Information Security Training

Confidentiality, Integrity, and Availability
DDoS
Password Control

2018-05-21 - ThaiNOG

APNIC

Threats and Countermeasures

- What is the CIA triangle / triad?
  - **Confidentiality** – preventing unauthorized people or processes from accessing the data
  - **Integrity** - maintaining and assuring the accuracy and completeness of data. Data cannot be modified in an unauthorized or undetected manner.
  - **Availability** – ensuring information is available when needed, within expected bounds*
    - Example: it is expected that tape backups will be slow to recover data

Threats and Countermeasures

- What is the CIA triangle / triad?
  - **Non-repudiation** – a small extension of the “CIA triad”
  - the prevention of either the sender or receiver from denying that the message was sent or received.

Threats and Countermeasures

- What are common attacks against CIA?
  - Confidentiality is attacked through breaking layers of protection to disclose information intended to be kept private.
    - A server may be compromised to extract the database of personal information.
    - Example: Ashley Madison is a cheating/dating site that had its customer information very publicly exposed
    - Sometimes the goal is password databases that can be decrypted and exposed (see: haveibeenpwned.com)

Threats and Countermeasures

- What are common attacks against CIA?
  - Integrity is attacked through modifying information, or modifying the pointers to point to different information.
    - A common example here is web site defacements, where the primary motivation for the attacker is to change the homepage of a web site
(see: www.zone-h.org/archive)

Threats and Countermeasures

- What are common attacks against CIA?
  - Availability is attacked through taking the system or service offline.

    Denial of Service (DoS) attacks typically target vulnerabilities in the application or operating system with small specially crafted packets.

    Distributed Denial of Services (DDoS) attacks can be done in many ways:
    - The network can be made unavailable by flooding the upstream connections with an excessive volume of data to fill the limited bandwidth. Attackers may also send an excessive number of small packets in order to fill up the router’s connection tables.

Threats and Countermeasures

- The server operating system can be made unavailable in the same way as the network attacks mentioned previously (exhausting bandwidth or connection tables), and is common for single servers that have less bandwidth than the upstream connections.
- Some attacks are the traditional Denial of Service (without being distributed) that involve sending specially crafted packets that exploit a vulnerability in the operating system causing the server to crash or reboot.

Threats and Countermeasures

- Server software can be made unavailable through exhausting the server resources (CPU, RAM, connection tables) through sending either legitimate or forged excessive connections, or through sending specially crafted packets to exploit vulnerabilities in the server software, or even through deleting (or ransomware encrypting) data.

– Through all of the previous DDoS scenarios, we are assuming a remote attacker. Other scenarios involve malicious insiders, accidents, and forces of nature.

- Discuss: Does anyone have any good outage stories?

Threats and Countermeasures

- What are common defences for CIA?
  - Confidentiality
    - Access control, encryption
  - Integrity
    - Hashing, encryption, digital signatures
  - Availability
    - Redundancy, high-availability, patching, increasing resources, backups, disaster recovery and business continuity plans (DR / BCP)

Information Security Training

DDoS

APNIC

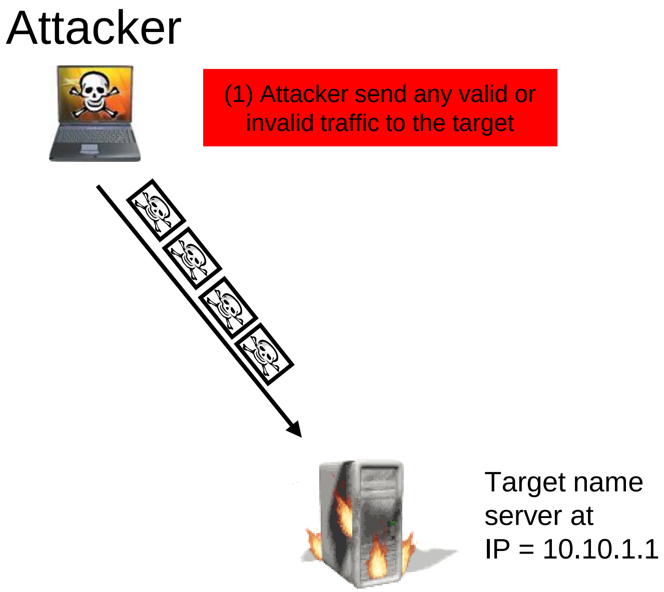
What is DoS and DDoS?

