Cybersecurity in 2016 and Lessons learned

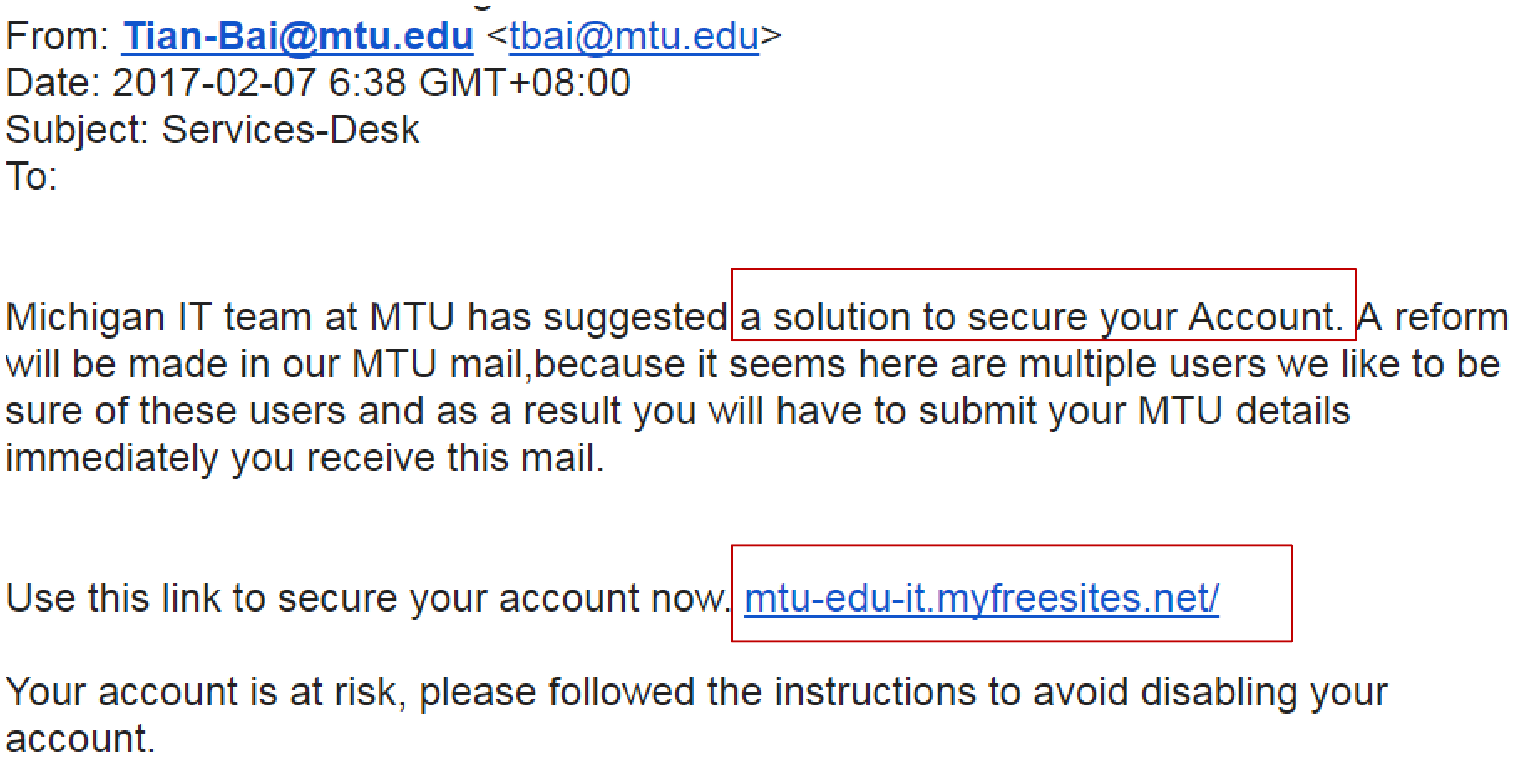
Dr. Yu Cai

Associate Professor
Program Chair, Computer Network & System Administration
School of Technology
Michigan Technological University
cai@mtu.edu

