Lecture 20 – Passwords and Authentication

Stephen Checkoway

Oberlin College

Slides based on Bailey’s ECE 422

Major Portions Courtesy Ryan Cunningham

AUTHENTICATION

Authentication Basics

- Authentication binds identity to a subject
- Two step process
  - Identification - establish identity to system
  - Verification - process verifies and binds entity and identity

PASSWORD AUTHENTICATION

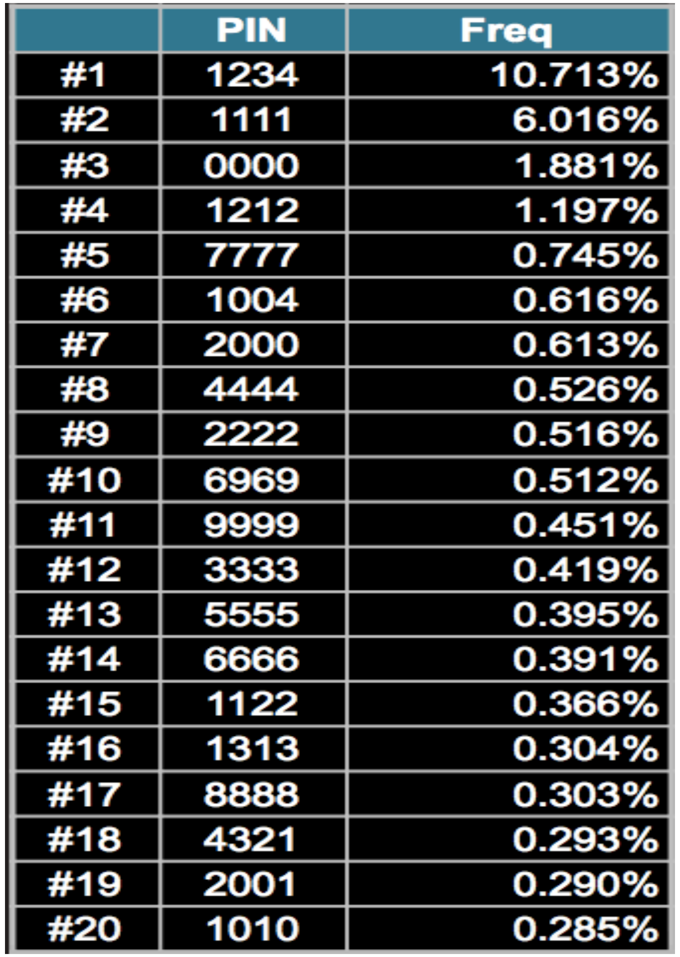
Basics

- User keeps a secret string (password)
- Something the user *knows*
- Advantages?
- Disadvantages?

Attacks

- Steal from the user
  - Install a keylogger (hardware or software)
  - Find it written down
  - Social engineering/Phishing
  - Intercept the password over network
  - Use a side channel
- Steal from the service
  - Install malware on the web server
  - Dump the password database with SQL injection
- Steal from a third party (password reuse)

Password Guessing



	PIN	Freq
#1	1234	10.713%
#2	1111	6.016%
#3	0000	1.881%
#4	1212	1.197%
#5	7777	0.745%
#6	1004	0.616%
#7	2000	0.613%
#8	4444	0.526%
#9	2222	0.516%
#10	6969	0.512%
#11	9999	0.451%
#12	3333	0.419%
#13	5555	0.395%
#14	6666	0.391%
#15	1122	0.366%
#16	1313	0.304%
#17	8888	0.303%
#18	4321	0.293%
#19	2001	0.290%
#20	1010	0.285%

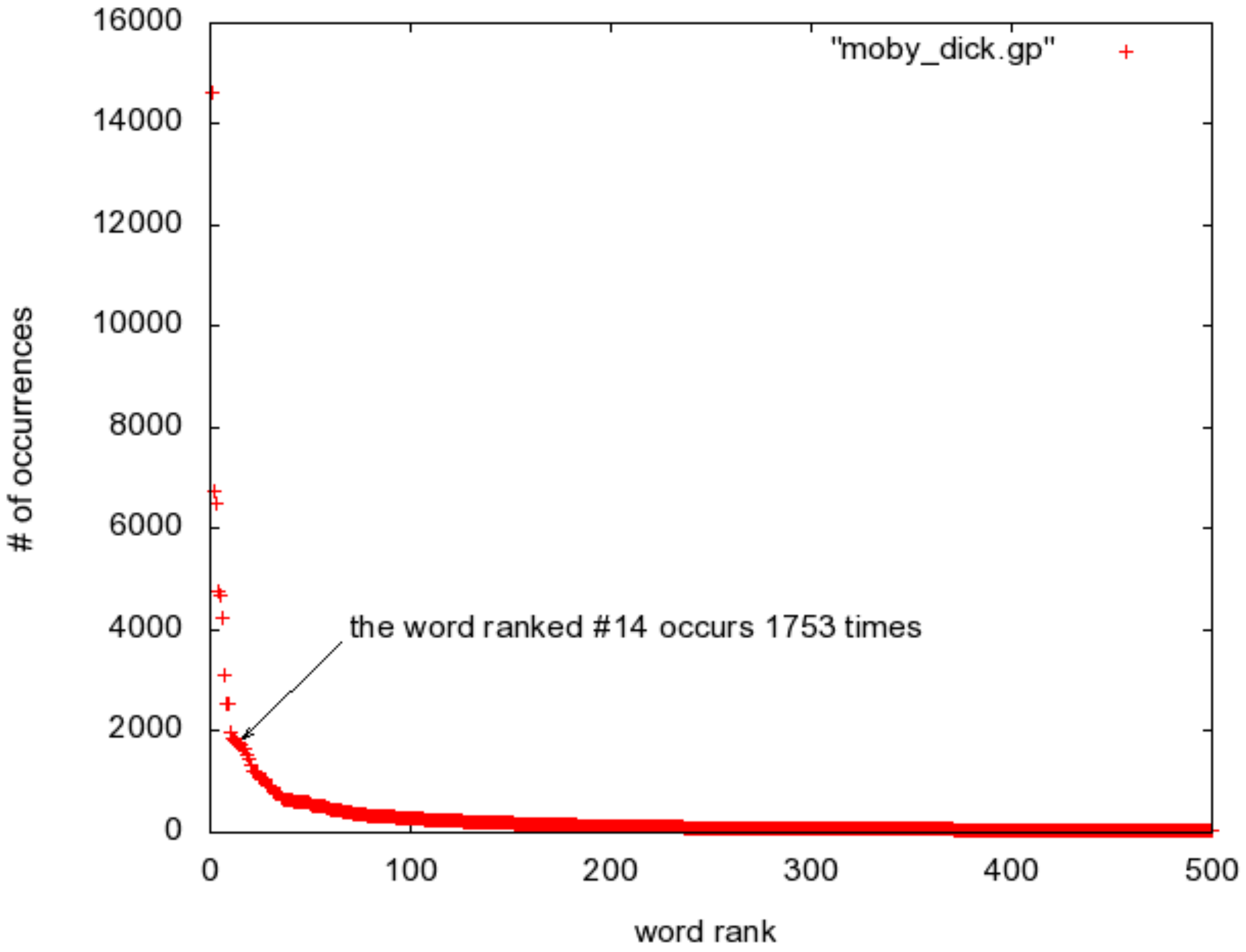
http://www.datagenetics.com/blog/september32012/

