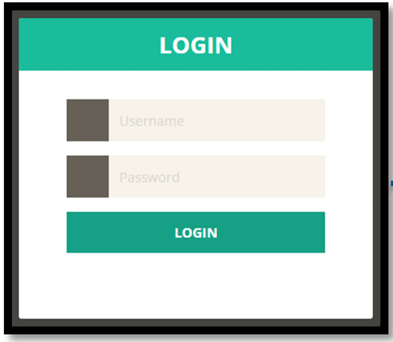
Gossamer:
Securely Measuring Password-based Logins

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

CORNELL TECH

THE UNIVERSITY of WISCONSIN MADISON

Modern Authentication Systems

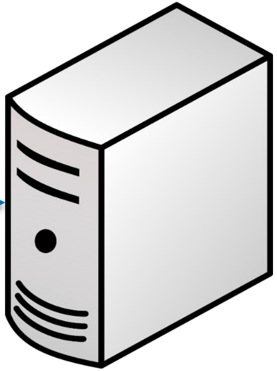


Client

username, password

+ IP address
+ user agent

+ password information



Is hash(password) in the database?

Freeman et al. 2016

Tian et al. 2019

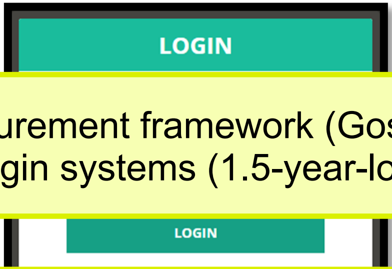
Passwords are no longer sufficient!

Credential stuffing is a huge source of account compromise.

How do we separate benign and malicious traffic?

How do we safely log information about actual passwords?

