UNIFACE

Security

Face to Face

November 2016

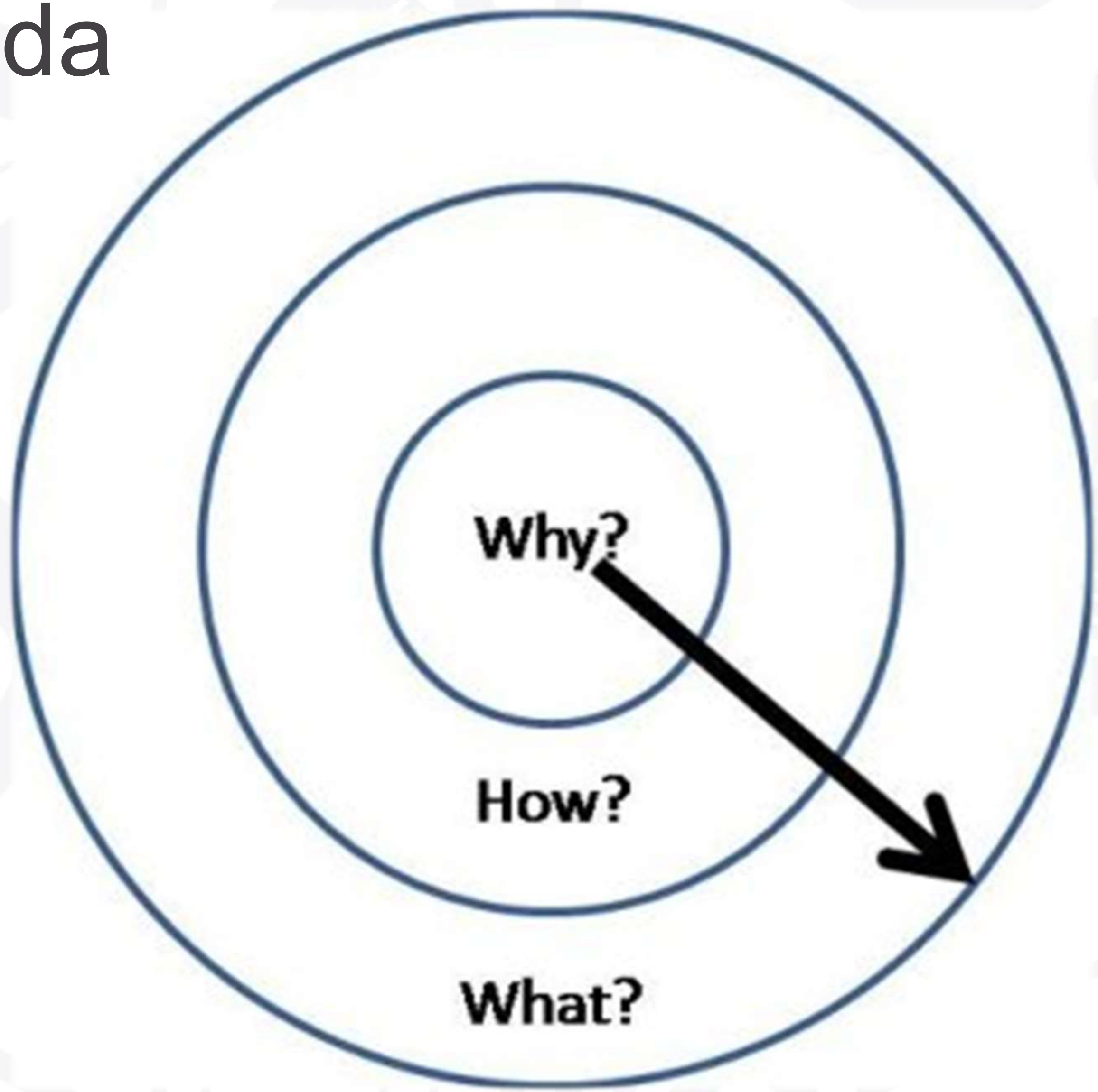
Security

Jason Huggins

Director, Global Delivery

30 November 2016

Agenda



Why?

What is this all about?

“I don’t need to worry…..”

