Better Security for Password and Two-Factor Authentication

Stanislaw Jarecki (University of California Irvine)

Nitesh Saxena (University of Alabama Birmingham)

Main collaborators:

Aggelos Kiayas (U Edinburgh)

Hugo Krawczyk (IBM Research)

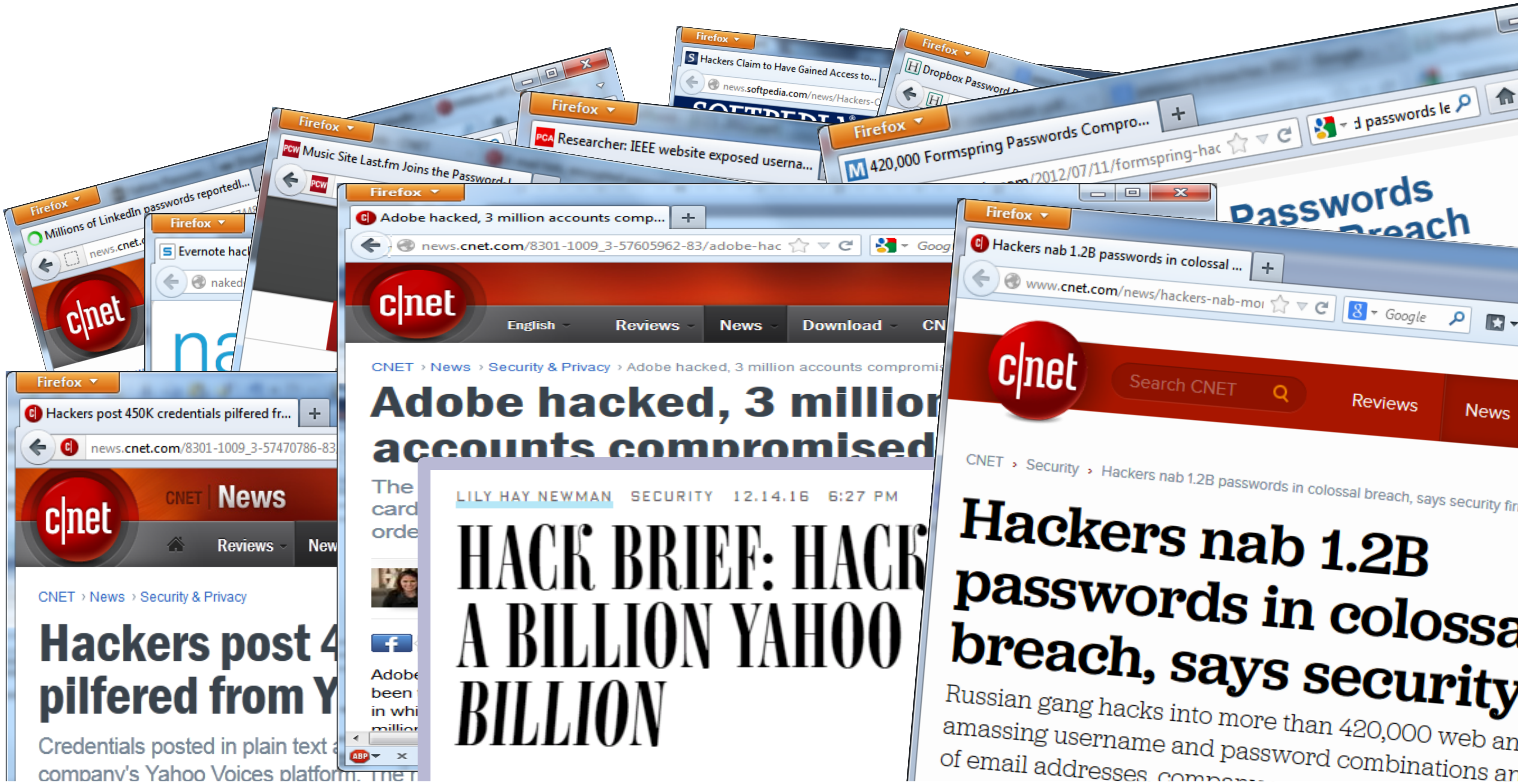
PhD students on the project:

Maliheh Shirvanian (UA Birmingham)

Jiayu Xu (UC Irvine)

Password (In)Security

- Passwords: **MAIN** authentication tool in the digital era
- Protect our lives and social order, *conveniently* and **Insecurely**



Millions of LinkedIn passwords reportedl...

