# Moving to client-side hashing for online authentication

Enka Blanchard[1] Xavier Coquand[2] Ted Selker[3]

Digitrust, Loria, Université de Lorraine, www.koliaza.com

Bsecure, Paris

University of Maryland, Baltimore County

9th International Workshop on Socio-Technical Aspects in SecuriTy
@ ESORICS September 26th, 2019

# Why hash passwords?

# Password hashing: best practices

How to hash correctly:

- Use a salt for each password
- Use a secure password hashing algorithm (Argon2 or bcrypt)
- Protect against side-channels (e.g. HTTP)
- Don't keep duplicates or logs

# Poll: how long have we been saying this?

# 1968: Sir Maurice Vincent Wilkes, commenting on Roger Needham's 1967 password system

# 2015-2016 leaks

| website | encryption | # accounts leaked | leak date |
|---|---|---:|---:|
| 000webhost.com | clear | 15035687 | Mar. 2015 |
| sprashivai.ru | clear | 3472645 | May 2015 |
| **ashleymadison.com** | **bcrypt** | 36140796 | July 2015 |
| 17.media | MD5 | 3824575 | Sep. 2015 |
| mpgh.net | MD5+salt | 3119180 | Oct. 2015 |
| r2games.com | MD5+salt | 11758232 | Oct. 2015 |
| nexusmods.com | MD5+salt | 5918540 | Dec. 2015 |
| mate1.com | clear | 27402581 | Feb. 2016 |
| naughtyamerica.com | MD5 | 989401 | Apr. 2016 |
| badoo.com | MD5 | 122730419 | June 2016 |

Table: Partial list of leaks analysed in 2016 by Jaeger et al.

# How about client-side hashing?

# Detecting client-side hashing

How we can find out if a website uses client-side hashing:

- Semantic and syntactic analysis: observe "password" in the packet or follow memory cells
- Computing load analysis: good hashing takes resources

This can only detect absence of good hashing, no positive guarantee.

# Client-side hashing in the Alexa 50

| Websites | | | | |
|---|---|---|---|---|
| google.com | tmall.com | blogspot.com | mail.ru | xvideos.com |
| youtube.com | reddit.com | netflix.com | bing.com | tribunnews.com |
| facebook.com | instagram.com | linkedin.com | microsoft.com | amazon.co.jp |
| baidu.com | live.com | bilibili.com | whatsapp.com | google.co.in |
| wikipedia.org | vk.com | twitch.tv | naver.com | github.com |
| qq.com | sohu.com | pornhub.com | aliexpress.com | okezone.com |
| yahoo.com | jd.com | login.tmall.com | livejasmin.com | imdb.com |
| amazon.com | yandex.ru | 360.cn | microsoftonline.com | google.com.hk |
| taobao.com | sina.com.cn | csdn.net | alipay.com | pages.tmall.com |
| twitter.com | weibo.com | yahoo.co.jp | ebay.com | stackoverflow.com |

# Client-side hashing in the Alexa 50

| Websites | | | | |
|---|---|---|---|---|
| google.com | tmall.com | blogspot.com | mail.ru | xvideos.com |
| youtube.com | reddit.com | netflix.com | bing.com | tribunnews.com |
| facebook.com | instagram.com | linkedin.com | microsoft.com | amazon.co.jp |
| **baidu.com** | live.com | bilibili.com | whatsapp.com | google.co.in |
| wikipedia.org | vk.com | twitch.tv | naver.com | github.com |
| **qq.com** | sohu.com | pornhub.com | aliexpress.com | okezone.com |
| yahoo.com | jd.com | login.tmall.com | livejasmin.com | imdb.com |
| amazon.com | yandex.ru | **360.cn** | microsoftonline.com | google.com.hk |
| **taobao.com** | **sina.com.cn** | **csdn.net** | **alipay.com** | pages.tmall.com |
| twitter.com | **weibo.com** | yahoo.co.jp | ebay.com | stackoverflow.com |

## 1-to-1 correspondance between client-side hashing and Chinese websites

# Why not use client-side hashing?

# Client-side hashing: drawbacks

Four potential drawbacks:

- Incompatibility with legacy protocols
- Same-site authentication attacks after leaks
- Computing power limits
- Script blocking

# Client-side hashing: advantages

Six main advantages:

- No credential reuse attack
- Lower server costs
- Stronger hashing
- Makes phishing slightly harder
- Simpler if standardised
- **Enforces accountability**

# Client-side hashing: advantages

Six main advantages:

- No credential reuse attack
- Lower server costs
- Stronger hashing
- Makes phishing slightly harder
- Simpler if standardised
- **Enforces accountability**

# Making changes: globally

To change the ecosystem:

- Update the belief that client-side is detrimental, for both researchers and developers
- Change the incentive structure, as with the padlock

Ideally: convince large browser developers or standards organisation

# Making changes: for the user

It should not affect their experience in general.

Two main immediate options:

- Create an extension to warn them in case of unsecure systems
- Detecting and hashing passwords on the client

**Thank you for your attention**