Top 20 Passwords (Mark Burnett)

1.	password,	32027
2.	123456,	25969
3.	12345678,	8667
4.	1234,	5786
5.	qwerty,	5455
6.	12345,	4523
7.	dragon,	4321
8.	pussy,	3945
9.	baseball,	3739
10.	football,	3682
11.	letmein,	3536
12.	monkey,	3487
13.	696969,	3345
14.	abc123,	3310
15.	mustang,	3289
16.	michael,	3249
17.	shadow,	3209
18.	master,	3182
19.	jennifer,	2581
20.	111111,	2570

https://xato.net/10-000-top-passwords-6d6380716fe0#.lo0geeq99

Power Law

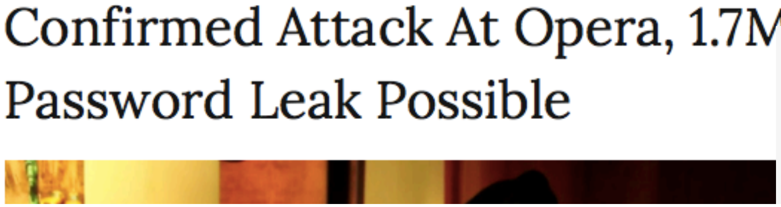


http://www.philippeadjiman.com/blog/2009/10/26/drawing-the-long-tail-of-a-zipf-law-using-gnuplot-java-and-moby-dick/

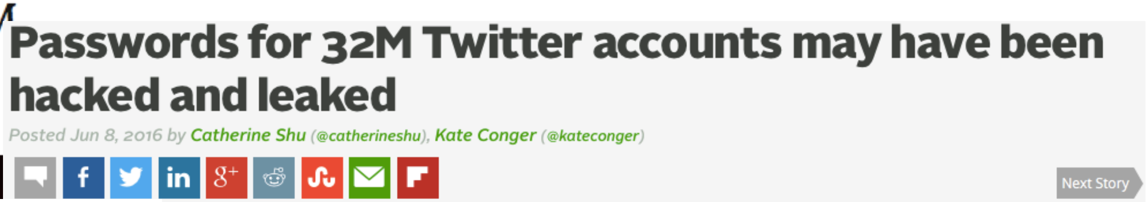
Secure Passwords

- Uneven distribution makes guessing easier
- Passwords should be uniformly distributed
  - All characters in password chosen with equal probability
- Passwords should be long
  - Longer password = larger brute force search space
- Passwords should never be reused
- Passwords chosen randomly are difficult to remember
  - Tradeoff of security vs. convenience

STORING PASSWORDS

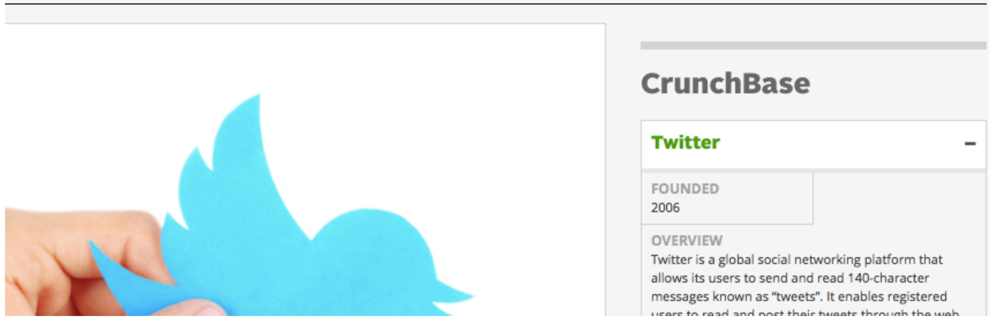


Confirmed Attack At Opera, 1.7M Password Leak Possible



Passwords for 32M Twitter accounts may have been hacked and leaked

Posted Jun 8, 2016 by Catherine Shu (@catherineshu), Kate Conger (@kateconger)

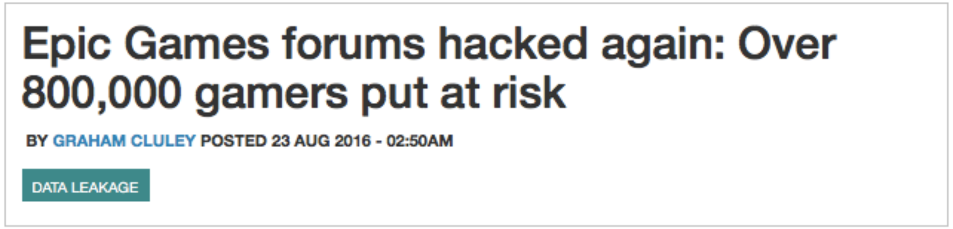


CrunchBase

Twitter –

FOUNDED
2006

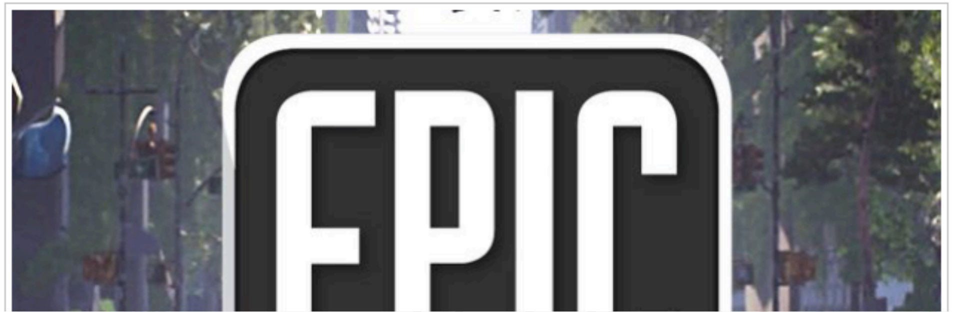
OVERVIEW
Twitter is a global social networking platform that allows its users to send and read 140-character messages known as "tweets". It enables registered users to read and post their tweets through the web

