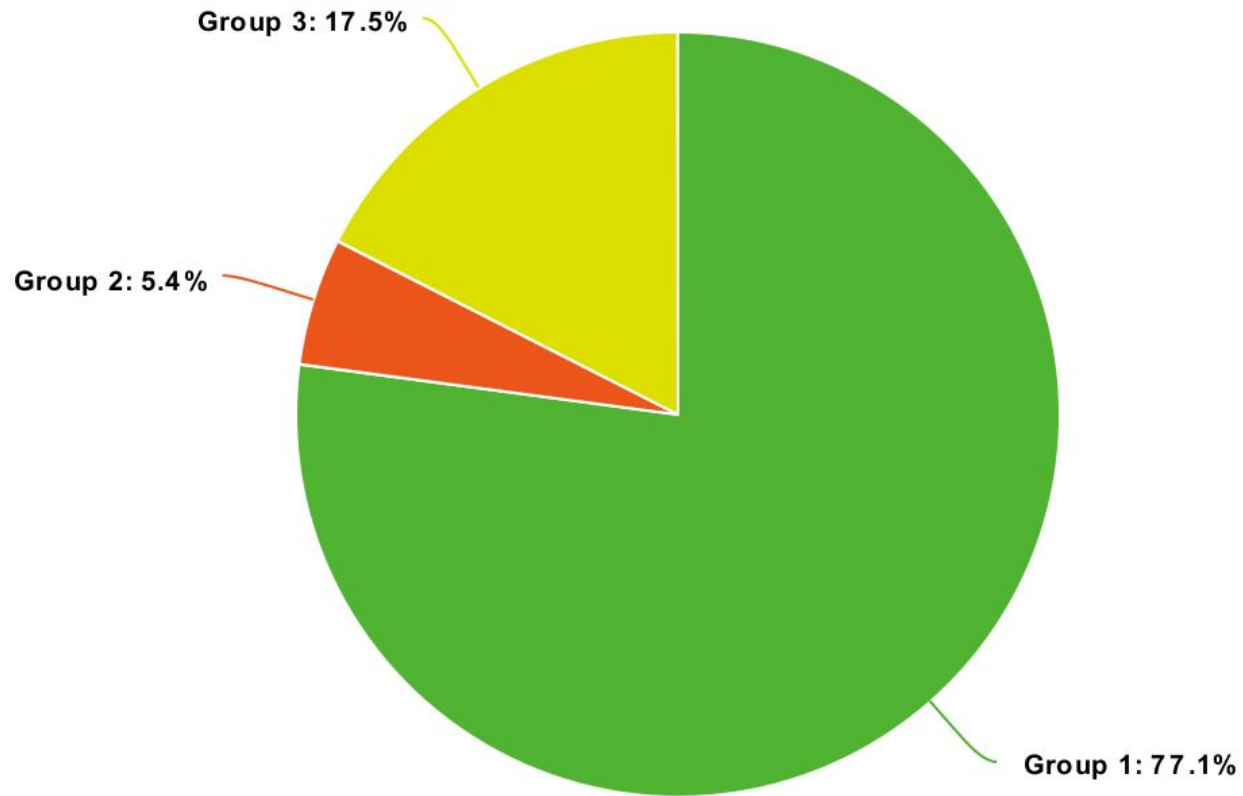


A mockup of a registration form. At the top, the word "Register" is centered. Below it, there are two tabs: "Login" and "Register", with "Register" being the active tab. The form contains three input fields, each with a blue icon on the left: a person icon for "Username", a lock icon for "Password", and an envelope icon for "Email". At the bottom of the form is a blue button labeled "Register".



A mockup of a login form. At the top, the word "Login" is centered. Below it, there are two tabs: "Login" and "Register", with "Login" being the active tab. The form contains two input fields, each with a blue icon on the left: a person icon for the username field, which contains the text "test", and a lock icon for the password field, which contains four dots. At the bottom of the form is a blue button labeled "Login".

Distribution of Password



■ Group 1 ■ Group 2 ■ Group 3

Challenges

- Lack of knowledge in login system
- Limit time and resource
- Website created lack of data collection

Finding & Learning

- Excessive login failure compare to login attempt should be alert as attack
- Typos are very common mistake among login attempts nearly 20-30%
- Breached passwords are still being widely used
- Password management are great tool to minimize login friction
- Two-factor password authentication slows logins process hinders user experience.

Future Goal

- Create a useful website (ie. coupon code site)
 - Generate repeated user contributing to login system.
 - Store valuable information on the user account.
- Implement Gossamer tool with extended period of time.
 - Possibly monitor real-world attack that challenge login system.
- Educate public on risk factor found with Gossamer

References

- M. S. Bohuk, M. Islam, S. Ahmad, M. Swift, T. Ristenpart, and R. Chatterjee, “Gossamer: Securely measuring password-based logins,” in 31th USENIX Security Symposium (USENIX Security ’22), USENIX Association, Aug. 2022. [Online]. Available: <https://www.cs.cornell.edu/~marina/Gossamer.pdf>