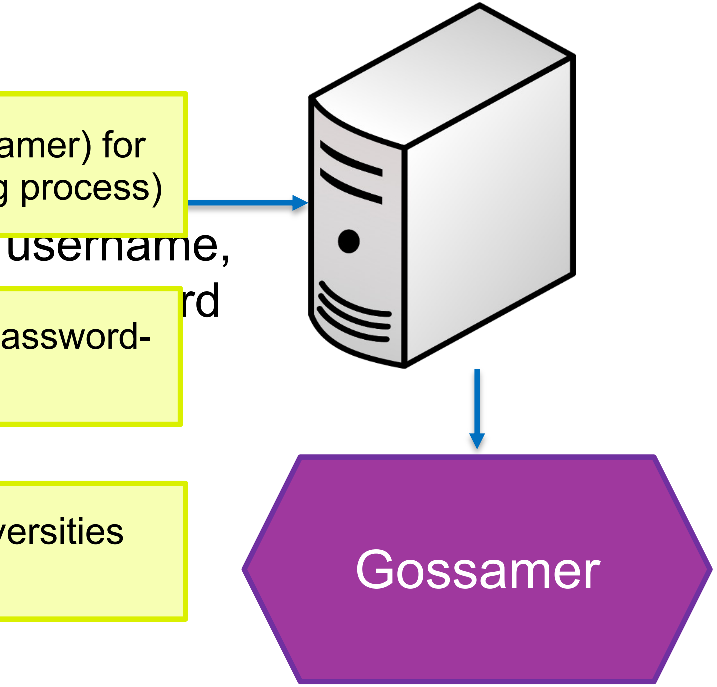
Logging Password-Derived Measurements



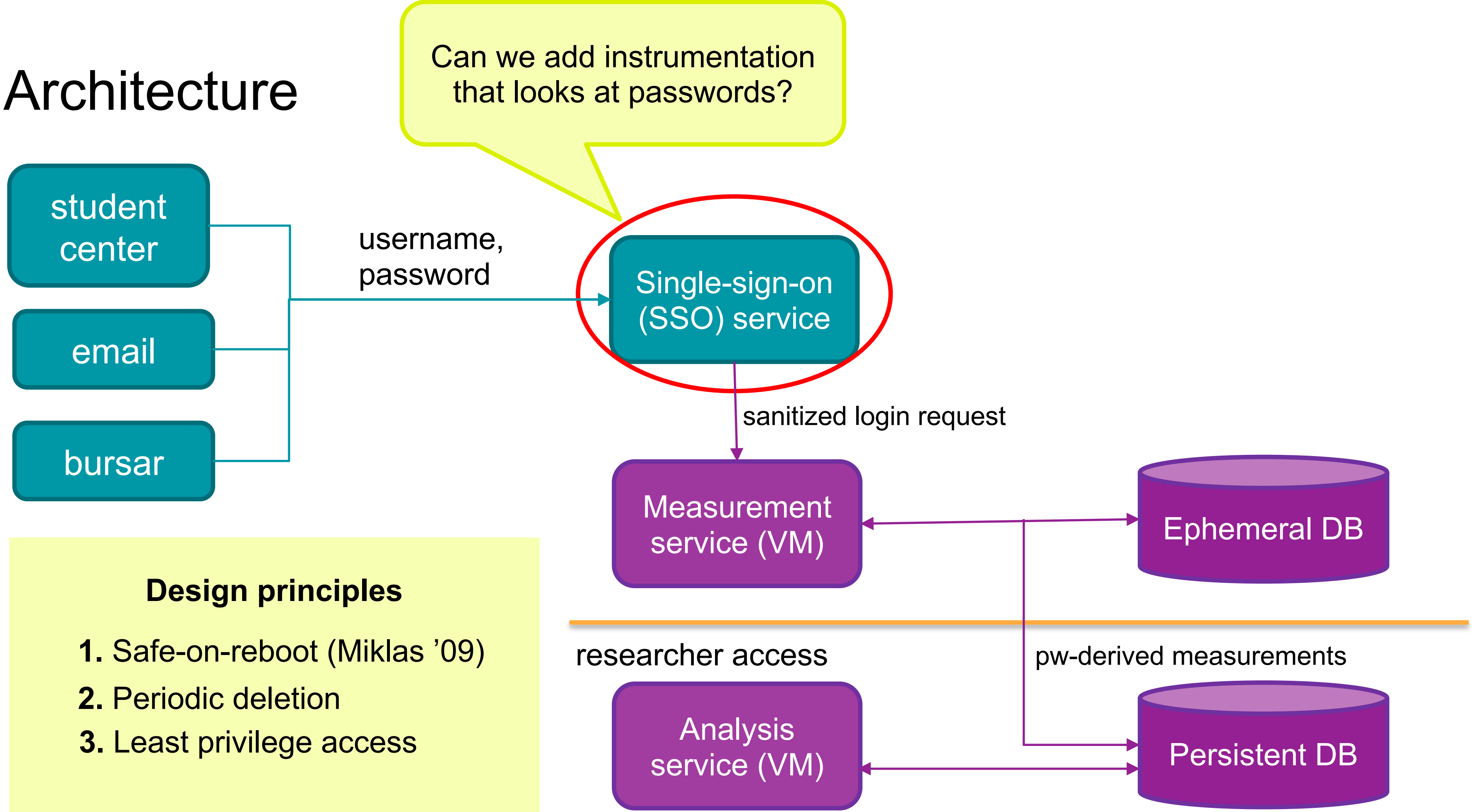
Design a measurement framework (Gossamer) for use with web login systems (1.5-year-long process)

Describe a process for assessing risk of password-based measurements.

Conduct a measurement study at two universities observing over 34M login requests.



