Basic’s of Privacy and Security

@LegendaryPatMan Paddy@legendary.industries

Topics Covered

- Basic Threat Modeling
- Bad Passwords & Password Advice
- Social Engineering
- Building a Secure Foundation
- Helping Others
- Sources and Resources
- Q&A

This talk isn’t a memory test, you can get a copy of the slides if you want to take more of the talk on board

You don’t have to use all or any of the tips, it’s up to you to take appropriate measures to protect yourself

Privacy != Security

They are co-dependent on each other

Privacy helps Security
Security helps Privacy

I don’t distinguish between benefits as they are so linked for the purpose of this talk

This talk will not help you hide from the NSA or whoever

If they want into your devices, no matter the precautions you take, as soon as you make a mistake, you will loose to them

You will make that mistake sooner or later

I absolutely guarantee that you will

Basic Threat Modeling

What is Threat Modeling?

We do instinctively, when we cross the road etc

In it’s simplest form, it allows us to anticipate the threats that could affect you

How to Threat Model

- Know what you want to protect
- Know the bad things that could happen
- Figure out how likely it is that bad things could happen
- Mitigate the bad things happening

What threats are there to a house?

What defensive measures do you take?

Your house has…?

Assets

- You have valuable items you'd like to keep

Threats

- Burglary is a thing

Risks

- There is a non zero chance that threats could succeed

Mitigations

- Locks, camera's, alarms, dogs etc

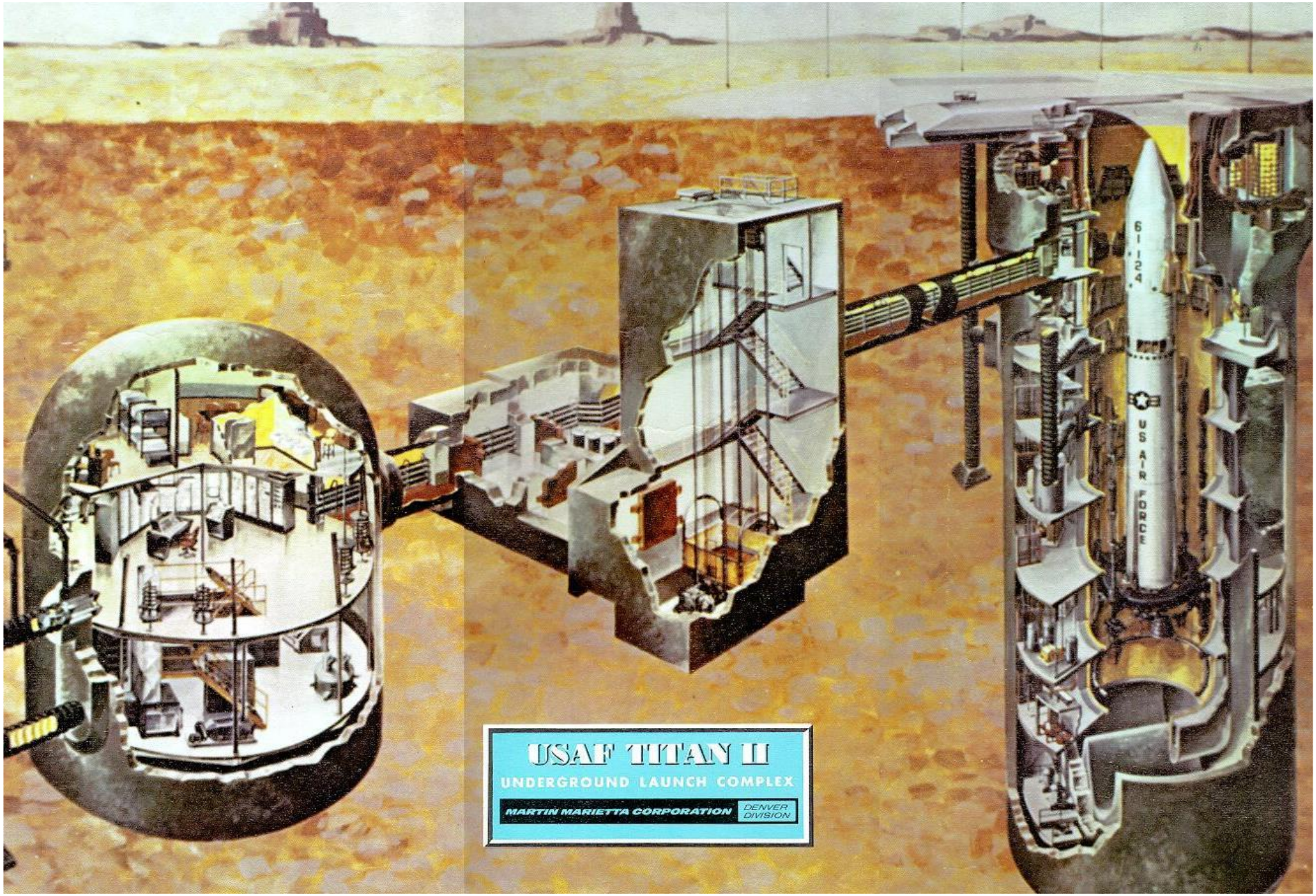
Improving our defences!