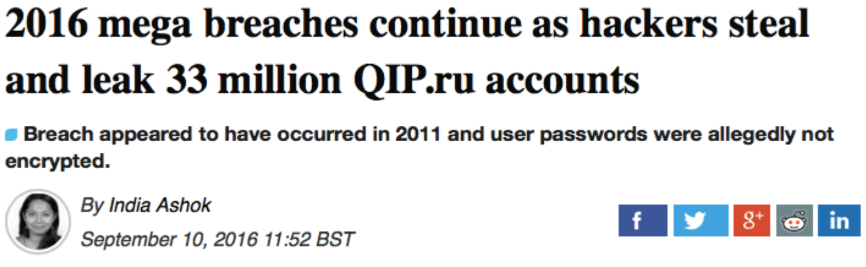


Epic Games forums hacked again: Over 800,000 gamers put at risk

BY GRAHAM CLULEY POSTED 23 AUG 2016 - 02:50AM

DATA LEAKAGE

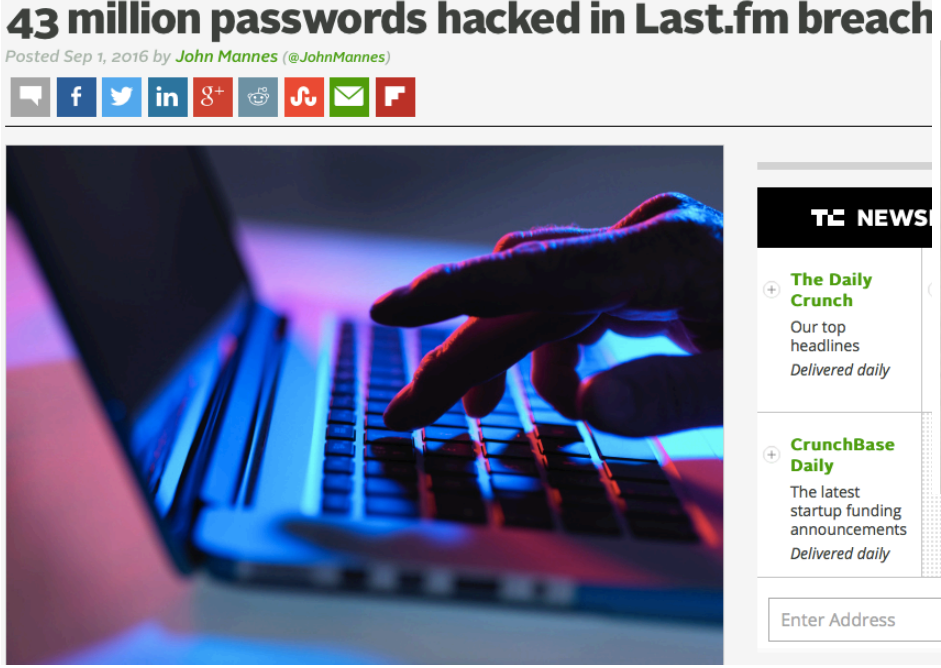




2016 mega breaches continue as hackers steal and leak 33 million QIP.ru accounts

Breach appeared to have occurred in 2011 and user passwords were allegedly not encrypted.

By India Ashok
September 10, 2016 11:52 BST



43 million passwords hacked in Last.fm breach

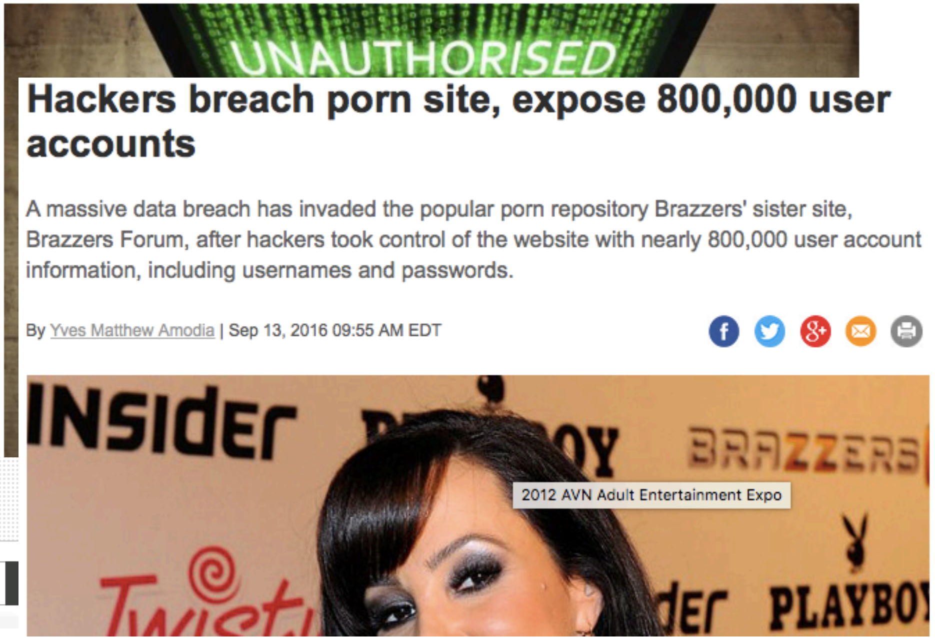
Posted Sep 1, 2016 by John Mannes (@JohnMannes)

TC NEWS

The Daily Crunch
Our top headlines
Delivered daily

CrunchBase Daily
The latest startup funding announcements
Delivered daily

Enter Address



Hackers breach porn site, expose 800,000 user accounts

A massive data breach has invaded the popular porn repository Brazzers' sister site, Brazzers Forum, after hackers took control of the website with nearly 800,000 user account information, including usernames and passwords.

By Yves Matthew Amodia | Sep 13, 2016 09:55 AM EDT

2012 AVN Adult Entertainment Expo

Storing Passwords

- Password database is highly sensitive
- We should ***never*** store *plaintext* passwords
- Store something that lets user prove they know the password

Hash functions (more later)

- Input – data of an arbitrary size
- Output – fixed length
- Same input always produces the same output
- One way function – cannot deduce input from output
- A “fingerprint” for the input
- Examples: ~~MD5~~, ~~SHA-1~~, SHA-256, SHA-512, SHA-3
  - `md5("welcome")= 40be4e59b9a2a2b5dffb918c0e86b3d7`
- ***None of these should be used directly used for password hashing***

Noncryptographic hash functions (and more)

- Cyclic redundancy checks (CRC)
  - CRC-16, CRC-32, etc.
  - Based on polynomials, many variants
- Checksums
  - sum-8, sum-16, Adler-32, Luhn algorithm, etc.
- Noncryptographic hash functions
  - FNV-1, Berstein hash (djb2), Java’s hashCode()
- ***None of these should be used used for password hashing***