- In general, a denial of service is an attack against availability of a service
  - A service can be a network, or a specific service such as a web site
- DoS - Denial of Service
  - Usually from only one source
- DDoS - Distributed Denial of Service
  - Attack originates from multiple sources
  - This is caused through resource exhaustion

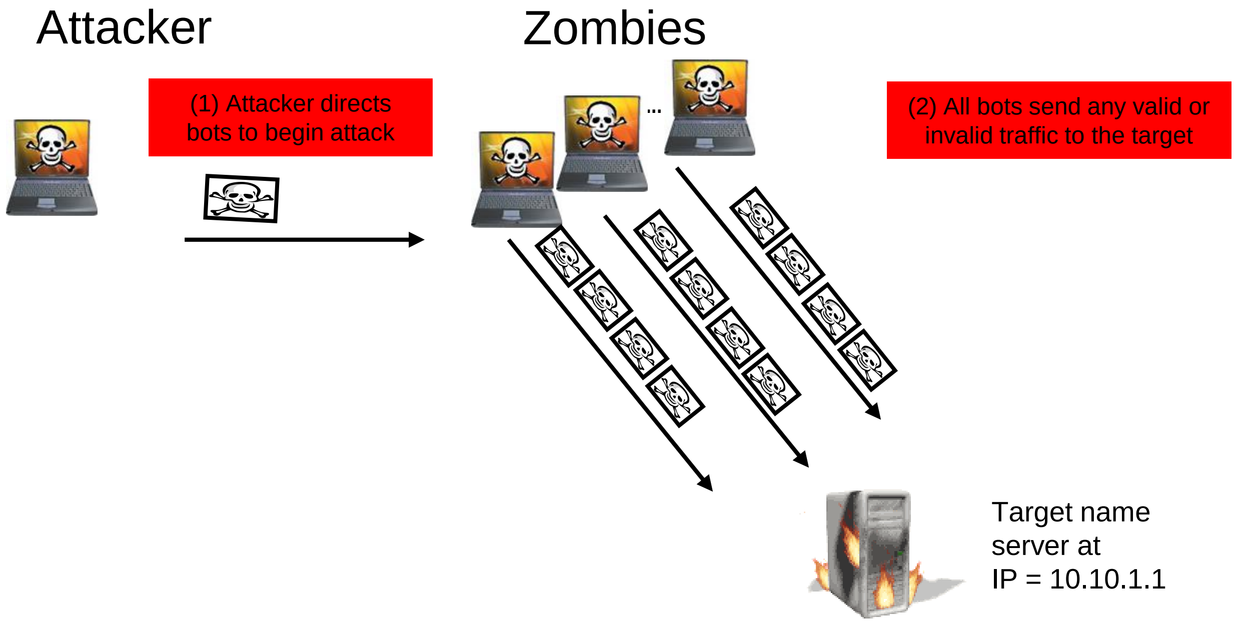
Impacts of a DDoS

- Users sees DDoS as an outage
- Security team sees DDoS as a loss of availability
  - Think back to CIA triad
- Business management, sees DDoS as impacting the business financially
  - Especially if the business makes money using the Internet
    - ISP, credit card gateway, online casino