Architecture



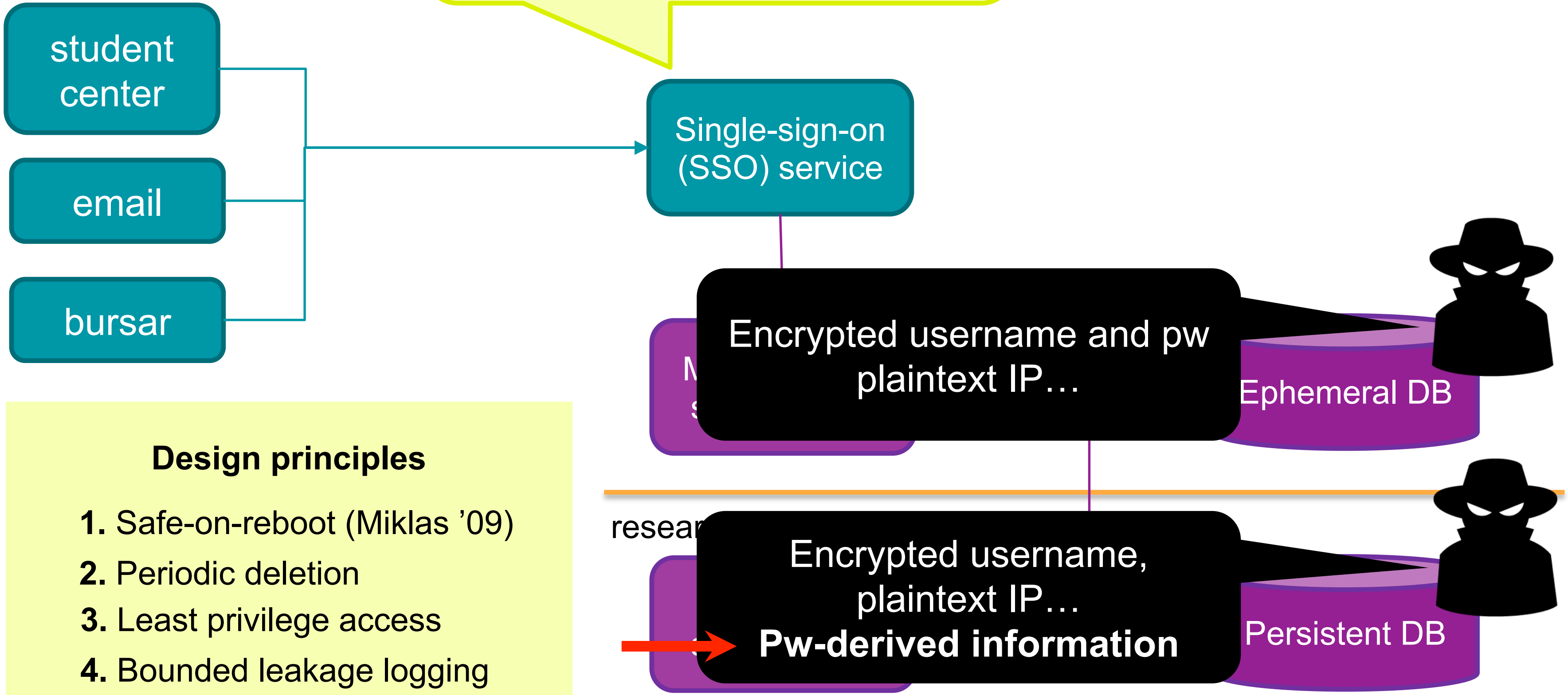
Can we add instrumentation that looks at passwords?

Design principles

1. Safe-on-reboot (Miklas ’09)
2. Periodic deletion
3. Least privilege access

Architecture

If compromised, how could attackers use password-derived measurements to speed up attacks?



student center

email

bursar

Single-sign-on (SSO) service

M

s

Ephemeral DB

Encrypted username and pw plaintext IP…

resear

Persistent DB

Encrypted username, plaintext IP…
Pw-derived information

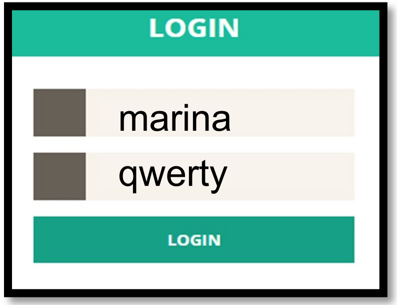
Design principles

1. Safe-on-reboot (Miklas ’09)
2. Periodic deletion
3. Least privilege access
4. Bounded leakage logging

How can we choose safe measurements to log?