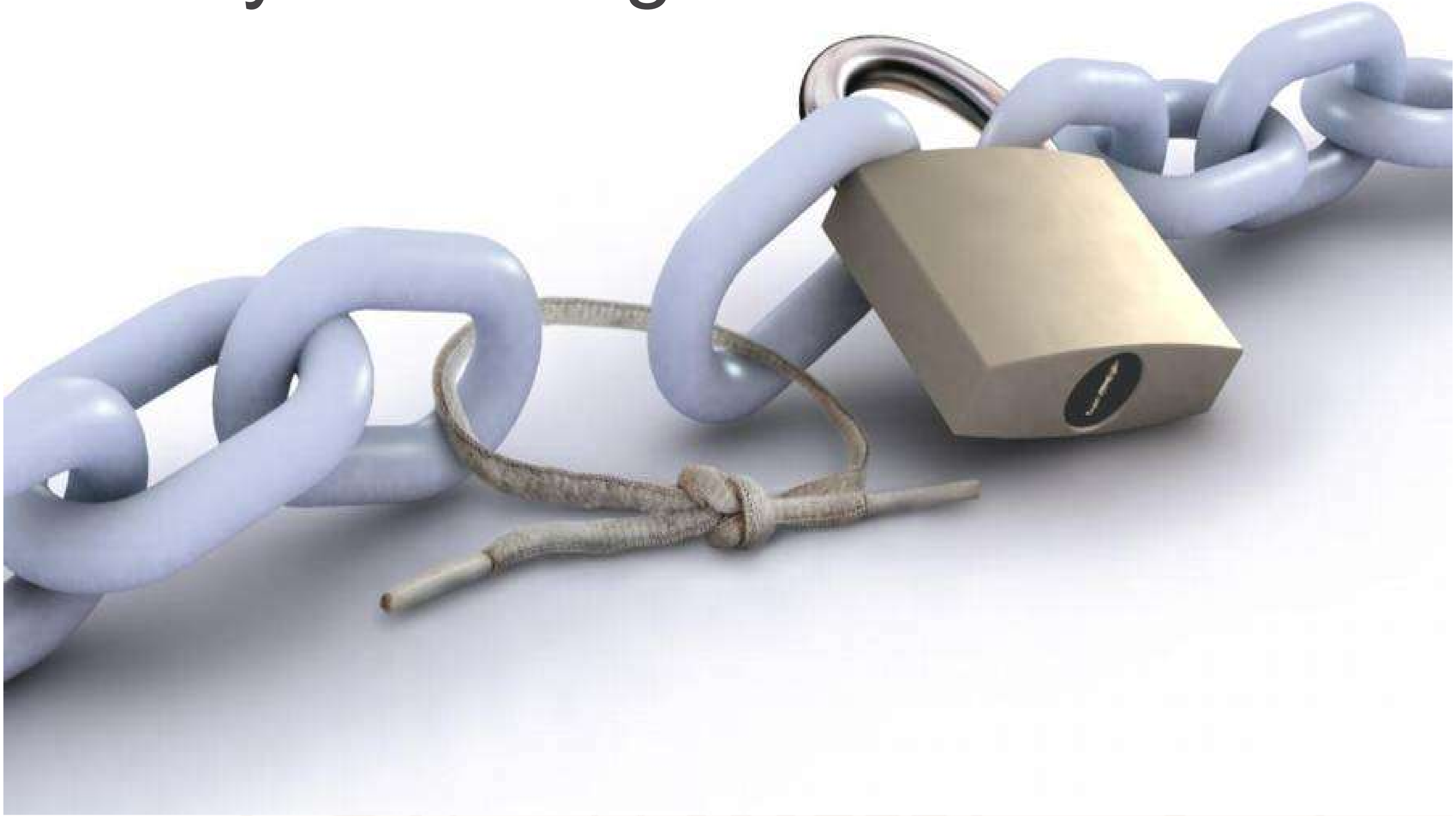
- ...it’s an internal application
- …our team would never….
- …we’ve never had a attack
- …we’re not that interesting to hackers
- …searching for Uniface hacks yields little
- …our data is public record
- …I’m not doing web, I’m okay
- …my password is strong
- …it is too complicated

WRONG!

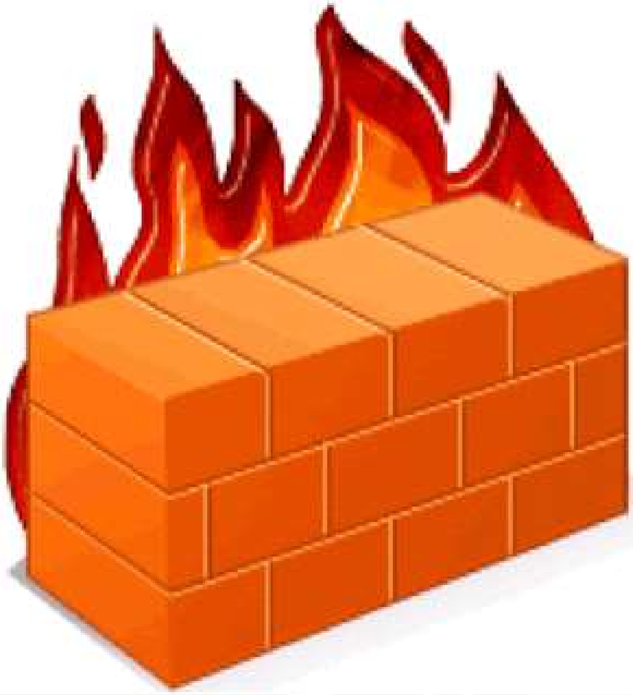
"…everyone needs to worry"

- Accidental hacker
- Cyber criminals
- Not just a privacy issue
- Increasingly connected, integrated & exposed
- Desktop, Web, Mobile, …as a Service
- Increasingly a developer role
- …

Only as strong as…



These are not the solution:



It gets us all however big or small

- Man acquires search engine domain
- Man acquires webmail provider domain
- Free pizza
- Heartbleed
- Stuxnet
- Identity theft
- Luke destroys Death Star

It can get complex

$$W(E_N) = \max_{M,u,v}|U(E_N, M, u, v)| = \max_{M,u,v}\left|\sum_{j=0}^{M-1} e_{u+jv}\right|$$

$$C_k(E_N) = \max_{M,D}|V(E_N, M, D)| = \max_{M,D}\left|\sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k}\right|$$