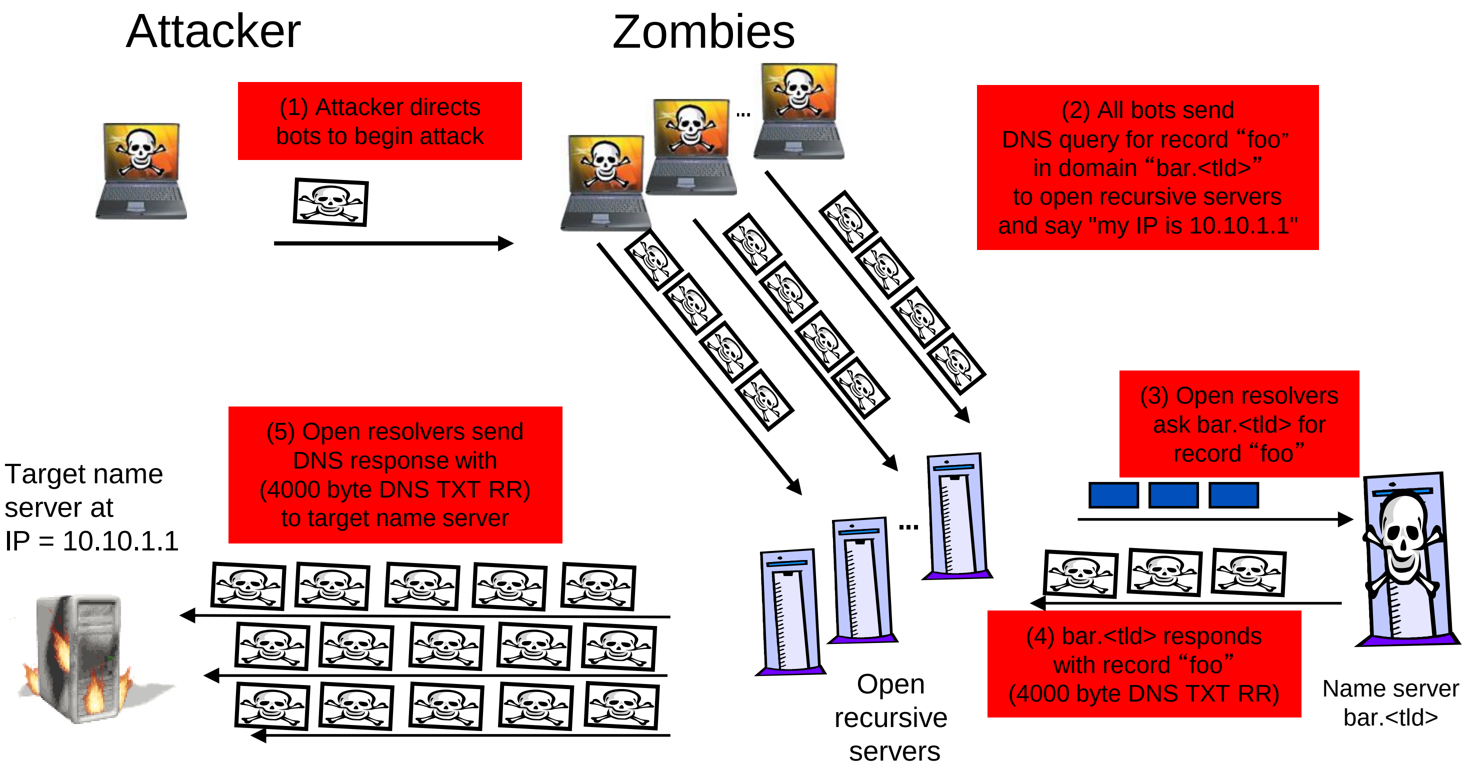
Anatomy of a Plain DoS Attack



Anatomy of a Plain DDoS Attack



Anatomy of a Reflected Amplification Attack



DDoS by Layers

OSI Model	TCP/IP Model	Protocols and Services	Attacks
Application	Application	HTTP, FTP, DHCP, NTP, TFTP, DNS	Reflection and Amplification (DNS, NTP, etc), Slowloris, Complex DB Queries
Presentation			
Session			
Transport	Transport	TCP, UDP	SYN Flood
Network	Network	IP, ICMP, RIP	ICMP Flood
Data Link	Network Interface	WiFi, Ethernet, Fiber, Copper	Electrical Interference Construction Equipment
Physical			

Reflection and Amplification

- What makes for good reflection?
  - UDP
    - Spoofable / forged source IP addresses
    - Connectionless (no 3-way handshake)
- What makes for good amplification?
  - Small command results in a larger reply
    - This creates a Bandwidth Amplification Factor (BAF)
    - Reply Length / Request Length = BAF
      - Example: 3223 bytes / 64 bytes = BAF of 50.4
    - Chart on next slide created with data from https://www.us-cert.gov/ncas/alerts/TA14-017A

Amplification Factors

Protocol	Bandwidth Amplification Factor
Multicast DNS (mDNS)	2-10
BitTorrent	3.8
NetBIOS	3.8
Steam Protocol	5.5
SNMPv2	6.3
Portmap (RPCbind)	7 to 28
DNS	28 to 54
SSDP	30.8

Protocol	Bandwidth Amplification Factor
LDAP	46 to 55
TFTP	60
Quake Network Protocol	63.9
RIPv1	131.24
QOTD	140.3
CHARGEN	358.8
NTP	556.9
Memcached	10,000 to 51,000