So obviously what we need is

1. Key card access on all doors and entry points, including for pets and your armed guards

2. Air tight rooms where Oxygen/CO2 consumption and motion is monitored

3. The only entrance being blast proof doors


61-124
US AIR FORCE
USAF TITAN II
UNDERGROUND LAUNCH COMPLEX
MARTIN MARIETTA CORPORATION
DENVER DIVISION

Can everyone but me live in a bunker?

So how does the threat act?

There are two types of Burglars, Opportunistic & Targeted

Targeted are like they NSA.

They can defeat and undermine your defences

They will do surveillance and know your movements

If they want what you have, they get it.

Opportunistic Burglary

- The most common form of attacker
- Will break in quickly, for short periods of time in broad daylight
- Looks for valuable but quickly fencible or launderable items
- The go for the least visibly secured target

Not being at the bottom

- Locked doors, in theory stops people
- External letterbox/no keys near the front door
- Privacy blinds to hide/obscure assets
- CCTV camera’s real or fake
- Gate and fenced front garden slow them down

Threat Modeling Us and Others

What are we worried about?

Mostly just cyber crime

- We or family members are hacked
- Attacked by malware
- Victims of phishing or scams

So what threats do we face?

- Bad passwords/password advice
- Social Engineering
- Not having a secure foundation to work from

Bad Passwords & Password Advice

Does anyone know who Bill Burr is or what NIST Special Publication 800-63 Appendix A is?

A minimum of 8 character passwords

Include at least one upper case letter, one lower case letter, one number and one special character

Used a dictionary to prevent subscribers from including common words and prevented permutations of the username as a password

Change it every 90 days.

Bill was a manager at NIST

He had no knowledge of security

His entire set of recommendations was based off of one paper, from the 1980’s when there was no internet and the threat landscape was very different

In short;

"Much of what I did, I regret"

Bill Burr
Aug. 7, 2017

https://www.wsj.com/articles/the-man-who-wrote-those-password-rules-has-a-new-tip-n3v-r-m1-d-1502124118

Password Best Practices

Be sure to use a different passphrase for every account or device you have.

Never share a passphrase or your strategy for creating them with anyone else, including coworkers/family etc

Avoid easy-to-guess or commonly used passphrases

Be careful of websites that require you to answer personal questions

Mobile devices often require a PIN to protect access to them and Pin == Password

Do not use public computers

https://www.sans.org/security-awareness-training/resources/passphrases

Password Managers

Encrypted database of your passwords

It should be simple for you to use

It should work on all devices you need to use passwords on

Only use well-known and trusted password managers

Lastpass, Dashlane, KeyPass

It should automagically generate strong passwords

It should be able to store other data too

Make sure your choice patches regularly

https://www.sans.org/security-awareness-training/ouch-newsletter/2017/password-managers