Password Hashes

- We store a database of password *hashes*
- e.g., /etc/shadow on UNIX

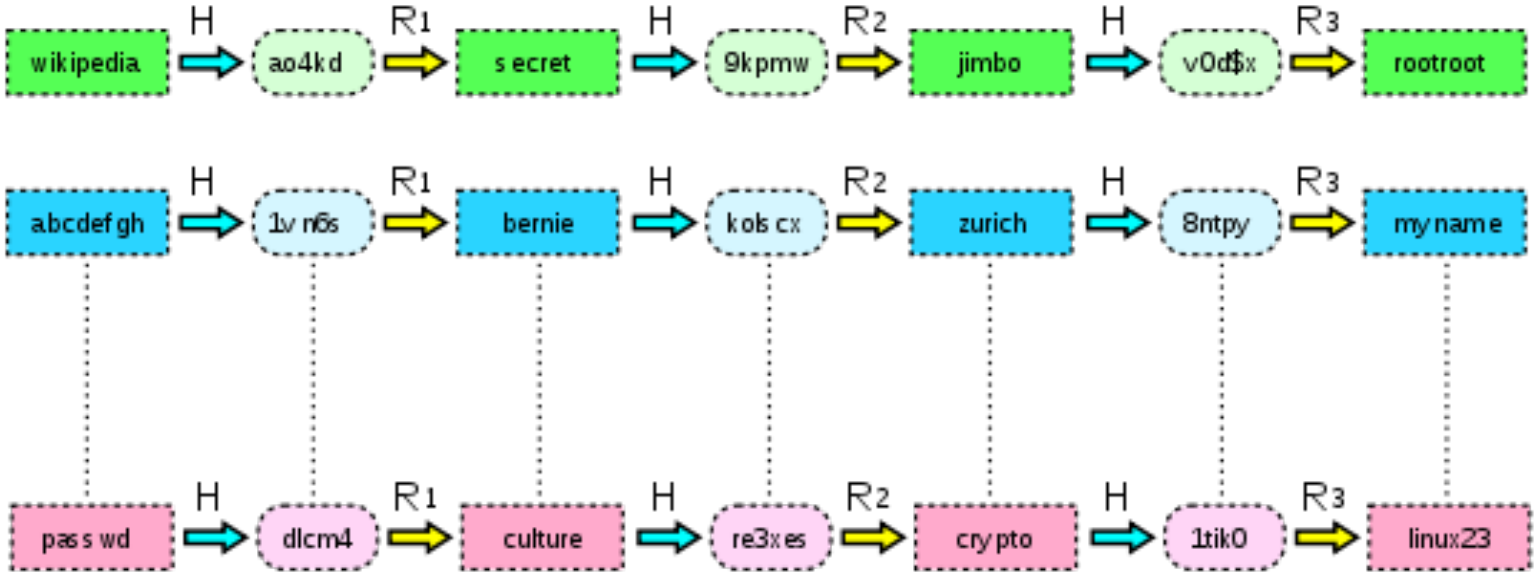
```
rcunnin2:$6$vb1tLY1qiY$M.1ZCqKtJBxBtZm1gRi8B
bkn39KU0YJW1cuMFzTRANcNKFKR4RmAQVk4rqQQCkaJT
6wXqjUkFcA/qNxLyqW.U/:15405:0:99999:7::
```

Password Cracking

- Brute force search through all possible passwords in order
- Use a dictionary
- Use a dictionary of common passwords
- Combine dictionary with common passwords and heuristics (e.g. p@$$w0rd and password123)
- Use statistical models of user passwords
- Easy to parallelize: hash password guess, compare to entire hash database
- Commonly done with arrays of GPUs

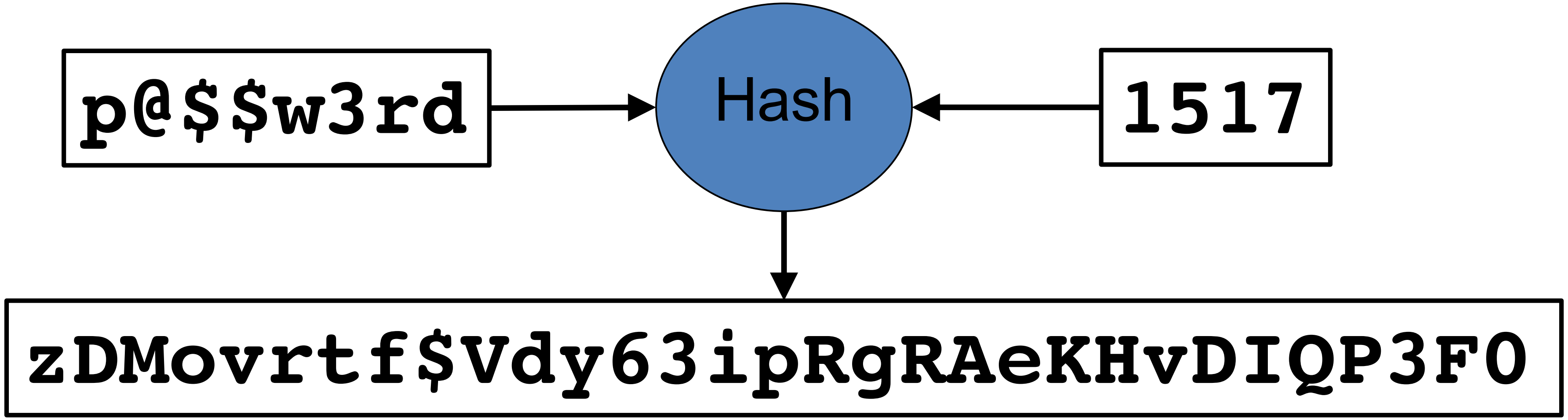
Rainbow Tables

- Many passwords are common
- Precompute them in a lookup table
- Time/space tradeoff



Salting Password Database

- Generate and store a random number, the salt for each password
- Concatenate password and salt to compute hash
- Effectively a unique hash function for each password



p@$$w3rd

Hash

1517

zDMovrtf$Vdy63ipRgRAeKHvDIQP3F0

Password Security Policies

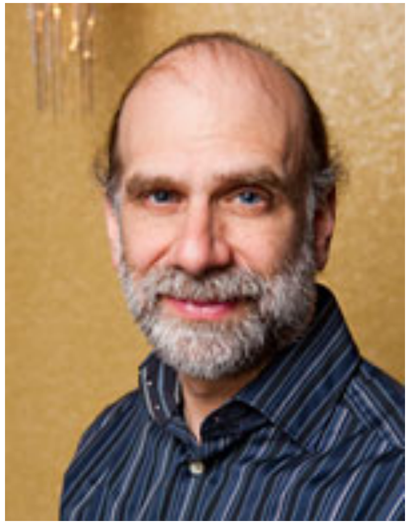
- Educate users about password security
  - Specifically train them to use good passwords
  - But they might or might not follow through
- Generate passwords randomly
  - Perfect uniform distribution
  - But not very psychologically acceptable
- Reactive password checking
  - Crack your own user’s passwords
  - But expensive and passwords vulnerable until cracked
- Complex password policy/proactive checking