DNS Amplification Example

Protocol	Length	Info
DNS	80	Standard query 0x0001 PTR 8.8.8.8.in-addr.arpa
DNS	372	Standard query response 0x0001 PTR 8.8.8.8.in-addr.arpa PTR google-public-dns…
DNS	73	Standard query 0x0002 ANY microsoft.com
DNS	539	Standard query response 0x0002 ANY microsoft.com TXT TXT TXT TXT TXT TXT

```
> dig ANY microsoft.com @8.8.8.8
microsoft.com.  21599   IN   NS   ns1.msft.net.
microsoft.com.  3599 IN      SOA ns1.msft.net. msnhst.microsoft.com. 2018052001 7200 600 2419200 3600
microsoft.com.  3599 IN      MX   10 microsoft-com.mail.protection.outlook.com.
microsoft.com.  3599 IN      TXT  "facebook-domain-verification=bcas5uzlvu0s3mrw139a00os3o66wr"
microsoft.com.  3599 IN      TXT  "adobe-sign-verification=c1fea9b4cdd4df0d5778517f29e0934"
microsoft.com.  3599 IN      TXT  "facebook-domain-verification=gx5s19fp3o8aczby6a22clfhzm03as"
microsoft.com.  3599 IN      TXT  "v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft.com include:_spf-c.microsoft.com
                                  include:_spf-ssg-a.microsoft.com include:spf-a.hotmail.com ip4:147.243.128.24 ip4:147.243.128.26
                                  ip4:147.243.1.153 ip4:147.243.1.47 ip4:147.243.1.48 -all"
microsoft.com.  3599 IN      TXT  "FbUF6DbkE+Aw1/wi9xgDi8KVrIIZus5v8L6tbIQZkGrQ/rVQKJi8CjQbBtWtE64ey4NJJwj5J65PIggVY
                                  NabdQ=="
```

Mitigation Strategies

- Protect your services from attack
  - Anycast
  - IPS / DDoS protection
  - Overall network architecture
- Protect your services from attacking others
  - Rate-limiting
  - BCP38 (outbound filtering) source address validation
  - Securely configured DNS, NTP and SNMP servers
  - No open resolvers

Information Security Training

Password Control

APNIC

Password Control

- What makes a bad password
  - 8 characters long (or less, such as a PIN of 4 digits long)
  - A wild mix of upper case, lower case, number, and special characters
  - 30 day mandatory password rotation (even 90 days is rough)
  - Make sure to setup “secret questions” in case you forget your password

… wait, weren’t these the “good” recommendations?!?

What Makes a Good Password

- Longer is stronger (usually*). 15 character passphrases *should* be normal, and 30+ for more sensitive sites
    - * “usually” means that if you force users to use 16 character passwords and they don’t use a password manager, then you’ll get passwords like: fourfourfourfour or passwordpassword
    - “should” is my perfect world full of rainbows and unicorns, and where everyone is secure
  - Choosing 4 (or more) random words gives you a strong password that humans can remember (see XKCD comic on next slide)
  - To increase the complexity, break up a word by putting a number in the middle of it and/or using something other than a space between words
    - some password crackers use dictionary words and assume spaces between words as a way to break passwords faster