Two Factor Auth

aka Two Step Verification/2FA

Even bad passwords are saved by 2FA

Protects against phishing

Imperfect solution sometimes if not FIDO Certified

SMS messages

Yubikey with U2F and NFC is good enough

Google Titan Key’s are the gold standard

https://www.sans.org/security-awareness-training/resources/two-step-verification

A note on bad passwords & 2FA

Mark Risher, Google's account security guy @00:26:30;

"Some bad advice we've given for years and years and years, which is you should never write down your passwords, and that comes from a bygone era where people had a workstation or a mainframe that was in their office and their threat model was the cleaning crew or people coming through the building, who might see a postit note stuck on your monitor and use that to login. That advice no longer works in global threats and remote login scenarios"

If you can't remember long passwords OR use password managers, there's no issues using bad and/or written down passwords and 2FA given the assumed threat model of cyber crime etc

https://www.lawfareblog.com/lawfare-podcast-mark-risher-google-advanced-protection

Social Engineering

Social Engineering

The art or better yet, science, of skilfully manoeuvring human beings to take action in some aspect of their lives

Has a valid place in Security and society

But tends only to be used by criminal, con men and magicians

Scammers will attempt to maneuverer or engineer you into giving up some detail about you in order to complete a scam

Scams

- Nigerian Princes
  - You pay *‘legal fees’* get money
- Tech Support Scams
  - Microsoft doesn’t take such personal care to call you about your problems
  - Used to take control of PC’s and deploy banking malware etc
- Bank impersonations
  - If banks call you, stop and you call them back
  - Do not give the caller any confidential information

Building a Secure Foundation

The Secure Foundation

Choosing the right devices

Choosing the right tools

Securing your devices

Choosing the Right Devices

Device Selection

- You need to go beyond the spec’s and look at the supply chain as many devices come with bloatware
  - Can be to *improve* user experience or also as a way to monetize devices
  - But can also be Malware such as Spyware and Rootkits
- Good devices should allow you to do a clean OS install without add-ons OR come without bloatware
  - Device has Linux support or buy Win 10 Pro

Lenovo

Ship devices with:

- Rootkits preinstalled
- Spyware
- SuperFish MITM tool

1. https://boingboing.net/2015/08/12/lenovo-preloaded-laptops-with.html
2. https://www.computerworld.com/article/2984889/lenovo-collects-usage-data-on-thinkpad-thinkcentre-and-thinkstation-pcs.html
3. https://www.theguardian.com/technology/2015/feb/19/lenovo-accused-compromising-user-security-installing-adware-pcs-superfish
3. https://www.pcworld.com/article/2886827/bravo-windows-defender-update-fully-removes-lenovos-dangerous-superfish-malware.html

Huawei

Ship devices with:

- Drivers that mimic DoublePulsar
- Has API’s with undocumented root API privileges

1. https://arstechnica.com/gadgets/2019/03/how-microsoft-found-a-huawei-driver-that-opened-systems-up-to-attack/
2. https://medium.com/@topjohnwu/huaweis-undocumented-apis-a-backdoor-to-reinstall-google-services-c3a5dd71a7cd

OnePlus

Ship devices with:

- Software that collects data you copy that contains keywords
- Software that extensively monitors your device usage and calls home

1. https://twitter.com/fs0c131y/status/956628910308982785?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E956628910308982785&ref_url=https%3A%2F%2Fbgr.com%2F2018%2F01%2F26%2Foneplus-data-collection-clipboard-app%2F2.
2. https://www.reddit.com/r/oneplus/comments/4t20ri/oxygenos_reports_back_tons_of_data_with/

Samsung

Ship devices with:

A storage system that sends data back to an Anti Virus company that you should not trust

https://www.reddit.com/r/Android/comments/ektg8u/chinese_spyware_preinstalled_on_all_samsung/

Useful Privacy & Security Tools

I can’t tell you what the best tool is. I can only tell you that tools exist and that they can defend you against certain threats

No tool will defend you against all threats

You need to look at the threats to you and to choose the best tool for you to defend against the threats you worry about

Firefox

Give you full control of what you want your browser to do even enabling and disabling security features

Fully sandboxed with strict same origin policy and forces HTTPS with DNS over HTTPS

Blocks trackers, pixels and malicious content

Containerizes sites like Facebook with exceptionally excessive tracking

Provides guides on securing yourself how you want

1. https://support.mozilla.org/en-US/products/firefox/privacy-and-security
2. https://support.mozilla.org/en-US/products/firefox/protect-your-privacy

Why not Chrome?!