Guess list
Gossamer logs
(Encrypted) username

Sends guess



marina
qwerty

Attacker guess list

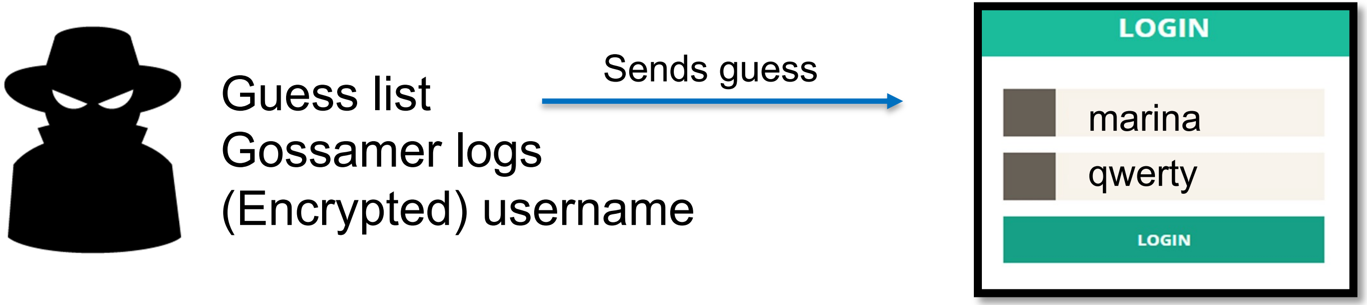
Guess rank	Password
1	qwerty
2	abc123
3	hunter
4	jessica
5	spider

5 guesses

Gossamer logs

Encrypted username	zxcvbn score
01VB5TH	2
gk3pPhL	1
trZQA1L	3
jNKR3Yp	2
OXJFw2r	4

How can we choose safe measurements to log?



Guess list
Gossamer logs
(Encrypted) username

Sends guess

Attacker guess list

Guess rank	Password	zxcvbn score
~~1~~	~~qwerty~~	~~1~~
~~2~~	~~abc123~~	~~0~~
~~3~~	~~hunter~~	~~4~~
~~4~~	~~jessica~~	~~2~~
5	spider	3

1 guess

Gossamer logs

Encrypted username	zxcvbn score
01VB5TH	2
gk3pPhL	1
trZQA1L	3
jNKR3Yp	2
OXJFw2r	4

How can we choose safe measurements to log?

Dataset: 307 million breached passwords

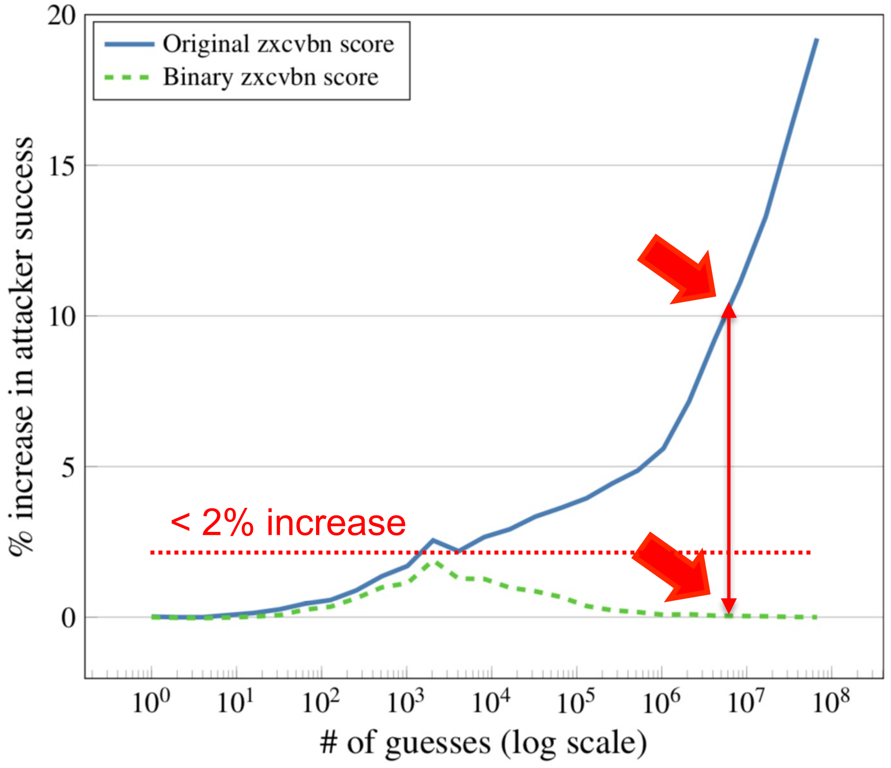
Attacker’s guess list: 80% split

Target passwords: 10k passwords sampled from remaining 20%

Problem: Original zxcvbn score leaks too much information!

