Online Privacy, Security and Password Management

Penguicon
2021Apr25 @ 15:00 UTC-4
Virtual

der.hans
CDE
Object Rocket, a rackspace company
https://www.ObjectRocket.com/

ObjectRocket
https://www.objectrocket.com/careers/

Rackspace Technologies
https://rackspace.jobs/

Upcoming Conferences and Presentations

- GeekBeacon Fest - cfp open now
- SeaGL - organizing now, cfp opens soon
- List of Some Upcoming and Previous Talks and Publications
    - https://www.LuftHans.com/talks

Social Media / Fediverse

- FLOX_advocate on Mastodon
  - https://floss.social/@FLOX_advocate
- LuftHans on PLUME
  - https://fediverse.blog/~/LuftHans
- LuftHans on Freenode IRC
  - usually in #SeaGL, #PLUGaz and #LOPSA

First off,

IANAL

And,

Specifically…

More Importantly,

IANYL

If you need legal review for any ideas from this talk, please talk to YOUR lawyer

Why do we need security?

Spectre/Meltdown (again)

— Equifax admin/admin — Gentoo GitHub // password policy that mandates password managers is planned — Heartbleed — Apple SSL — Apple iCloud — Home Depot — Target — Yahoo! x 2 — LinkedIn x 3 — Eharmony — Last.FM — TJ Maxx / Marshalls — Adobe — Nieman Marcus — 7-eleven — Barnes and Noble — TriCare x 2

— Mat Honan — Jennifer Lawrence — Kate Upton — Rhianna

Cost

> "They could have used my e-mail accounts to gain access to my online banking, or financial services. They could have used them to contact other people, and socially engineer them as well." – Mat Honan

What’s really at Stake?

> "more than a year’s worth of photos, covering the entire lifespan of my daughter" – Mat Honan

> "including those irreplaceable pictures of my family, of my child’s first year and relatives who have now passed from this life" – Mat Honan

Data Collection

- 90% of data ever collected was collected in last 2 years
    - from 2019 Freakanomics podcast

First Things First

- Use only trusted software sources!
- Install Security Updates!

Encryption Example

- Postcard vs Envelope

When to Use Encryption

- All the time!
- Every time!
- HTTPS Everywhere browser Add-on from the EFF
    - Mozilla is adding most of the features to Firefox

What to Encrypt

- Log in credentials
- Personal (identifying) information
  - Name
  - Address
  - Phone Number
  - Credit Card Information
  - Medical Information
  - Private Photos
  - Shoe Size

Password Bleed Over

- Same password at multiple sites?
- One site compromise could quickly expose your data at multiple sites
- Use different passwords for every site!

Credentialed access

- Credentials are the combination of tokens used for authentication

Are you you?

- Username, often email address
- Password
- Security Questions
- PIN
- Multifactor Authentication (MFA)
- Body Parts

Unique

- Every one of those should be unique to every site
- Each item, not just combinational uniqueness
- Some restrictions may apply

Random String

- Random sequence of text gibberish
- Longer and more random are both better
- Use
    - Letters (upper case and lower case)
    - Numbers
    - Punctuation (`!@#$%^&*.,/:\;`)
- Be cautious of
    - Similar looking characters
    - Underline and dash
    - Spaces and tabs
- Example: `fnYV@tki4M’jj;iTW]21`

Random Word Salad

- Random sequence of unrelated words
- Longer and more random are both better
- Use multiple languages if you can
- Declension, conjugation, etc.
- Add mid-word capital letters
- Use randomish punctuation
- Example: purPlish lechE verFaehrt sInging liberte
- XKCD Example: correct battery horse staple

ERROR: /dev/brain read-write failure

But, Hans, that’s way too much to memorize and it’s not near as interesting as baseball stats…

Password Managers

- Securely store credential information
- Easy to use for authentication

Password Manager Requirements

- Free Software
- Hidden Password Entries (`*` not `hunter2`)
- Locally Encrypted, Operating System Independent File
- Data Liberation
- Automagic Clipboard Entry Clearing
- Easy Copy and Paste
- Configurable Password Generator
- Space For Notes
- Entries Organization

Password Manager Bonus Features

- Human Readable Password Generation
- Random Word Salad Generation
- Pronunciation Guide
- Random String Generation from Anywhere in UI
- Secondary Key/Value Storage
- Copy/Paste of Secondary Key/Value
- Data Export with Sync
- Site safety verifications
- Automated password changes