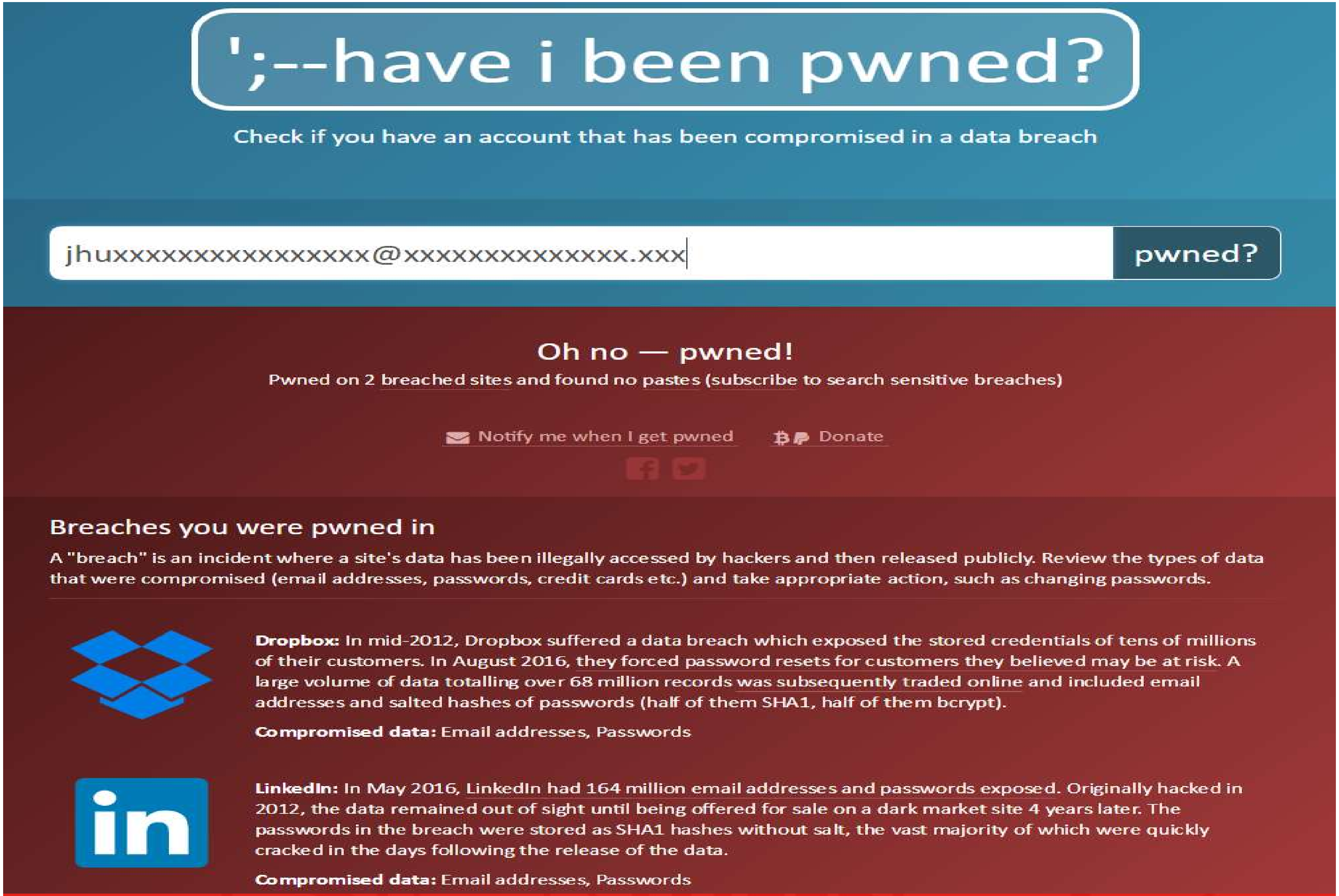
- Don’t be put off
- Call the experts too

Confidentiality
Integrity
Availability

How?

To Beat The Hacker, Understand The Hacker

Confidentiality
Is your data safe?



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

jhuxxxxxxxxxxxxxxxx@xxxxxxxxxxxxxx.xxx

Oh no — pwned!

Pwned on 2 breached sites and found no pastes (subscribe to search sensitive breaches)

Breaches you were pwned in

A "breach" is an incident where a site's data has been illegally accessed by hackers and then released publicly. Review the types of data that were compromised (email addresses, passwords, credit cards etc.) and take appropriate action, such as changing passwords.