Complex Password Policy/Proactive Checking

- Let the user select their own password
- Force them to follow a policy
- Reject passwords that don’t follow policy
- But…
  - Technically *reduces* number of possible passwords
  - Policy might not be psychologically acceptable
  - We don’t know if users are reusing their passwords

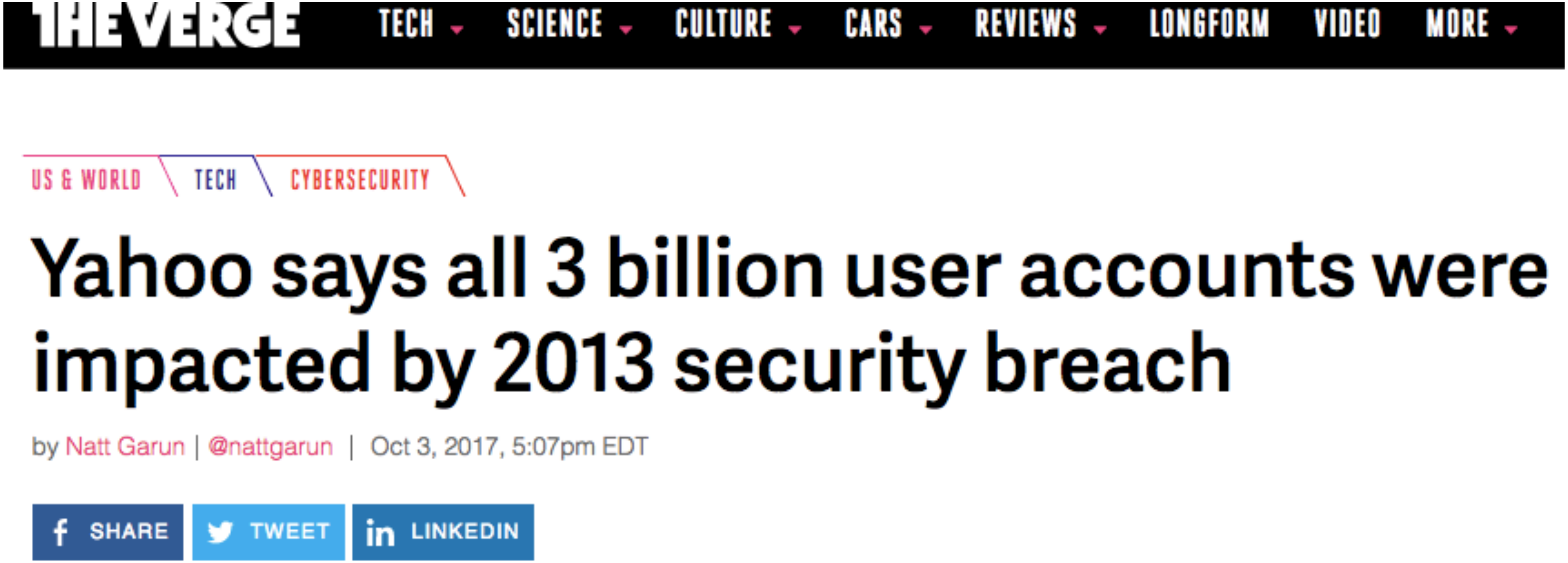
Security Questions

- Are also a shared secret
- Bruce Schneier calls them “a backup password”
- Easier to guess and social engineer
- Some cannot be changed
- Some websites have a fixed set of answers!



Breaches happen

- Databases of usernames and passwords are exposed
- https://haveibeenpwned.com/ ← Use this!



Yahoo says all 3 billion user accounts were impacted by 2013 security breach

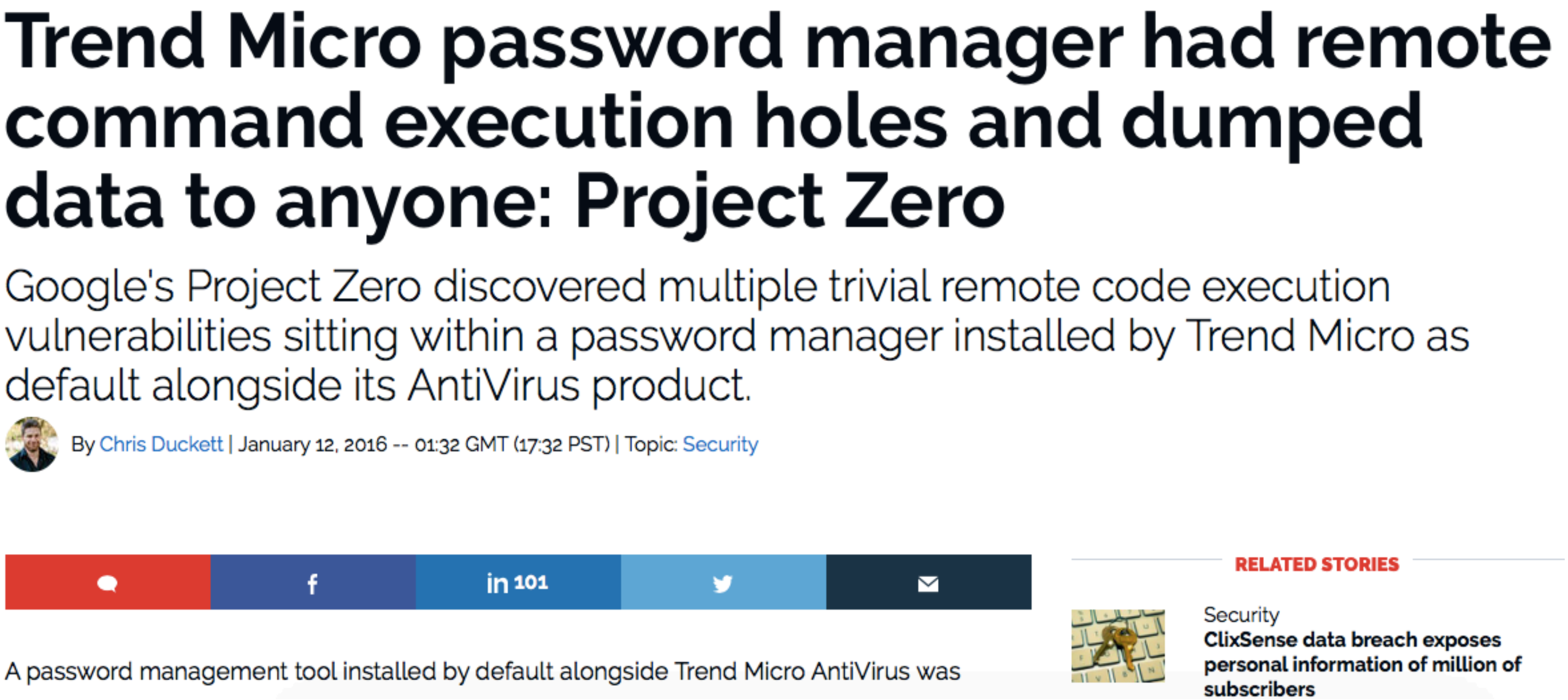
by Natt Garun | @nattgarun | Oct 3, 2017, 5:07pm EDT