Passwords

Lowercase = 26

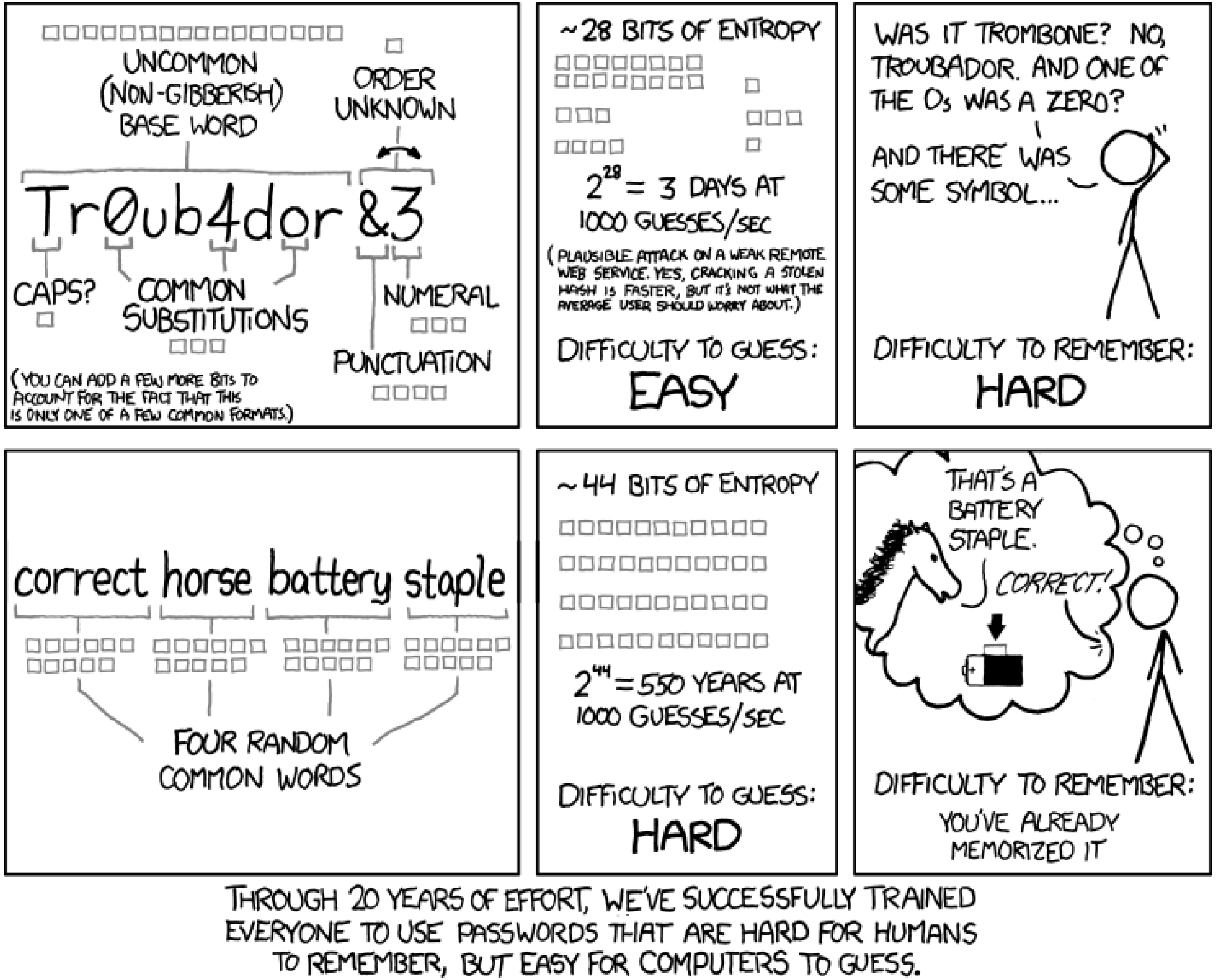
+ Uppercase = 52

+ Numbers = 62

+ Special = 94

EFF long list = 7776
for using 6 dice

EFF short list = 1296
for using 4 dice



Passwords

The top table shows the number of possible passwords, using $(\text{characters})^{\text{length}}$

i.e. $(26)^3 = 17{,}576$

The bottom table shows the password complexity as entropy, using log2(num of passwords)

Length	10 Numbers	26 Character	52 Character	94 Character	1296 Words	7776 Words
1	10	26	52	94	1296	7776
2	100	676	2704	8836	1679616	60466176
3	1000	17576	140608	830584	2.177E+09	4.702E+11
4	10000	456976	7311616	78074896	2.821E+12	3.656E+15
5	100000	11881376	380204032	7.339E+09	3.656E+15	2.843E+19
6	1000000	308915776	1.977E+10	6.899E+11	4.738E+18	2.211E+23
7	10000000	8.032E+09	1.028E+12	6.485E+13	6.141E+21	1.719E+27
8	100000000	2.088E+11	5.346E+13	6.096E+15	7.959E+24	1.337E+31
9	1E+09	5.43E+12	2.78E+15	5.73E+17	1.031E+28	1.039E+35
10	1E+10	1.412E+14	1.446E+17	5.386E+19	1.337E+31	8.083E+38

Length	10 Numbers	26 Characters	52 Characters	94 Characters	1296 Words	7776 Words
1	3	5	6	7	10	13
2	7	9	11	13	21	26
3	10	14	17	20	31	39
4	13	19	23	26	41	52
5	17	24	29	33	52	65
6	20	28	34	39	62	78
7	23	33	40	46	72	90
8	27	38	46	52	83	103
9	30	42	51	59	93	116
10	33	47	57	66	103	129

Passwords

The table expands the password complexity up to 20 characters/words in length

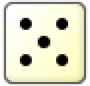
Which would you prefer to remember?

- correct horse battery staple
- Vg*8Tb7u
- gcFQGFhyW
- FQJZAVGZDAR

Length	10 Numbers	26 Characters	52 Characters	94 Characters	1296 Words	7776 Words
1	3	5	6	7	10	13
2	7	9	11	13	21	26
3	10	14	17	20	31	39
4	13	19	23	26	41	52
5	17	24	29	33	52	65
6	20	28	34	39	[illegible]	78
7	23	33	40	46	72	90
8	27	38	46	52	83	103
9	30	42	51	59	93	116
10	33	47	57	66	103	129
11	37	52	63	72	114	142
12	40	56	68	79	124	155
13	43	61	74	85	134	168
14	47	66	80	92	145	181
15	50	71	86	98	155	194
16	53	75	91	105	165	207
17	56	80	97	111	176	220
18	60	85	103	118	186	233
19	63	89	108	125	196	246
20	66	94	114	131	207	258