A Quick Review on Email Phishing

- I gave a talk on email phishing at Senate in 2016.
  - The situation seems to only get worse since then.
  - You can contact me to get phishing education slides
- A quick review:
  - Email is "ok" for daily, non-sensitive communication.
  - It is incredibly easy to forge an email which looks exactly like an legitimate one!
    - All students in my cybersecurity class know how to do this!
    - A phishing test site: http://www.tech.mtu.edu/~cai/temp/
  - It is possible to fool and bypass the email filters and other email security measures!
  - Be careful when opening email attachments
  - Be careful when clicking links in emails
    - If you have to, double check the URL!

A recent phishing email example



From: Tian-Bai@mtu.edu <tbai@mtu.edu>
Date: 2017-02-07 6:38 GMT+08:00
Subject: Services-Desk
To:

Michigan IT team at MTU has suggested a solution to secure your Account. A reform will be made in our MTU mail,because it seems here are multiple users we like to be sure of these users and as a result you will have to submit your MTU details immediately you receive this mail.

Use this link to secure your account now. mtu-edu-it.myfreesites.net/

Your account is at risk, please followed the instructions to avoid disabling your account.

Michigan Technological University.

A small percentage of phishing emails bypassed the email filters.

The real talk starts here

The most devastating hack in 2016

- 1.5 billion Yahoo accounts were hacked
  - Two different and independent hacks:
    - On Sept. 2016, Yahoo announced the 1st hack with 500m accounts stolen in 2014;
    - On Dec. 2016, another hack with 1b accounts stolen in 2013;
  - Worst thing is: Yahoo still doesn’t know exactly what happened!!!
  - A YouTube video (2m):
    - https://www.youtube.com/watch?v=2eTAVBfGdUA

The 2nd most devastating hack in 2016

- Old breaches come back to haunt - LinkedIn, Myspace, Dropbox hacks
  - We didn't discover the actual scope and real damage of these old breaches until 2016!
- LinkedIn data breach in 2012.
  - Previously thought to affect 6 million users
  - Actually hit 117 million users
  - How did we know these?
    - The user information is for sale on darkweb.
- Myspace hack in 2013 affected 360 million accounts.

Another Major Hack in 2016

- We don’t talk about politics here.
- Russian hack during US elections
- “Russian state-sponsored hacker group Fancy Bear” hacked DNC (Democratic National Committee) and John Podesta (Hillary Clinton campaign chief)
- WikiLeaks involved

CROWDSTRIKE
RESTROOMS
RESTROOMS
CROWDSTRIKE
Introducing
FANCY BEAR
A Black Hat special edition T-shirt available at our print station behind this video wall
FREEBUF

Lessons learned on Cybersecurity in 2016

- A few noticeable things in 2016
  - Email phishing
  - Ransomware
  - Password leaking
  - DDoS attacks
  - IoT security
- Future trends of cybersecurity
  - More cyber hacks at ordinary people…
  - National security, cyber warfare…