Evernote hac

Music Site Last.fm Joins the Password-...

Hackers Claim to Have Gained Access to...

news.softpedia.com/news/Hackers-C

Dropbox Password P

Researcher: IEEE website exposed userna...

420,000 Formspring Passwords Compro...

/2012/07/11/formspring-hac

d passwords le

Passwords Breach

Adobe hacked, 3 million accounts comp...

news.cnet.com/8301-1009_3-57605962-83/adobe-hac

English Reviews News Download CN

CNET › News › Security & Privacy › Adobe hacked, 3 million accounts compromis

Adobe hacked, 3 million accounts compromised

Hackers post 450K credentials pilfered fr...

news.cnet.com/8301-1009_3-57470786-83

CNET News

Reviews New

CNET › News › Security & Privacy

Hackers post 4 pilfered from Y

Credentials posted in plain text company's Yahoo Voices platform. The

LILY HAY NEWMAN SECURITY 12.14.16 6:27 PM

HACK BRIEF: HACK A BILLION YAHOO BILLION

Hackers nab 1.2B passwords in colossal ...

www.cnet.com/news/hackers-nab-mo

Search CNET Reviews News

CNET › Security › Hackers nab 1.2B passwords in colossal breach, says security fir

Hackers nab 1.2B passwords in colossal breach, says security

Russian gang hacks into more than 420,000 web an amassing username and password combinations ar of email addresses. Compan

Password (In)Security

Unacceptable State of Affairs

- Attackers routinely compromise servers
  - □ Steal password-related data
  - □ Recover user's password via Offline Dictionary Attack
- BILLIONS of passwords stolen
  - □ MySpace 360M, LinkedIn 165M, eBay 145M,…, Yahoo 3B (!!)
  - □ … Twitter, RSA, Google, Dropbox, PayPal, Sony, …
- *Current* Two-Factor Authentication schemes do not stop this leakage
  - □ TFA reduces to 2nd factor (e.g. cell phone) security if password leaks
  - □ But current TFA's do nothing to protect passwords from leakage

Cryptography Can Help!

- We show ways to strengthen password and two-factor protocols
- Using simple, well-established techniques
  - Mostly blinded Diffie-Hellman [Chaum, Ford-Kaliski, Boyen, …]
- Efficient. Mature. Applicable to the infrastructure used today. **Ready for deployment** in the **real world**.
- Please talk to me if you are interested to learn more (esp. if you see where we can improve, or if you want to transfer this to practice).

Attacks on Password Authentication #1: Offline Dictionary Attack (ODA)

- ODA is the main source of password compromise:
  - □ *Deadly combination* of human memory limitation (→ low entropy passwords) and server compromise
  - □ Stealing the "password file" allows testing password guesses against stored hashes; millions++ of password per second (from s/w to dedicated h/w)

Goal: Render these unavoidable exhaustive attacks ineffective!

How: Enforce high-entropy passwords using additional devices/servers

Attacks on Password Authentication #1: Offline Dictionary Attack (ODA)

- ODA is the main source of password compromise

Goal: Render these unavoidable exhaustive attacks ineffective!