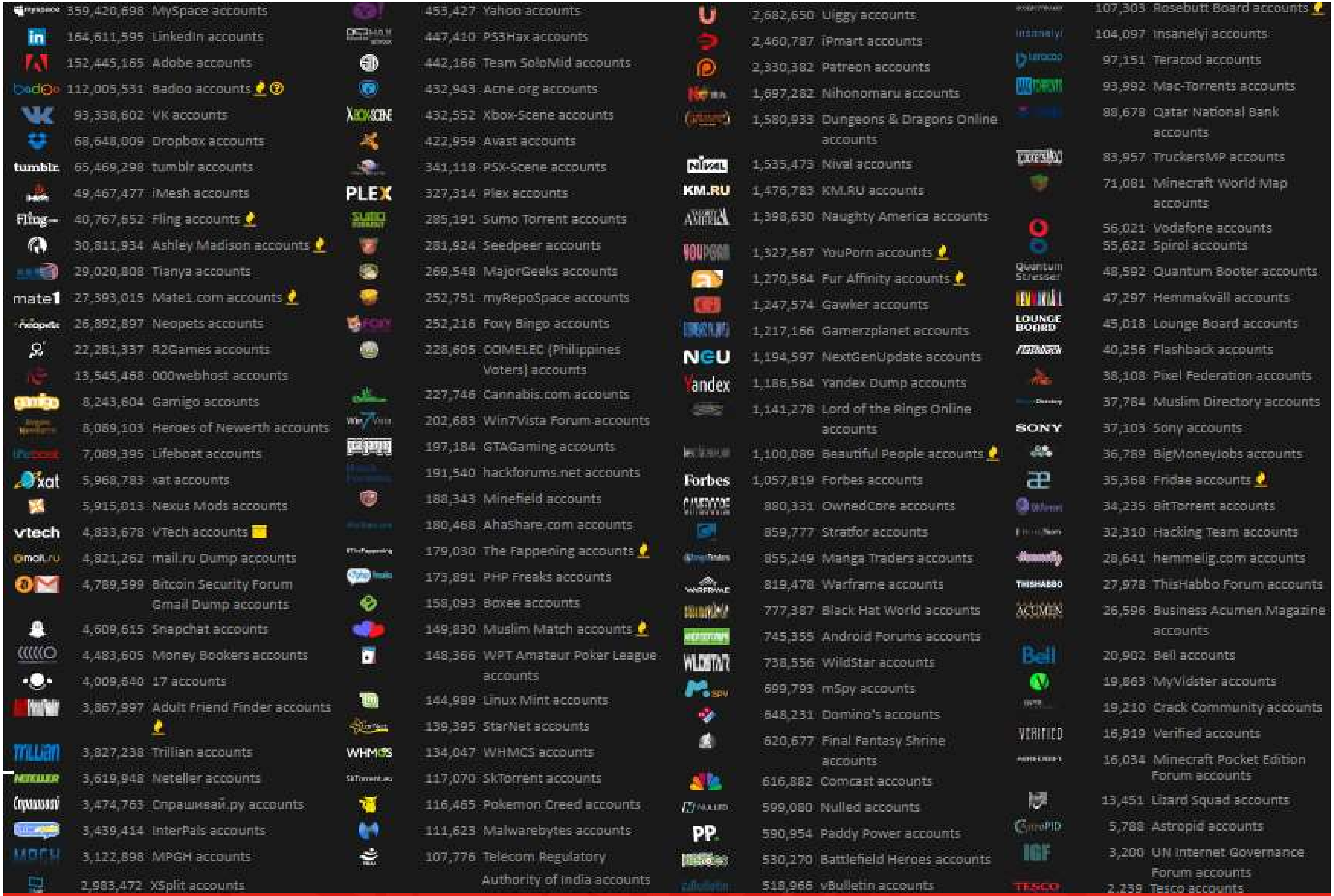
Dropbox: In mid-2012, Dropbox suffered a data breach which exposed the stored credentials of tens of millions of their customers. In August 2016, they forced password resets for customers they believed may be at risk. A large volume of data totalling over 68 million records was subsequently traded online and included email addresses and salted hashes of passwords (half of them SHA1, half of them bcrypt).

Compromised data: Email addresses, Passwords

LinkedIn: In May 2016, LinkedIn had 164 million email addresses and passwords exposed. Originally hacked in 2012, the data remained out of sight until being offered for sale on a dark market site 4 years later. The passwords in the breach were stored as SHA1 hashes without salt, the vast majority of which were quickly cracked in the days following the release of the data.