RECENT PASSWORD SOLUTIONS

Password Managers

- Application that generates and maintains passwords
- Examples: Browsers, LastPass, KeePass, DashLane, 1Password
- Advantages:
  - Can handle random passwords
  - **Can create unique passwords for every website and service**
- Disadvantages
  - One point of failure
  - Requires a strong password (could be snooped)
  - Could be hacked (only as secure as the password manager)
  - Inconvenient (doesn’t work for some sites, set up time, etc.)

One Point of Failure…



Trend Micro password manager had remote command execution holes and dumped data to anyone: Project Zero

Google's Project Zero discovered multiple trivial remote code execution vulnerabilities sitting within a password manager installed by Trend Micro as default alongside its AntiVirus product.

By Chris Duckett | January 12, 2016 -- 01:32 GMT (17:32 PST) | Topic: Security

A password management tool installed by default alongside Trend Micro AntiVirus was

RELATED STORIES

Security
ClixSense data breach exposes personal information of million of subscribers

Single Sign-On (SSO)

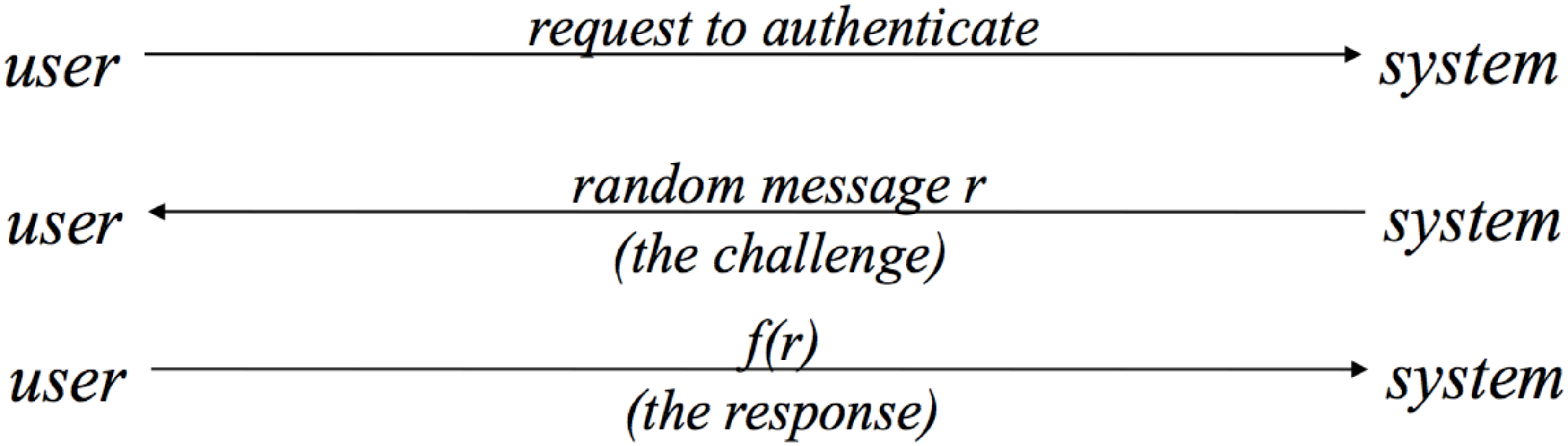
- Login to trusted 3rd party (identity provider), who vouches for user identity
- Examples: Facebook Connect, OAuth, OpenID Connect
- Pros and cons similar to Password Managers
- Third party can track users…

TOKEN-BASED AUTHENTICATION

Basics

- Something the user *has*
- Static memory cards
  - Read only
  - e.g. ATM card/Credit Card
  - Vulnerable to replay attack
- Smart card
  - Storage and computation
  - Enables challenge-response or one-time password
  - Protects against replay attack

Challenge-Response



One-time password (OTP)

- Smart card can also implement one-time password scheme
- S/Key is one such scheme
- Time-based one-time password is another (TOTP)
- Vulnerable to man-in-the-middle (MitM)

S/Key

- Server
  - Generates random seed S
  - Computes H(S), H^2(S), H^3(S), ..., H^{n+1}(S) and gives the first n of them to the client in reverse order
  - Server stores H^{n+1}(S) and discards the rest
- To authenticate
  - Client sends the first unused value P (initially P=H^n(S)) to the server
  - Server computes H(P) and compares to the stored value
  - If there’s a match, the client is authenticated and discards P; the server discards the stored value and stores P in its place

TOTP

- The current time is turned into time-counter TC
  - TC = floor((now – start_time)/time_step)
- TC and a secret key are used to create TOTP
  - TOTP = HOTP(secret_key, TC)
  - HOTP is based on a keyed-hash function
- The output is TOTP mod 10^d for d digits
- Client and server both compute the output value based on the current time and the client sends it to the server