What Makes a Good Password

- Longer is stronger… (1/3)
  - Problem: humans are bad at selecting random words (or random anything)
  - Solution: use the EFF's long list (example on next slide) https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt
  - References and background reading:
    - https://www.eff.org/dice
    - https://www.eff.org/deeplinks/2016/07/new-wordlists-random-passphrases
  - If you don't have dice handy, use https://www.random.org/dice/



  - Exercise: Open up the long list and random dice URLs above to create some passphrases

What Makes a Good Password

- Longer is stronger… (2/3)
  - Example from the EFF's long list and random.org/dice

61261	superbowl
61262	superglue
61263	superhero
61264	superior
61265	superjet
61266	superman
61311	supermom
61312	supernova
61313	supervise

What Makes a Good Password

- Longer is stronger… (3/3)
  - Better solution: use a password manager with completely random passwords using maximum character sets
    - Although you still need a memorable master password for your password manager, so keep those dice handy
    - We discuss password managers in a few slides

What Makes a Good Password

- Passwords should be globally unique across all sites, both internal and external
  - Problem: humans are bad are remembering 40+ unique 12 character long passwords
  - Solution: use a password manager

What Makes a Good Password

- Passwords may need to be rotated, either for compliance (☹) or after a web site has been compromised (1/2)
  - Password resets can exhaust your users, especially if they are not using password managers
    - Ref: https://arstechnica.com/information-technology/2016/08/frequent-password-changes-are-the-enemy-of-security-ftc-technologist-says/

      and the longer article at

      https://www.ftc.gov/news-events/blogs/techftc/2016/03/time-rethink-mandatory-password-changes

What Makes a Good Password

- Passwords may need to be rotated (2/2)
  - Password manager helps here too, as you don't need to remember the new rotated password
  - New passwords should be randomly generated so you don't have users introducing weakness by creating password variations
    - Password1, Password2, Password3 PasswordJan, PasswordFeb, PasswordMar
    - PasswordGoogle, PasswordYahoo, PasswordEbay, PasswordLinkedin
- One university study found that 17% of new passwords could be guessed easily by knowing what the previous password was. 50% could be guessed within a few seconds of a computer trying
  - Ref: https://www.cs.unc.edu/~reiter/papers/2010/CCS.pdf

Password Control

- Password managers
  - Many to choose from, each with different features and options.
    - Some use cloud storage for easy sync between devices, but also makes it possible to attack remotely
    - Some use 2FA and source-country restrictions for logins to limit the above-mentioned issue, but this can increase the complexity for average users
    - Some are non-cloud based to mitigate remote attacks, but then makes it difficult to sync between devices, and would require something like Dropbox or Google Drive
    - Determine your threat profile to help you choose which password manager is best for you
    - In the end, password managers don’t have to be perfect, they just need to be better than not using one!
  - The best password to use is one that you can’t remember
    - People gave away their passwords for a pen (social engineering)

Password Control

- Server Side Passwords
  - If you are running a server that requires users to create accounts and passwords, you are in a very unique situation to either make the password problem worse, or better.
  - Most of the following recommendations are from the updated NIST document 800-63B on Digital Identity Guidelines
    - https://pages.nist.gov/800-63-3/sp800-63b.html

Server Side Passwords

- DON'T force arbitrarily short passwords
  - Why do some sites restrict you to a maximum of 16 characters?
  - When you hash a password, the output will always be the same length irrespective of how long the input is. (more on hashing in the cryptography module)
  - You can set the minimum password length to something reasonable like 8 or 10 characters, but do not restrict the maximum length to less than 64 characters. Some sites allow up to 128 or 200 characters.

Server Side Passwords

- DON'T exclude which characters can be used.
  - This is done by lazy programmers that don't sanitize the user's input before it is processed or stored (usually in a database as plaintext)
  - This breaks password managers creating random passwords, frustrating your users who are trying to be more secure.
- Similarly, DON'T force which characters MUST be used.
  - This just makes things hard for the user without applying any real test to the strength of the password.

Server Side Passwords

- DON'T force periodic password resets or expiry
  - This just frustrates everyone
  - As mentioned earlier, some compliance standards and auditors will tell you this is required. Use the research info from earlier slides to explain the current state of password control. Sometimes auditors will allow for exceptions or compensating controls which may allow you to get around forced rotation (or at least short reset periods). And we can always hope for standards to get updated with new info!