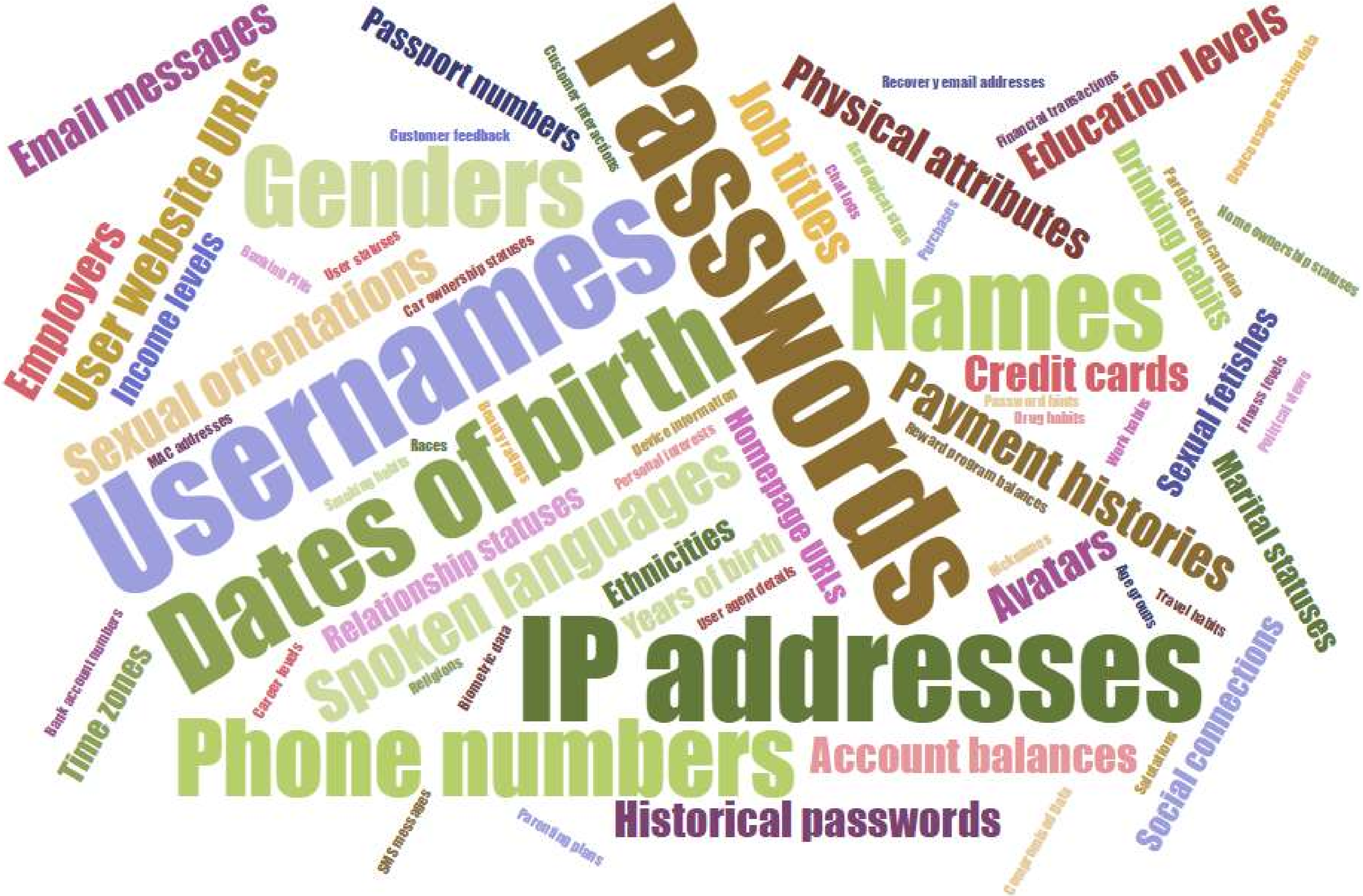
Compromised data: Email addresses, Passwords

[Ref: https://haveibeenpwned.com/]



359,420,698	MySpace accounts
164,611,595	LinkedIn accounts
152,445,165	Adobe accounts
112,005,531	Badoo accounts
93,338,602	VK accounts
68,648,009	Dropbox accounts
65,469,298	tumblr accounts
49,467,477	iMesh accounts
40,767,652	Fling accounts
30,811,934	Ashley Madison accounts
29,020,808	Tianya accounts
27,393,015	Mate1.com accounts
26,892,897	Neopets accounts
22,281,337	R2Games accounts
13,545,468	000webhost accounts
8,243,604	Gamigo accounts
8,089,103	Heroes of Newerth accounts
7,089,395	Lifeboat accounts
5,968,783	xat accounts
5,915,013	Nexus Mods accounts
4,833,678	VTech accounts
4,821,262	mail.ru Dump accounts
4,789,599	Bitcoin Security Forum Gmail Dump accounts
4,609,615	Snapchat accounts
4,483,605	Money Bookers accounts
4,009,640	17 accounts
3,867,997	Adult Friend Finder accounts
3,827,238	Trillian accounts
3,619,948	Neteller accounts
3,474,763	Спрашивай.ру accounts
3,439,414	InterPals accounts
3,122,898	MPGH accounts
2,983,472	XSplit accounts
453,427	Yahoo accounts
447,410	PS3Hax accounts
442,166	Team SoloMid accounts
432,943	Acne.org accounts
432,552	Xbox-Scene accounts
422,959	Avast accounts
341,118	PSX-Scene accounts
327,314	Plex accounts
285,191	Sumo Torrent accounts
281,924	Seedpeer accounts
269,548	MajorGeeks accounts
252,751	myRepoSpace accounts
252,216	Foxy Bingo accounts
228,605	COMELEC (Philippines Voters) accounts
227,746	Cannabis.com accounts
202,683	Win7Vista Forum accounts
197,184	GTAGaming accounts
191,540	hackforums.net accounts
188,343	Minefield accounts
180,468	AhaShare.com accounts
179,030	The Fappening accounts
173,891	PHP Freaks accounts
158,093	Boxee accounts
149,830	Muslim Match accounts
148,366	WPT Amateur Poker League accounts
144,989	Linux Mint accounts
139,395	StarNet accounts
134,047	WHMCS accounts
117,070	SkTorrent accounts
116,465	Pokemon Creed accounts
111,623	Malwarebytes accounts
107,776	Telecom Regulatory Authority of India accounts
2,682,650	Uiggy accounts
2,460,787	iPmart accounts
2,330,382	Patreon accounts
1,697,282	Nihonomaru accounts
1,580,933	Dungeons & Dragons Online accounts
1,535,473	Nival accounts
1,476,783	KM.RU accounts
1,398,630	Naughty America accounts
1,327,567	YouPorn accounts
1,270,564	Fur Affinity accounts
1,247,574	Gawker accounts
1,217,166	Gamerzplanet accounts
1,194,597	NextGenUpdate accounts
1,186,564	Yandex Dump accounts
1,141,278	Lord of the Rings Online accounts
1,100,089	Beautiful People accounts
1,057,819	Forbes accounts
880,331	OwnedCore accounts
859,777	Stratfor accounts
855,249	Manga Traders accounts
819,478	Warframe accounts
777,387	Black Hat World accounts
745,355	Android Forums accounts
738,556	WildStar accounts
699,793	mSpy accounts
648,231	Domino's accounts
620,677	Final Fantasy Shrine accounts
616,882	Comcast accounts
599,080	Nulled accounts
590,954	Paddy Power accounts
530,270	Battlefield Heroes accounts
518,966	vBulletin accounts
107,303	Rosebutt Board accounts
104,097	Insanelyi accounts
97,151	Teracod accounts
93,992	Mac-Torrents accounts
88,678	Qatar National Bank accounts
83,957	TruckersMP accounts
71,081	Minecraft World Map accounts
56,021	Vodafone accounts
55,622	Spirol accounts
48,592	Quantum Booter accounts
47,297	Hemmakväll accounts
45,018	Lounge Board accounts
40,256	Flashback accounts
38,108	Pixel Federation accounts
37,784	Muslim Directory accounts
37,103	Sony accounts
36,789	BigMoneyJobs accounts
35,368	Fridae accounts
34,235	BitTorrent accounts
32,310	Hacking Team accounts
28,641	hemmelig.com accounts
27,978	ThisHabbo Forum accounts
26,596	Business Acumen Magazine accounts
20,902	Bell accounts
19,863	MyVidster accounts
19,210	Crack Community accounts
16,919	Verified accounts
16,034	Minecraft Pocket Edition Forum accounts
13,451	Lizard Squad accounts
5,788	Astropid accounts
3,200	UN Internet Governance Forum accounts
2,239	Tesco accounts