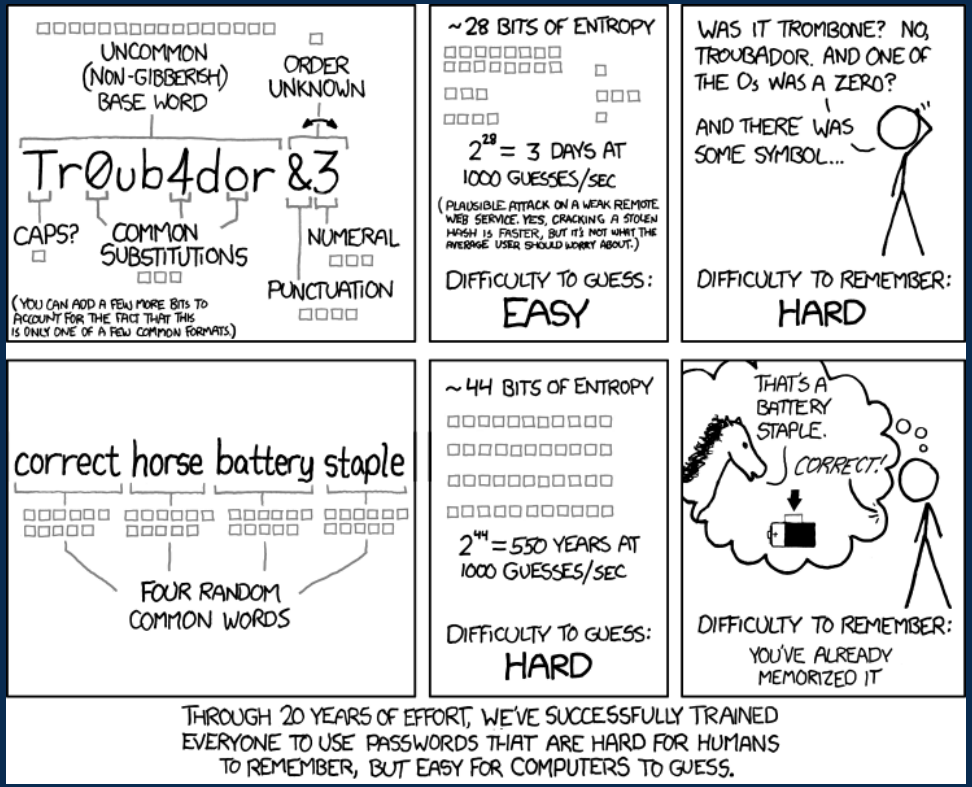
My Recommendations

- GNU/Linux or BSD Device
  - KeePassXC (keepassxc-cli)
  - KeePassX (kpcli)
- Web
  - Bitwarden
  - Nextcloud
    - WebAppPassword
    - Passman
    - Passwords
- Android
  - KeePassDroid
- Other Desktop
  - KeePass

One Password to Hold Them All

One Password to Protect Them All

Passphrases



XKCD: Password Strength - https://xkcd.com/936/

Pronounceable Strings

- Like Dr Seuss, but make less sense
- Useful for over the phone
- Avoid lookalike characters
    - 1 l
    - 0 O
- Pronunciation guides help
    - werecbyivofejmu (wer-ec-byiv-of-ej-mu)

I am me!

Authentication is identifying that you are you

How do you prove it?

- 3 types of authentication data
  - What you know
    - Ex: username, password, PIN
  - What you have
    - Ex: ID, smartphone app, physical token
  - What you are
    - Ex: fingerprint, DNA, facial recognition, retina scan

4th Element: You’ve been tokenized

- Cookies
- Device ID

5th Element

ID: Username

- random string: banks, shopping, utilities
    - Ex: `eddyityoz`
- recognizable handle: public and social sites
    - Ex: `FLOX_advocate`

ID: Email Address

- Subaddressing
  - `username@gmail.com`
  - `username+randomstring@gmail.com`
- Also great for mail filtering
  - `username+3qkrl-ebay@gmail.com`
- Limited use for social networking
  - Friends and colleagues
    - `I know username@gmail.com, please let us converse`
  - Great for notifications from social networks
    - `username+mastodon@pm.me`

ID: Using Subaddressing

- Unique ID and email address for every site
- Use a random token for subaddressing
  - Put site name or other human readable string after the token
    - `username+3qkrl-ebay@gmail.com`
      - account: `username`
      - token: `3qkrl`
      - site: `ebay`
- Don’t reuse that tokenized email address for anything else
- Bonus
  - Filter incoming email to the tokenized email address
  - File fake emails as spam

ID: Cookies

- 3rd party cookies can track you on multiple sites
- Lightbeam 3.0 Add-on
- uMatrix Add-on

ID: Device ID

- Mobile devices have unique ID

ID: Security Questions and Answers

Example: `What was your grandma’s name?+` Example: `What was your first pet’s name?+`
Example: `What is your grandma’s pet’s hairdresser’s shoe size?`