One-time Password MitM

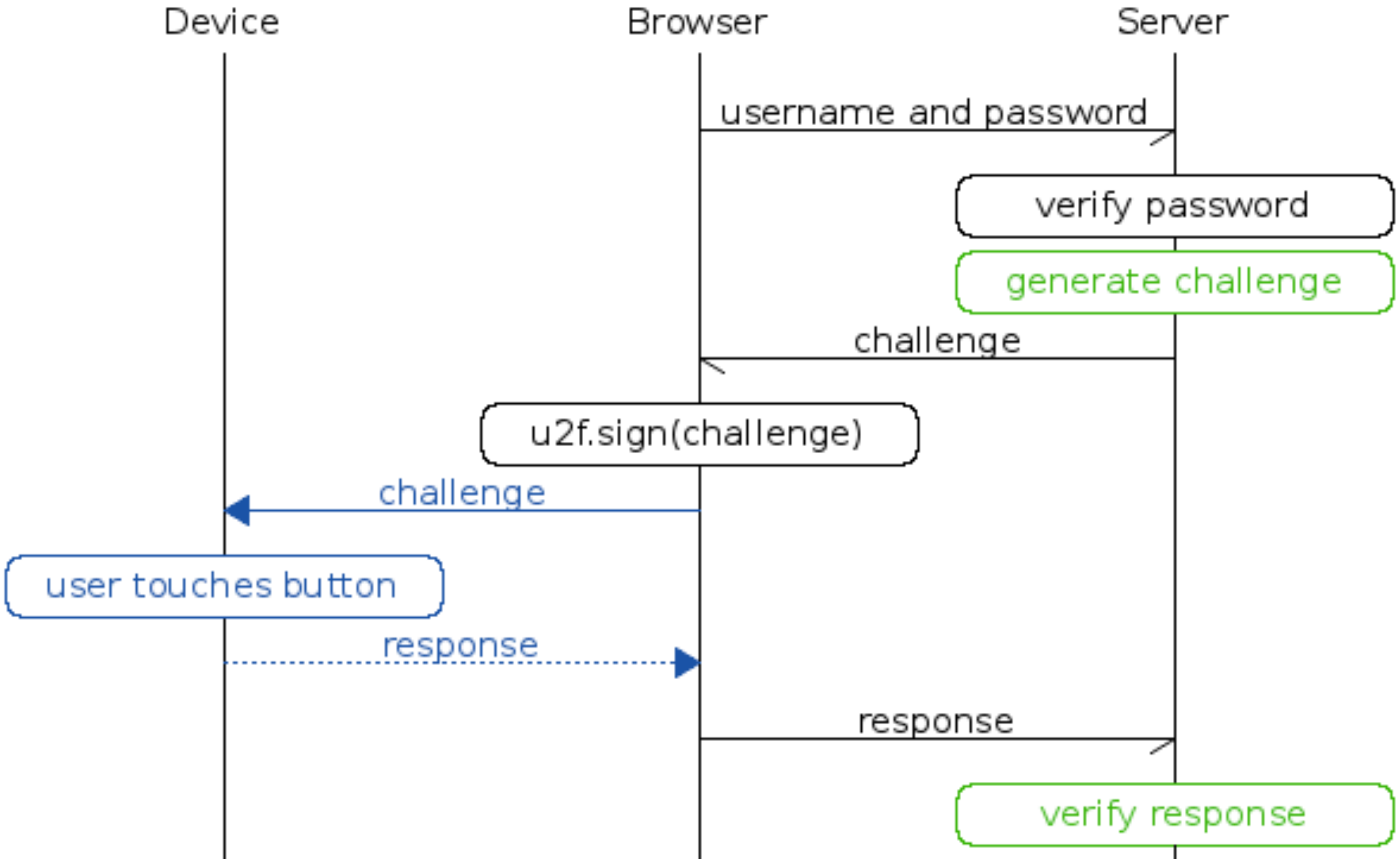
1. User sends username/password to phishing site
2. Phishing site forwards them to legitimate site
3. Legitimate site asks phisher for OTP
4. Phishing site asks user for OTP
5. User sends OTP to phisher
6. Phisher sends OTP to legitimate site

One-time Password MitM

- What’s the problem?
  - OTP not bound to the website it is sent to
  - OTP can be replayed
- What’s the solution?
  - Bind the OTP to the specific website
  - Then OTP sent to bankofthevvest.com can’t be sent to bankofthewest.com (for example)

Universal second factor (U2F)

- Addresses OTP's weakness to MitM
- Website's *origin* is cryptographically bound to the response (not displayed in the diagram)



https://developers.yubico.com/U2F/Libraries/Using_a_library.html

Disadvantages

- Token can be lost, stolen, or counterfeited
- Requires an individual physical token
- Requires an extra step (mildly inconvenient)
- Hardware can be expensive…
  - …but usually isn’t
  - $20 for U2F key from Yubico
  - Google, Facebook, and Yubico were all giving these away at a recent conference I attended

BIOMETRIC AUTHENTICATION

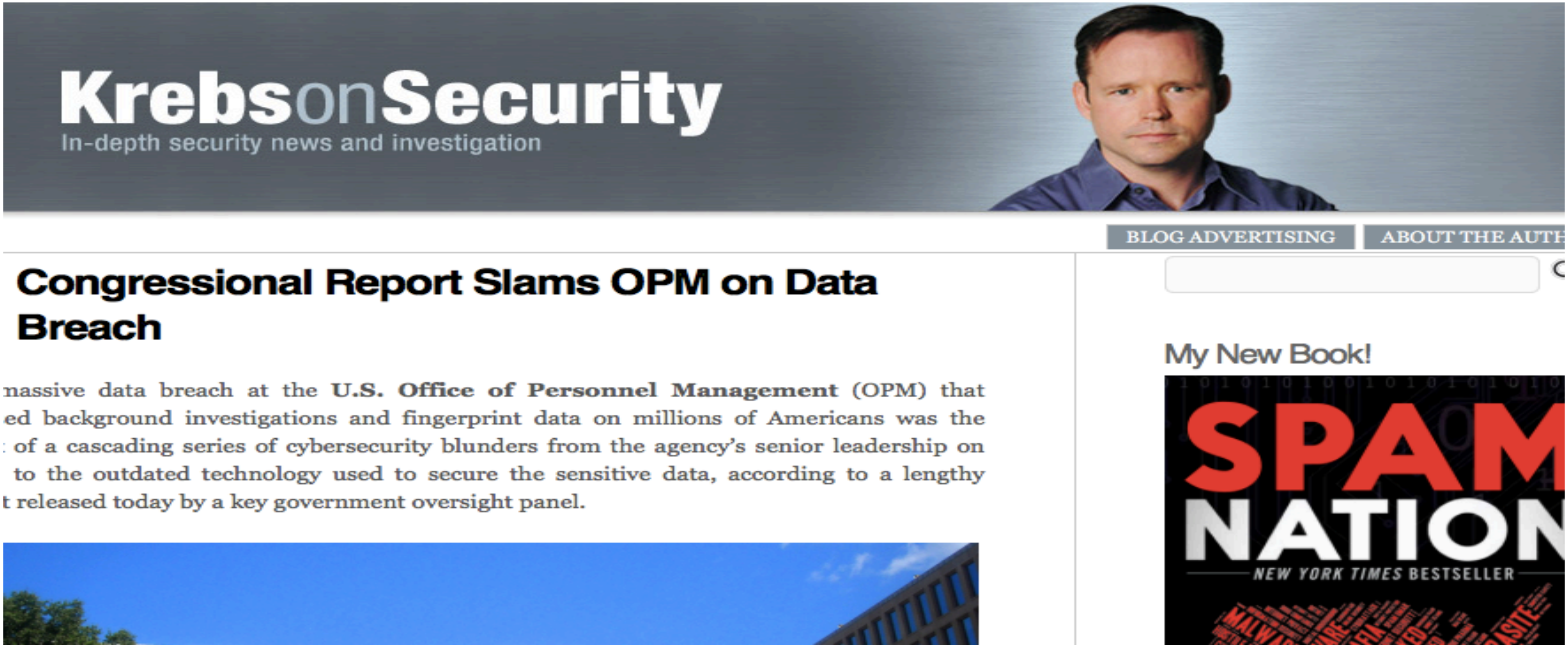
Biometrics

- Something the user *is* or *does*
- Derive a signature from biological features of user
  - Voice, fingerprint, face, retina, handwriting, gait
- Advantages?
- Disadvantages?