[Ref: https://haveibeenpwned.com/]



UNIFACE

Dev Conf

Social Engineering

- Exploit our inherent trust (& fear!)
- Have you ever heard
  - Can I borrow you password?
  - Can I run a test from your PC?
  - Can I try something on your phone?
  - ~~**I'm doing a talk on security, you can trust me**~~

https://youtu.be/Ic7scxvKQOo

Social Engineer Toolkit (SET) - Security Through Education

www.**social-engineer**.org/framework/se-tools/computer.../**social-engineer-toolkit-set**/

Integrity

Do you trust the data?

Integrity

- Consistency & accuracy
- Detect changes in transit
- Malicious or accidental
  - Cyber Criminal, Spyware…
  - Accidental Hacker, Bugs….

Availability

Denial of Service

- (Distributed) Denial of Service
  - Flood, Consume, Overload
- Ransomware

What?

How does it look in practice?

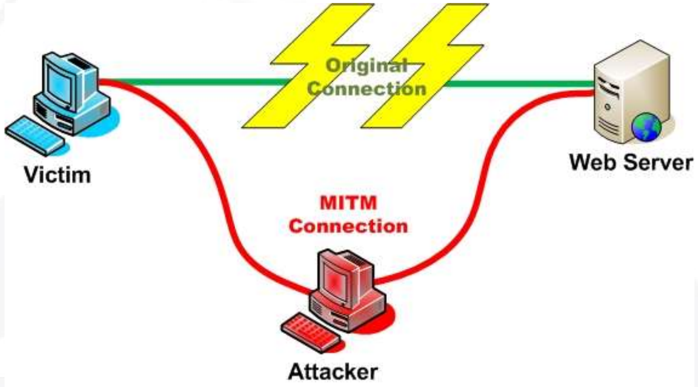
Common Threats

- Man in the Middle / Snooping
- Password Cracking
- Buffer overflows
- Interpreter Injection
  - SQL Injection
  - JavaScript Injection
  - Parameter Manipulation
- Session Hijacking

Man in the Middle / Snooping

- Privacy breach
  - Promiscuous mode
  - Spyware / Rootkits
  - Key loggers
  - Plugins
  - Proxies
- Decompilers & Debuggers
  - cavaj, mocha, ollydbg & many more