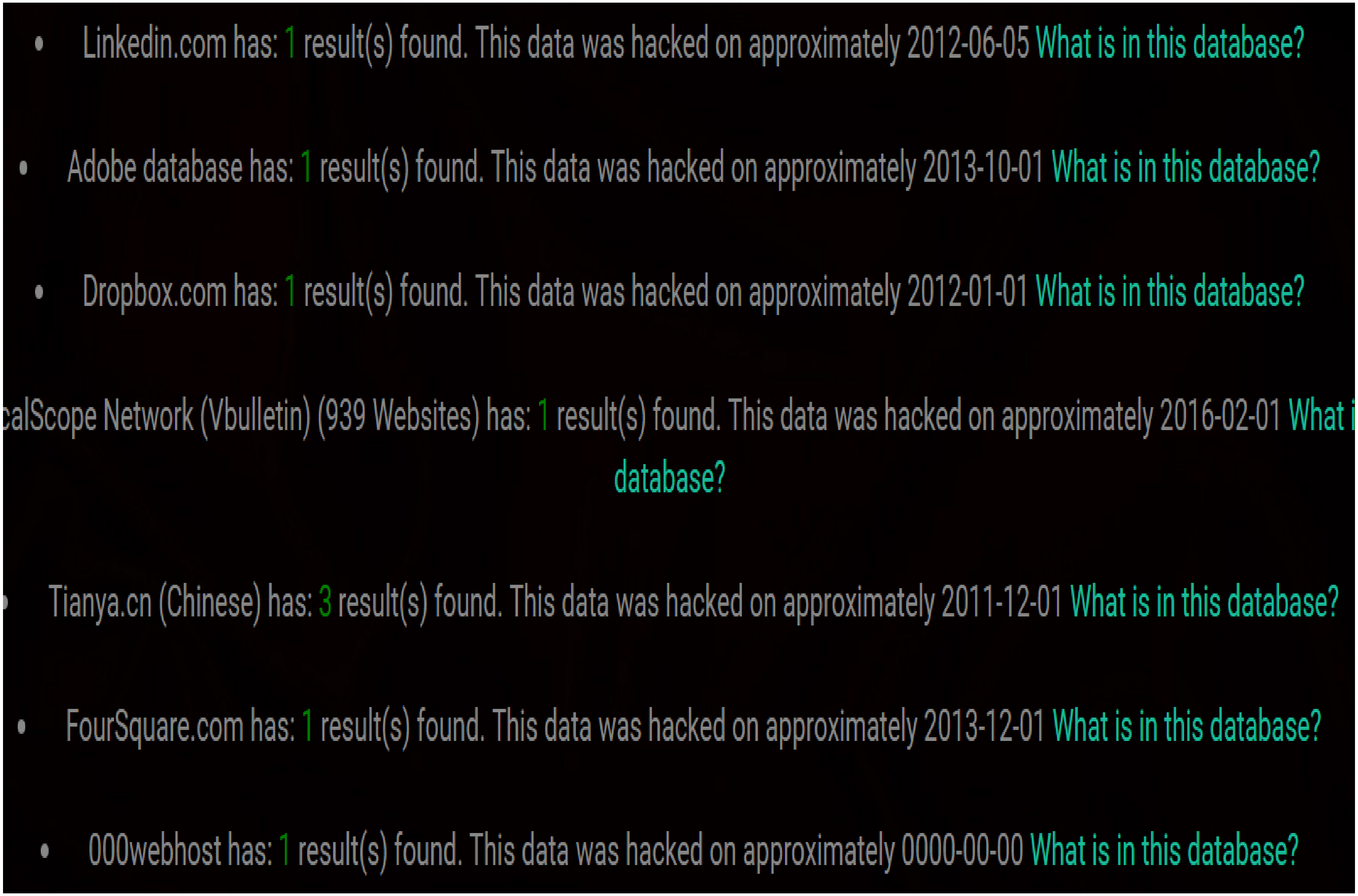
Password Management

Bad Password Behaviors

- Many people have bad password behaviors:
  - They may use a weak password
  - They are very likely to use the same password or similar passwords across multiple sites
  - They may not change their password for years
  - If one site got hacked, your passwords in other places may be in jeopardy!
    - The probability of password leaking is much higher than you expected!

Hacking your password is never easier!

- https://www.leakedsource.com/main
  - A new website established in 2016
    - You can pay $11 to view people’s passwords from old leaks.
  - This controversial site was brought down in Jan. 2017
    - But the leaked information are still there in the darkweb…
- https://haveibeenpwned.com/
  - A similar website which allows you to get leaking notifications
    - you won’t see the actual leaked passwords.