Server Side Passwords

- DON'T use "forgotten password questions/answers", "secret questions", or "knowledge based authentication"
  - This is usually the fastest way for an attacker to compromise an account.
  - Most information being asked can be found on Facebook accounts
    - Where did you grow up?
    - What is your oldest sibling's name?
  - Other questions are just plain weak
    - What is your favourite colour?

Server Side Passwords

- DO ensure you are storing passwords safely
  - Previously this meant hashing a password, but as we'll discuss in the cryptography module, normal hashing is no longer sufficient
  - Add a salt to your hashes
  - Change the salt for every password, every single time
  - Use a hashing algorithm that lets you define the work factor, and increase it over time
  - Ref: https://www.owasp.org/index.php/Password_Storage_Cheat_Sheet

Server Side Passwords

- DO check new passwords against a list of known-compromised passwords and force the user to try again if any match (1/2)
  - https://haveibeenpwned.com/Passwords
    - There's an API available, and you can download the 320 million compromised passwords (as SHA1 hashes) in a 5.5GB compressed file if you want to check passwords locally.
    - Background reading from the guy making the above site available, Troy Hunt https://www.troyhunt.com/introducing-306-million-freely-downloadable-pwned-passwords/
  - Exercise: Go to the above URL and test a weak password and a strong password, remember don't use any of your current/valid passwords as this is still an external site!

Server Side Passwords

- DO check new passwords against a list of known-compromised passwords (2/2)
  - If you can't implement checks against the HIBP list, or if you want to do additional checks for password strength, consider something like "zxcvbn"
    - https://github.com/dropbox/zxcvbn
      zxcvbn is open source software created by Dropbox, and their USENIX paper is linked at the top of the GitHub link
  - Exercise 2: Go to https://www.bennish.net/password-strength-checker/ and test fake passwords against the zxcvbn checker tool
    Shortened URL is: https://goo.gl/nE5Hhc

Server Side Passwords

- DO provide Two-Factor Authentication (2FA) or Multi-Factor Authentication (MFA)
  - And DO encourage or require it to be enabled for users.
  - Microsoft forces users to have one out of band factor verified (e.g. mobile phone, secondary email) and regularly prompts the user to confirm they are still valid.
    - Password reset success went from 67% to 93%
    - Recovery of compromised accounts went from 57% to 81%

Server Side Passwords

- DO notify your users if someone tried logging into their account with the correct password but an incorrect 2FA/MFA code
  - This is a clear sign that the user's password is compromised and they should change it

Server Side Passwords

- Exercise: Can you spot the problems with the following password restrictions?
  - Most of these are from 2012-2016, and only some have been fixed

Change My Password

Text Size: A A A ? Help Centre

Change your password

The password you create here can be used to access Online, Mobile and Telephone Banking.

All passwords must be six characters in length. Special characters (eg. *, %, $, etc) will not be accepted. Choose a password that's easy for you to remember, but difficult for others to guess. Avoid using birthdates, your name or initials, common phrases such as 'abc123' or passwords you have created for other systems. Do not keep a reminder of your password in an easily accessible place.