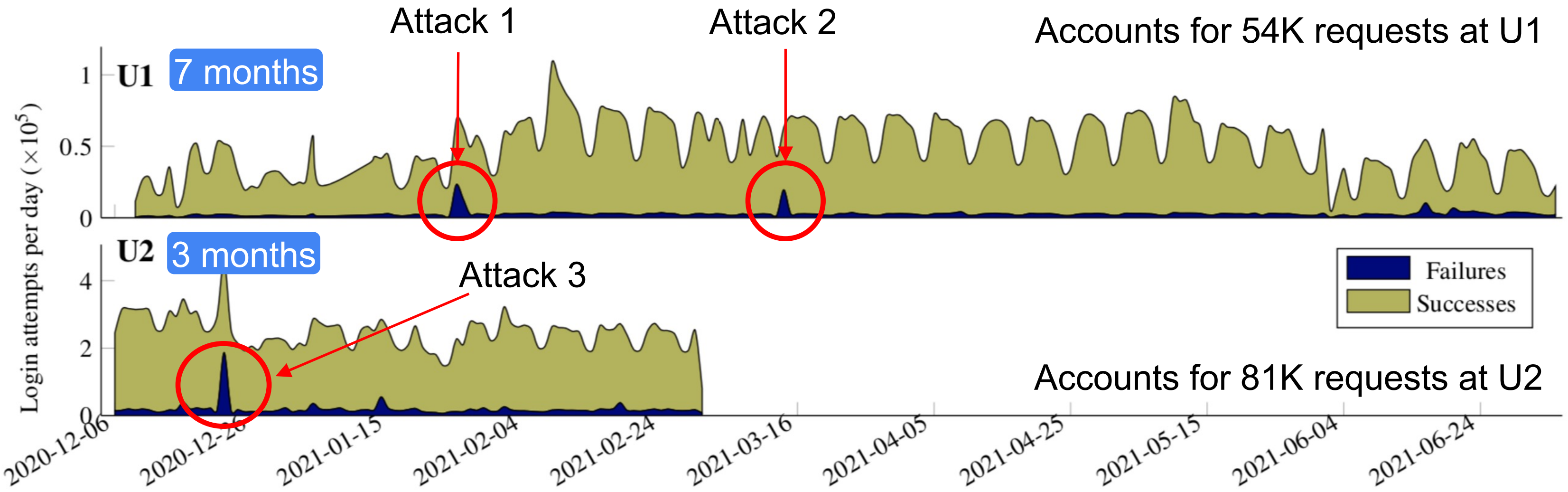
Solution: Bucketize score to [0, 1]

✓ **Bounded leakage logging**



Deploying Gossamer

Observed some high-volume attacks



Accounts for 54K requests at U1

Accounts for 81K requests at U2

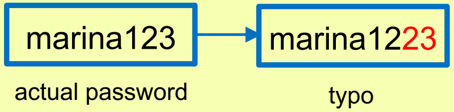
Obtained approval from respective IRB and the IT offices.

Collected **34M** total login requests

Login friction is still high

Typos are frequent

Over 1 in 3 failed requests at U1 were typos. Even more for mobile logins.



Retries are common

●○○○○ 1/5 at U1

●○○ 1/3 at U2

eventually successful sessions required more than one attempt.

2FA impedes usability

Duo adds an average of 14 seconds to a user’s login.

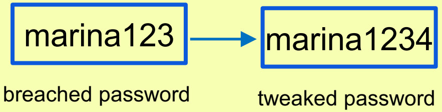
Password managers could help…

About 25% of users use password managers.

Breached credential use is a problem.

23 U1 users and 254 U2 users were using a **breached password**.

Over 2K U1 users and 1K U2 users were using a **tweaked breached** password



marina123 → marina1234

breached password

tweaked password

The high-volume attacks had **high fractions** of breached passwords.

Solution: Proactive breach alerting

Thomas et al. 2019, Li et al. 2019, Pal et al. 2022

Next: Investigate how to detect attacks better using these measurements

Gossamer

Safely record information about submitted passwords

- Bounded leakage logging
- Assess risk; reduce granularity

Extend with additional measurements

- Simulate improvement in attack

Gain insight into user and attacker behavior

- Can inform new policies
- Develop countermeasures

https://cs.cornell.edu/~marina/gossamer

Marina Bohuk | marina@cs.cornell.edu
Mazharul Islam | mislam9@wisc.edu