- Linkedin.com has: 1 result(s) found. This data was hacked on approximately 2012-06-05 What is in this database?
- Adobe database has: 1 result(s) found. This data was hacked on approximately 2013-10-01 What is in this database?
- Dropbox.com has: 1 result(s) found. This data was hacked on approximately 2012-01-01 What is in this database?
- calScope Network (Vbulletin) (939 Websites) has: 1 result(s) found. This data was hacked on approximately 2016-02-01 What i database?
- Tianya.cn (Chinese) has: 3 result(s) found. This data was hacked on approximately 2011-12-01 What is in this database?
- FourSquare.com has: 1 result(s) found. This data was hacked on approximately 2013-12-01 What is in this database?
- 000webhost has: 1 result(s) found. This data was hacked on approximately 0000-00-00 What is in this database?

Mark Zuckerberg Was Hacked 6/6/2016

- A hacker group called OurMine took over Mark Zuckerberg’s Twitter, Instagram and Pinterest account.
- Mark used the same password for his social media accounts.
- The hacker started with Linkedin data breach and password dump on 2012.
- The password is “dadada”.
- Video (1m)
  - https://www.youtube.com/watch?v=tzvIPrBgo0A

Practical suggestions on password

- Use a story to help you remember the password (at least 10-12 characters).
  - Kingkong@UP4Snow or panda2TX28bamb00
  - First letter of a song/poem/sentence
    - I usually buy milk from Walmart at 1400 townsend drive => IubmfW@1400td
- Avoid using the same password across multiple sites
  - You should have at least three different sets of passwords:
    - One for your job account;
    - One for important personal accounts, like bank, email…
    - One for other personal accounts.