CENSORED CENSORED



Password Cracking

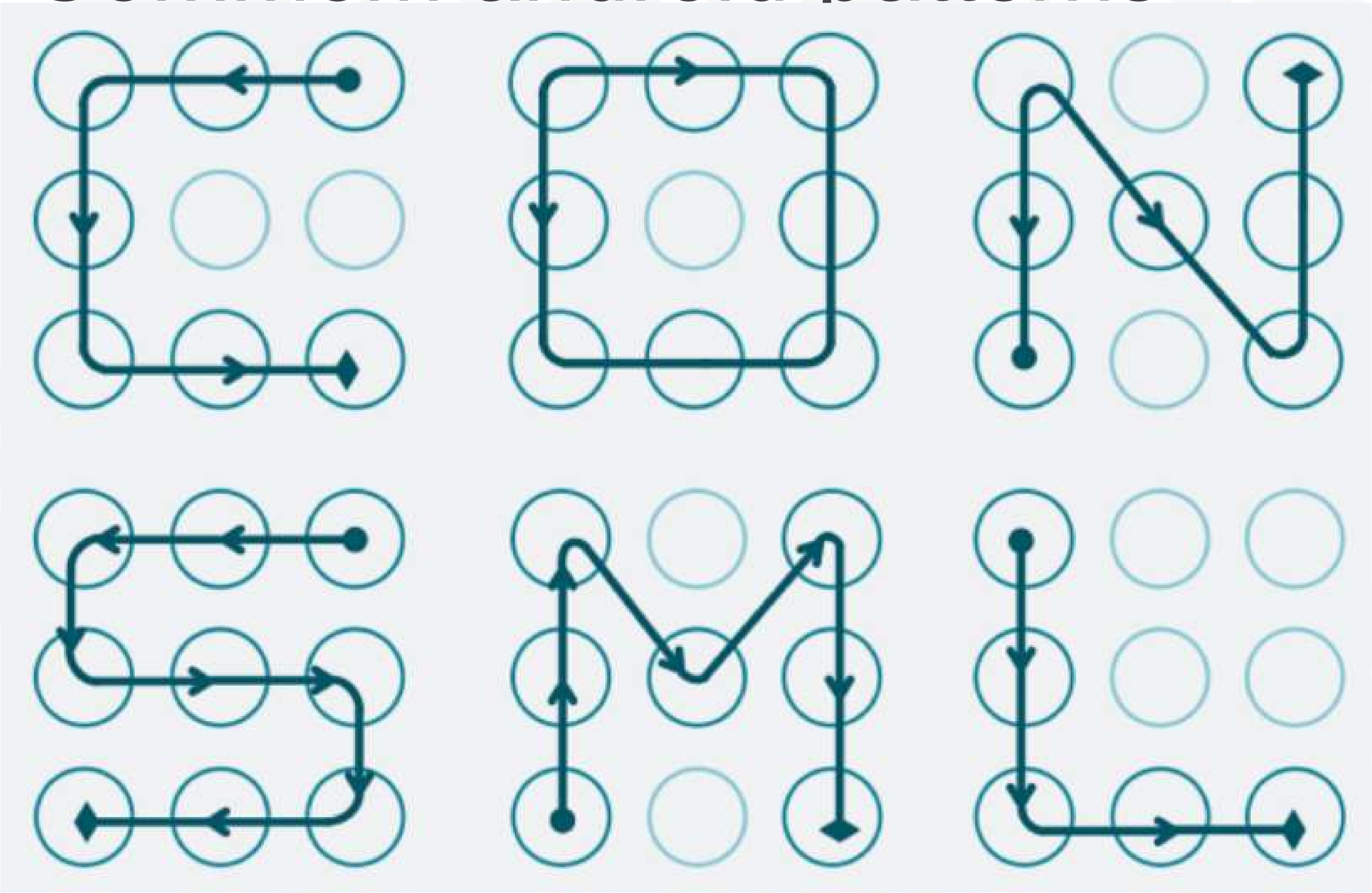
- Brute force the login page
- Brute force the database with common passwords
- Rainbow tables

```
!,MU99,#,Ms99,$,NE99,%,NU99,&,Nc99,
',Ns99,(,OE99,),OU99,*,Oc99,+,Os99,
,,HE99,-,HU99,.,Hc99,"/",Hs99,0,IE99
```