The most important thing is …

Nonsense Is More Secure

Reminder

IANYL

If any of my suggestions go against local laws requirements please consider your legal liabilities

ID: Security Questions and Answers

- Random answers
- Random questions
- Use pronounceable strings
- Key/Value Store

Multi-Factor Authentication (MFA)

- TOTP - Time-Based Tokens
- HOTP - Hash-Based Tokens (HMAC)
- Message - SMS
- Message - Push Notification
- Email
- Phone Call
- Body Part

MFA: TOTP (Application or Token)

- Time based tokens
- Site does not need phone number
- Use your device like a hardware token
- Time sync
- Backup/offline numbers
- OneTimePass, andOTP and more in F-Droid repo
- my recommendation

MFA: HOTP

- Each code used only once
- Must be kept in sync
- Client to server auth
- Server to client auth

MFA: Requires Phone Number

- SMS
  - MitM
  - "SMS should be avoided for anything security related"
    - Mitchell Clark @ The Verge 2021Mar15
- Push notification
- Phone call
  - Who is calling?
  - Alternative: Nextcloud Video Verification

MFA: Email

- See SMS :)
  - Spam rather than sales calls

MFA: Body Part

- Hard to change credential

ID: Birthdate

- Lie when you can
- February 31 no longer works :(
- One liner for randomish date between 1954 and 1999

```
- date -d @$RANDOM*24*3600/2-500000000 +%Y%b%d
```

ID: PINs

- some PINs can be 5 or 6 digits

Backups

- Make regular backups
- Make offsite backups
- Deletion
    - Clouds are forever

Going Forward

- Use long, random strings
- Use subaddressing
- Use multifactor authentication
- Ask vendors to encrypt email

Nicht Vergessen!

Please use unique credentials for every site!

Glossary

- Credentials
  - Anything used to identify you for authentication
- Passphrases vs passwords
  - Essentially the same
  - passphrases implies they are longer and it’s OK to use special characters and spaces
  - try code snippets as KeyPassXC passphrases
- Subaddressing delimiters
  - Often a '+', but doesn’t have to be
  - Depends on your mail provider

Other Privacy Talks and Tools

- The Privacy Tax: How tracking and hacking affect disabled people, and what we can do about it @ Linux.Conf.AU
- Cover Your Tracks / Panopticlick browser fingerprinting test
- The Elephant In The Background: Empowering Users Against Browser Fingerprinting @ rc3

Resources

- Linux Journal (2017Jan): Online Privacy and Security Using a Password Manager
  - https://www.LuftHans.com/LinuxJournal/Online_Privacy_and_Security_Using_a_Password_Manager
- My talks and publications
  - https://www.LuftHans.com/talks/
- Mat Honan Wired article
  - http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/
- Subaddressing list at Wikipedia
  - http://en.wikipedia.org/wiki/Email_address#Address_tags
- XKCD "Password Strength" explained
  - https://www.explainxkcd.com/wiki/index.php/936:_Password_Strength
- Nextcloud Video Verification
  - https://nextcloud.com/blog/unique-sharing-security-video-verification/
- SMS not safe
  - https://www.theverge.com/2021/3/15/22332315/sms-redirect-flaw-exploit-text-message-hijacking-

hacking

Obtaining Software

- KeePassXC
  - https://KeePassXC.org/
- KeePassX
  - https://www.KeePassX.org/
- FDroid
  - https://f-droid.net/
- Bitwarden
  - https://bitwarden.com/
- Nextcloud
  - https://Nextcloud.com/
    - WebAppPassword
    - Passman
    - Passwords

Privacy Enhancing Firefox Add-ons

- Lightbeam 3.0 from Princiya
    - forked from Mozilla by former Outreachy intern in Berlin
- uMatrix from Raymond Hill
- NoScript from Giorgio Maone
- uBlock Origin from Raymond Hill
- uBO-Scope from Raymond Hill
- Decentraleyes from Thomas Rientjes

Credits

- XKCD by Randall Munroe
  - http://XKCD.com
  - Password Strength XKCD 936
- Freakonomics Radio
  - America’s Math Curriculum Doesn’t Add Up (Ep. 391)

Bonus Rounds

Data Escrow

- Use a different KeePassXC file to store other important information
  - Bank account info
  - Life insurance info
  - Government citizen numbers
  - Passphrases for GPG keys
  - PDF copies of contracts and other documents
  - Use multiple different files

Tips

- Don’t use links in email to login
- Use application-specific passwords
- Don’t use Internet Explorer
- Don’t use Outlook

Getting Help

- Free Software Conferences (CLT, FOSSASIA, SeaGL, SCaLE, OLF)
- Local user groups
- Tech Support Fastlane XKCD 806