All fields are required

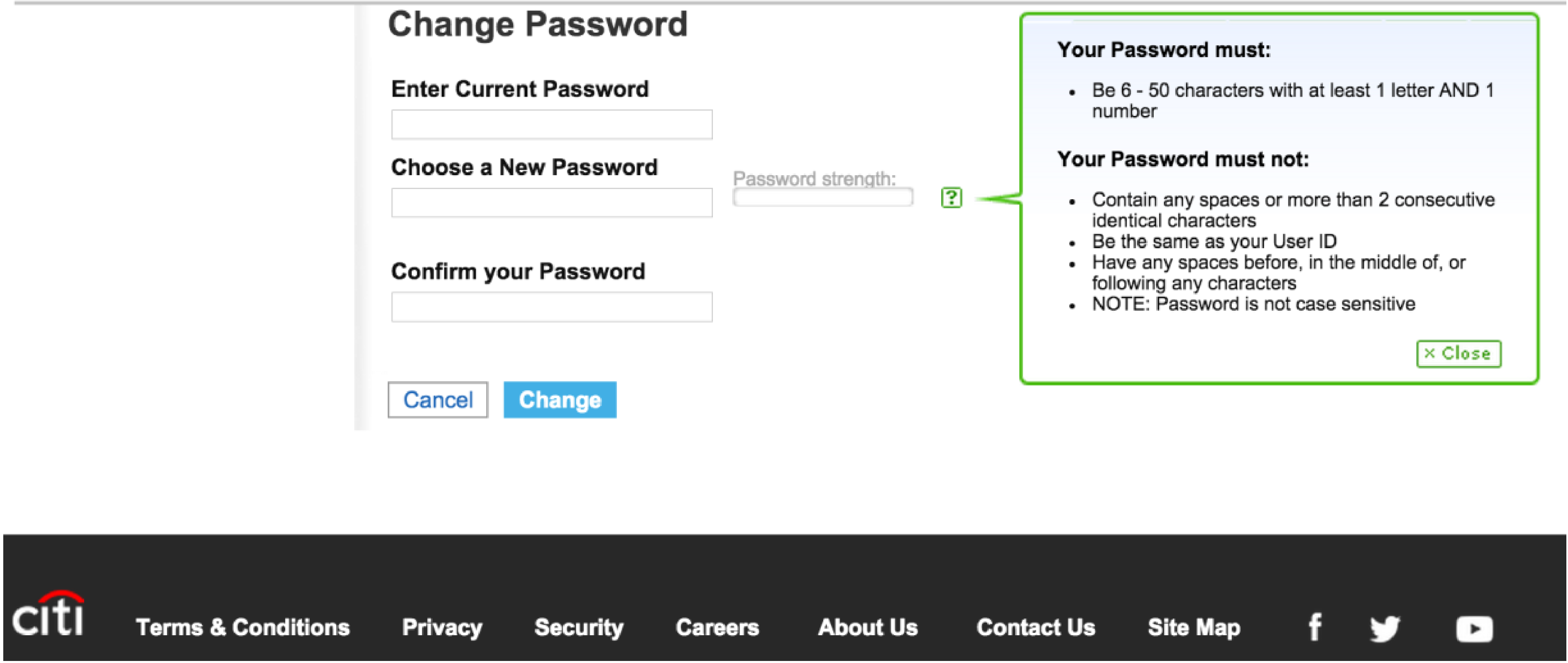
Enter your current password: ••••••

Enter your new password: ••••••

Re-enter your new password:

Your password must be exactly 6 characters in length. Enter only letters and/or numbers.

ACCOUNTS MANAGEMENT



Profile & Preferences

- Summary
- Contact Details
- Statement Delivery
- Card Alerts
- Marketing Preferences
- **Login Password**

Change Login Password

The password applies to your entire Online Services Account and is not Card specific.

Enter current password *

Enter new password *

Re-enter new password *

* Required fields

Clear details

Your password:

- Must be different from your User ID.
- Must contain 8 to 20 characters including one letter and number.
- May include the following characters: % & _ ? # = -
- Your new password cannot have any spaces and will not be case sensitive.

CHANGE YOUR PASSWORD

Step: 1 2

- Updates to your online banking password will take effect immediately.
- Changing your Online Banking password will not affect your telephone banking password.

CIBC card: 4506 4464 6653 3011

Current password:

••••••••

New password:

••••••••••••

Password strength:

Show password

Please enter a password that is 6 to 12 characters long and is made up of any combination of numbers, English letters or both.
{Result #0015}

Re-enter password:

••••••••••••

Password Tips & Tricks

- In addition to using strong passwords and using 2FA, here's a couple of things you can do to add a little extra assurance to your passwords…

Password Tips & Tricks

- On the haveibeenpwned.com site you can subscribe your individual email address or for an entire domain to be alerted for any new data breaches exposing your passwords
  - To verify ownership of a domain, you will need to produce one of:
    - Email verification to security@, hostmaster@, postmaster@, or webmaster@
    - Meta tag on your web server root index page
    - A special file uploaded to the root of your web server
    - DNS TXT record
    - Ref: https://haveibeenpwned.com/DomainSearch
  - To verify ownership of an email address, you just need to respond to a verification email
    - Ref: https://haveibeenpwned.com/NotifyMe

Password Tips & Tricks

- When creating passwords to be used inside a company, consider prepending the randomly generated password with `/!`
  - The `/` (slash) as the first character will prevent the password from accidentally being pasted into IRC or Slack channels or direct messages (IRC/Slack will think it is a command)
  - The ! (exclamation mark) will prevent the password from being saved as a command in the history/bash_history file if you paste your password into a Linux shell
    - This can make it tricky (using quotes, escaping) if you need to embed your password into a command line such as running mysql with a password, but using passwords on command lines is not good security practice anyways, so don’t do that!
    - This also assumes you have history expansion turned on, which it is be default. If history expansion is turned off, your password will be saved in history

Password Tips & Tricks

- Exercise: Log into Kali, open a terminal/console window and type in the following two “passwords” (press enter after each)

  `/ ! A B C 3 5 6`

  `X Y Z 9 8 7`

- Now run the following command to view command history

  `history`

- You can also press the up and down arrow keys to see previous commands