How: Enforce high-entropy passwords using additional devices/servers

- What Devices?
  - □ Cell phone, USB stick: Already used in Two-Factor Authentication!
- What Servers?
  - □ Can be hosted by any cloud service
  - □ End-users can utilize it *transparently* to web servers
  - □ Web servers can utilize it *transparently* to end-users

Attacks on Password and Two-Factor Authentication #2,3,4,…

2. Online dict. attacks (<u>unavoidable</u>): Guess password; try it online.
   - Works w/weak pwds and in targeted attacks (pers. info, sister pwd)
   - 2nd factor helps, but we could do better even here!
3. Phishing/PKI attack: User tricked to send password to the attacker
   - paypa1.com, overwritten links in email, URL-browser manipulation, …
   - *Cert signed by rogue CA* (do ***you*** know your browser's CA's?)
   - *A* certificate flagged by the browser but user accepts ("clicking through")
4. Malware on the client (terminal, laptop, phone), e.g. *keyloggers*

Goal: Eliminate, neutralize, or reduce exposure to these attacks

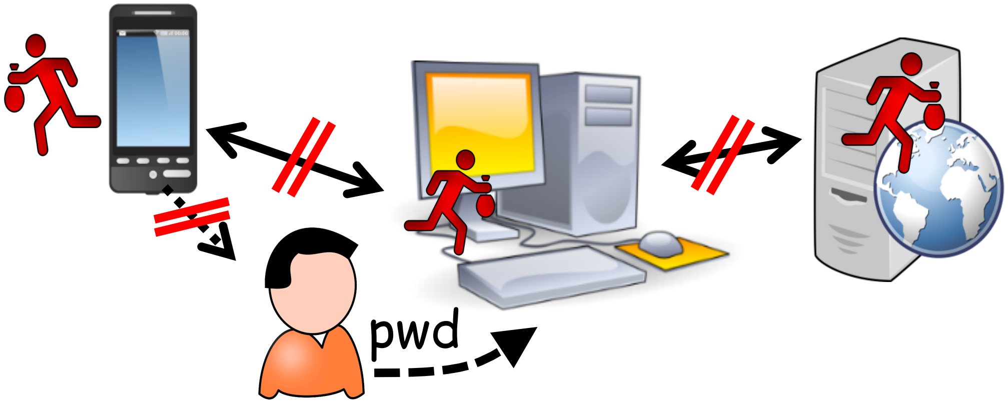
How: Additional devices/servers help, and better cryptography helps!

Better Security for Password and Two-Factor Authentication

Stanislaw Jarecki (UC Irvine), Nitesh Saxena (UA Birmingham)

PASSWORD AUTHENTICATION with 2nd FACTOR

End-to-end security = each component can be compromised:
(2nd Factor Device, Client, Server, communication links)



MOTIVATION:

- Password authentication is a *security bottleneck*
- Web services routinely compromised, hashed passwords leak
  → Hackers recover passwords via Offlline Dictionary Attack
- Current Pwd/TFAuth insecure against this (and other attacks)

MAIN OBJECTIVES:

- Achieve end-to-end (maximal) security in all attack scenarios
- Eliminate hashed passwords on servers
  → Protect passwords even if servers are compromised

SECONDARY OBJECTIVES:

- Improve TFA *usability* (e.g. PIN-copying is not necessary)

REQUIREMENTS:

- Browser Extension on Client
- Data-Connectivity on 2nd Factor Device (= Cell Phone)

SOLUTION TECHNIQUES / SPECS:

- Standard Diffie-Hellman, e.g. EC groups, as in TLS/SSL
- Computational cost = 2-3 exp's/party (≈ TLS handshake)

SEVER-TRANSPARENT MODE:

- Client gains strong authentication token from
  2nd Factor Device and/or 3rd-party Security Service

CLIENT-TRANSPARENT MODE:

- Server interacts with 3rd-party Security Service

POTENTIAL ADOPTERS:

- *Any internet user*: PwdAuth/TFA transparent to web server
- *Any internet service*: PwdAuth/TFA transparent to end-user

FIST ADOPTERS (PILOTS):

- Internet end-users using 3rd party service
- Educational Institution logon server?
- Industry PwdAuth / TFA providers as partners?

TECHNOLOGY TRANSFER:

- Software libraries will be made available

CONTACT :

- Stanislaw Jarecki, UC Irvine, sjarecki@uci.edu
- Nitesh Saxena, UA Birmingham, saxena@uab.edu