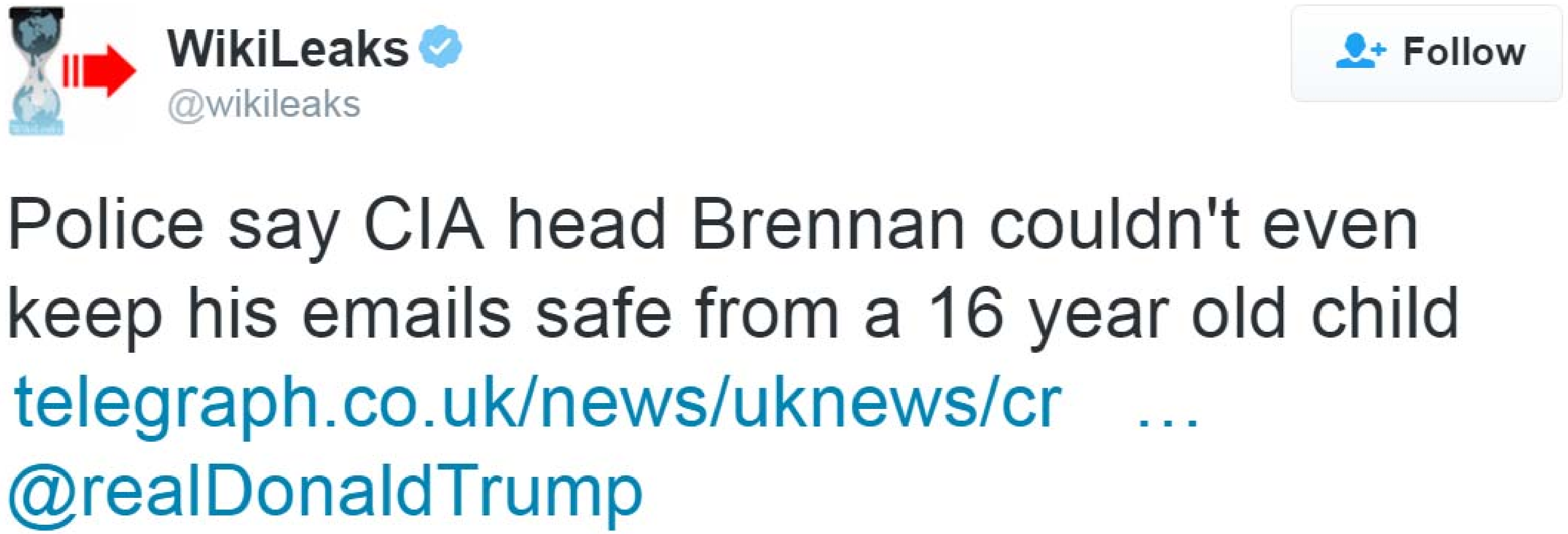
Practical suggestions on password

- We all use notes, smartphones, or something to store password.
  - Notes might not be a bad idea…
  - Password management apps is ok too…
    - Something like 1password or LastPass
    - However, should you trust these apps?
- Another important point: For security questions or password reset questions, add special characters to your answers
  - Which foreign countries have you visited?
  - Canada## instead of Canada

Sarah Palin's Email Was Hacked in 2008

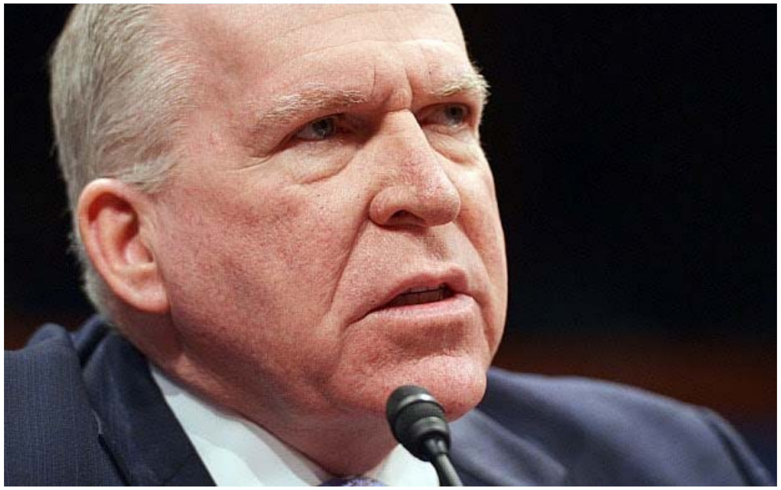
- Hackers used Yahoo!'s password recovery feature, and then proceeded to fill in the answers using Google and Wikipedia.
  - Answer the question "where did you meet your spouse?"
    - They are high school sweethearts
    - Google search for "palin eloped"
    - High school, eventually hit on "Wasilla high"

CIA boss John Brennan’s email was hacked by a British 16-year-old boy in 2016



WikiLeaks
@wikileaks

Police say CIA head Brennan couldn't even keep his emails safe from a 16 year old child telegraph.co.uk/news/uknews/cr … @realDonaldTrump



How to enable two-factor authentication (2FA)?

- Many websites did provide 2FA, but as a hidden feature which many people don’t know how to find it.
  - For example, Gmail,
  - Google “two-factor authentication in Gmail” to get help
- You can do 2FA for Amazon, Facebook, Wells Fargo Bank…..
- 2FA is a bit inconvenient sometimes…
- Some sites don’t provide 2FA.

Recap on password management

- Check if your passwords were leaked
  - https://www.leakedsource.com/main
  - https://haveibeenpwned.com/
- Change your password with stronger ones and do it today!
- Do not share password across different domains
- Make answers to security questions or password reset questions harder to guess
- Enable two-factor authentication when possible
- Turn on your human firewall

Study shows that half of the people will ignore my warning anyway!

A Report from Lab42

- 91 percent know there is a risk when reusing passwords, but 61 percent continue to do so, and 55 percent do so while fully understanding the risk.

COGNITIVE DISSONANCE is the psychological conflict resulting from an individual performing an action that is contradictory to their beliefs, ideas or values.

Source: http://prod.cdata.app.sprinklr.com/DAM/434/LastPass_ExecutiveSummary_fina-88e8a5a2-00cb-4a09-b363-e01a45f829d6-1389898992.pdf