Disadvantages

- Imprecise measurements require *approximate* matching
  - Essentially a machine learning task
  - False negatives *and* false positives have a cost
- Measurements change over time
- Poor accessibility
- Cannot be replaced or concealed
- Replay attacks/spoofing possible
- Can be legally compelled to provide biometrics

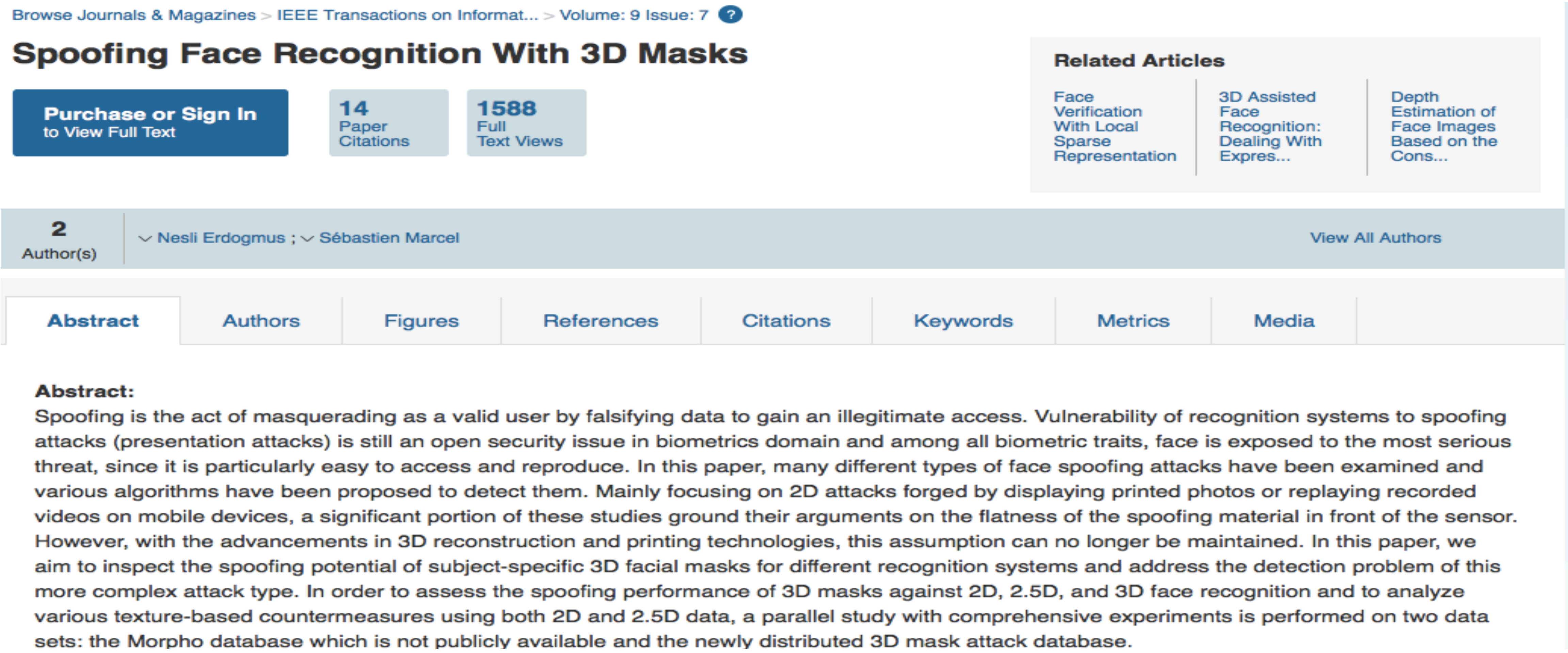
OPM Breach



Congressional Report Slams OPM on Data Breach

nassive data breach at the **U.S. Office of Personnel Management** (OPM) that ed background investigations and fingerprint data on millions of Americans was the : of a cascading series of cybersecurity blunders from the agency's senior leadership on to the outdated technology used to secure the sensitive data, according to a lengthy t released today by a key government oversight panel.

Facial Recognition



Browse Journals & Magazines > IEEE Transactions on Informat... > Volume: 9 Issue: 7
?
Purchase or Sign In to View Full Text
14 Paper Citations
1588 Full Text Views

Spoofing Face Recognition With 3D Masks

Related Articles

- Face Verification With Local Sparse Representation
- 3D Assisted Face Recognition: Dealing With Expres...
- Depth Estimation of Face Images Based on the Cons...

2 Author(s) Nesli Erdogmus ; Sébastien Marcel

View All Authors
Abstract
Authors
Figures
References
Citations
Keywords
Metrics
Media

Abstract:

Spoofing is the act of masquerading as a valid user by falsifying data to gain an illegitimate access. Vulnerability of recognition systems to spoofing attacks (presentation attacks) is still an open security issue in biometrics domain and among all biometric traits, face is exposed to the most serious threat, since it is particularly easy to access and reproduce. In this paper, many different types of face spoofing attacks have been examined and various algorithms have been proposed to detect them. Mainly focusing on 2D attacks forged by displaying printed photos or replaying recorded videos on mobile devices, a significant portion of these studies ground their arguments on the flatness of the spoofing material in front of the sensor. However, with the advancements in 3D reconstruction and printing technologies, this assumption can no longer be maintained. In this paper, we aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type. In order to assess the spoofing performance of 3D masks against 2D, 2.5D, and 3D face recognition and to analyze various texture-based countermeasures using both 2D and 2.5D data, a parallel study with comprehensive experiments is performed on two data sets: the Morpho database which is not publicly available and the newly distributed 3D mask attack database.

OTHER SCHEMES

2 Factor Authentication (2FA)

- Something you have AND something you know
- Either factor is useless without the other
- Chip and PIN
- Commonly implemented in mobile phones via SMS
  - Disadvantages:
    - ONE device (if hacked)
    - SMS is easy to redirect
    - ONE point of failure for SE (phone company)
- Google authenticator, Duo Mobile, Authy, Yubico Authenticator
- OTP tokens (e.g., TOTP), U2F keys

Multifactor Authentication

- Next level 2FA
- Combination of biometrics, knowledge, and possession

Behavior Profiling

- Track access behavior of users
  - Systems used
  - Times and locations when active
  - Typical usage
- Look for anomalous or fraudulent behavior
- “Why is this person who was in Iowa 2 minutes ago logging in from Nigeria?”
- Used in fraud prevention