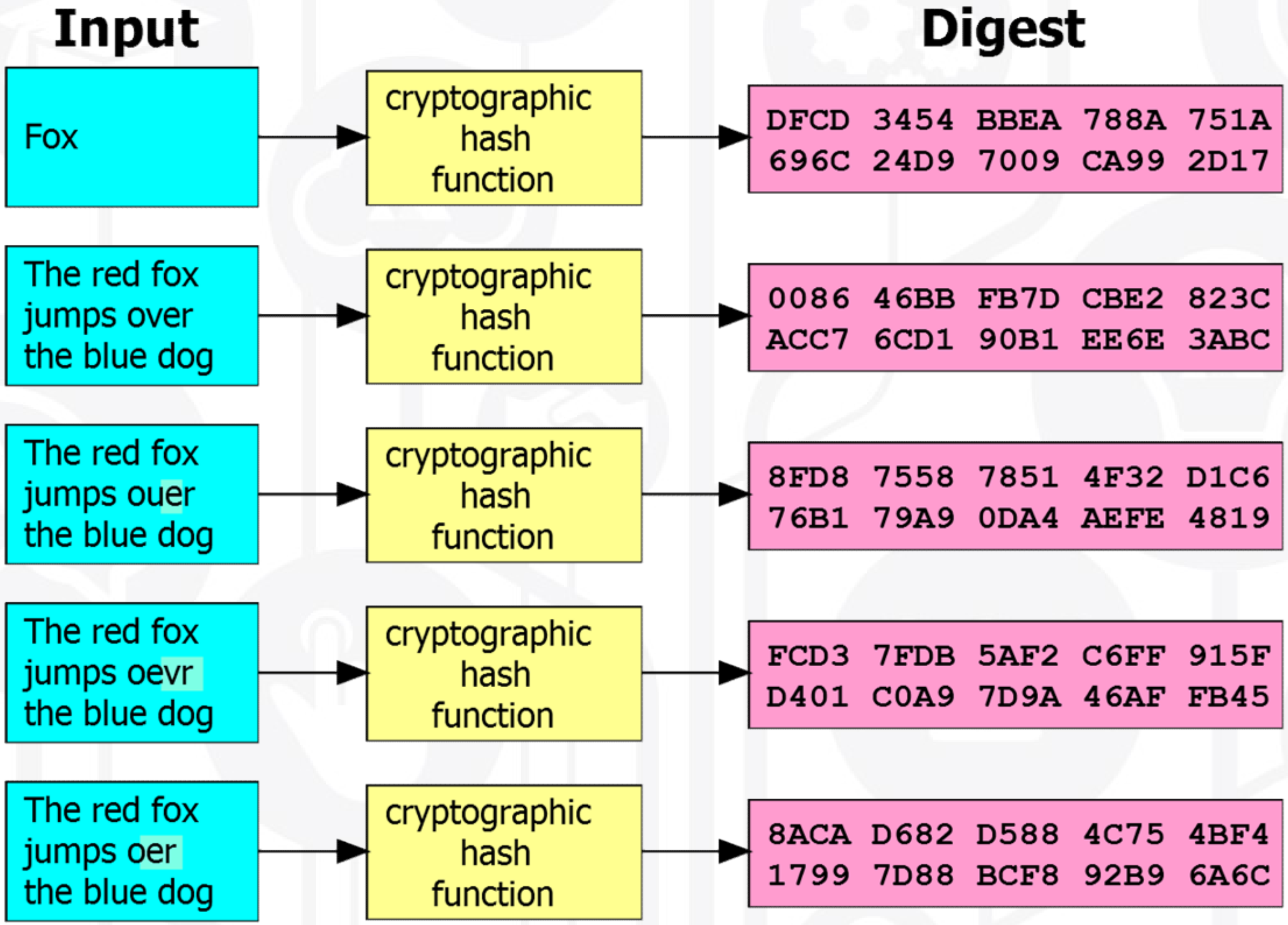
Most common passwords 2015

1. 123456
2. password
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. football
8. 1234
9. 1234567
10. baseball
11. welcome
12. 1234567890
13. abc123
14. 111111
15. 1qaz2wsx
16. dragon
17. master
18. monkey
18. monkey
19. letmein
20. login
21. princess
22. qwertyuiop
23. solo
24. passw0rd
25. starwars

Commom android patterns



Password Hashing Basics



Input

Digest

Fox → cryptographic hash function → DFCD 3454 BBEA 788A 751A 696C 24D9 7009 CA99 2D17

The red fox jumps over the blue dog → cryptographic hash function → 0086 46BB FB7D CBE2 823C ACC7 6CD1 90B1 EE6E 3ABC

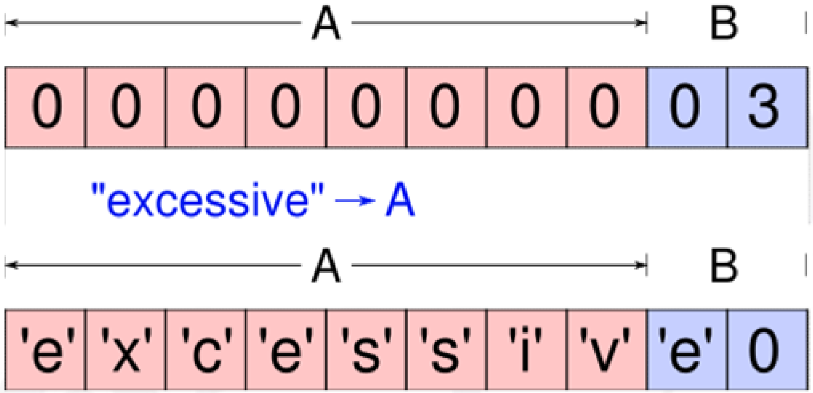
The red fox jumps ouer the blue dog → cryptographic hash function → 8FD8 7558 7851 4F32 D1C6 76B1 79A9 0DA4 AEFE 4819

The red fox jumps oevr the blue dog → cryptographic hash function → FCD3 7FDB 5AF2 C6FF 915F D401 C0A9 7D9A 46AF FB45

The red fox jumps oer the blue dog → cryptographic hash function → 8ACA D682 D588 4C75 4BF4 1799 7D88 BCF8 92B9 6A6C

Buffer overflows

- Ancient but ever present
- Accesses memory & instructions
- Alters execution path
- Inject instructions



A								B	
0	0	0	0	0	0	0	0	0	3

"excessive" → A

A								B	
'e'	'x'	'c'	'e'	's'	's'	'i'	'v'	'e'	0

Interpreter injection

- Cross site scripting
- SQL Injection
- JavaScript injection
- Parameter Manipulation

A problem wherever data forms part of the interpreted statement

Session Hijacking

These attacks include techniques like:

- Session Fixation
- Session Sidejacking
- Physical Access

Uniface

Put in context

Uniface inherent security

- Database drivers prevent SQL injection
- Widgets correctly escape HTML
- Model definitions used for validation
- Read-only field handling
- Public web / Public trigger
- Standard triggers
- Path Scrambler

Uniface counter measures

- $webinfo(“SESSIONCOMMANDS”)
- $webinfo(“WEBSERVERCONTEXT”)
- HTTPS only cookies by default
- $encode/$decode
- LDAP driver
- Read Only Fields
- sleep

Uniface – always keep in mind

- Path Scrambler
- SQL statement and where
- RAW HTML
- $webinfo
- WRD error page
- Hitlist, profiles, table scan

Summary

- Security needs to be designed in
- How safe are external parties - Weakest link
- DTA – Don’t Trust Anyone
- Conduct professional security audits
- Verify/Sanitize user input
- Enforce standards, use the model, use templates.
- Coach, train, mentor team

LET'S RECAP...

Thank You!

Questions?

uniface.com