1. Google is introducing Manifest V3 which doesn't have the `webRequest` API and without it, you can't request what URL's are loading to block tracking or prevent drive by malware
2. Google is actively blocking new builds of adblockers just beacuase

1. https://www.forbes.com/sites/kateoflahertyuk/2019/05/30/google-just-gave-2-billion-chrome-users-a-reason-to-switch-to-firefox/#7a554fe6751f
2. https://github.com/uBlockOrigin/uBlock-issues/issues/745

uBlock Origin

Security

Filters malicious URL’s

Audits hyperlinks

Strict malicious domain blocking

Prevents most Drive-by attacks

Privacy

Blocks ads and does cosmetic filtering to fill gaps for ads

Blocks link prefetching

Prevents IP address leaks

Blocks pop ups better than Chrome

Blocks remote fonts and JS requests

Other Tools

Privacy Badger

- Prevents multisite trackers
- Audits cookies
- Blocks more hidden forms of tracking like super cookies and behavioural tracking

HTTPS Everywhere

- Chrome & Firefox force HTTPS but doesn’t block non-HTTPS requests, this does.
- Breaks trackers

This isn’t without it’s flaws...

Some sites hate that you attempt to protect your privacy… Some of these add-ons to FireFox can break some sites

Privacy Badger causes the most issues but it’s still once in a blue moon and easily fixed my moving sliders from red to green

VPN’s

Pros

Prevents Metadata leakage such as domains to network providers and ISP’s

Pirate Content

Stream Content form the UK or US etc

Military Grade Encryption

Cons

- VPN’s cause Choke Points and Choke Points are excellent for monitoring traffic and doing traffic analysis
- Unprovable security claims
  - No logs
- Good crypto is great but implementations can be poor (CVE-2020-0601)

Trade Off's

- While it does prevent metadata leakage to ISP's and network providers, it just changes who can see the metadata
- Doesn't protect your data over open WIFI because HTTPS does since TLS

Private Internet Access

- Private Internet Access is now owned by Kape Technologies
- Kape used to be Crossrider
- Crossrider distributes AdWare and tracks everything you do in a browser
- Your VPN might now work like HotSpot Shield Free

https://telegra.ph/Private-Internet-Access-VPN-acquired-by-malware-business-founded-by-former-Israeli-spies-12-01

Also if I was the NSA, the first thing I would have done post Snowden when VPN marketing exploded was pump billions into a global VPN with HUGE marketing and get everyone on board and collect metadata that way

So What if you want a VPN?

Honestly, the only good one is one you control in a location you want to pirate content from or you want to stream content from

VPN’s you set up can also block ads at the network level by blackholing

Alternatives?

- Using TLS 1.3 and DNS over HTTPS
  - End to end encrypted connections
  - Less Metadata leaks - Domains and Server Name Indication
  - Perfect Forward Secrecy guaranteed
- You still have trade off’s like IP’s leaking and geo blocking.

https://content.sciendo.com/view/journals/popets/2019/4/article-p190.xml?lang=en
https://support.mozilla.org/en-US/kb/firefox-dns-over-https

Anti Virus

Lets Talk about Anti Virus

Their basic function is as a kernel hooking engine, identically to how malware uses a hooking engine

Malware takes advantage of the fact that AV hooking engine and this is why AV products sometimes are flagged as malicious

BUT if you OS Provider has an AV system use it! Like say Windows Defender – Literally the top rate AV

Don’t waste your money on garbage third party AV

https://www.av-test.org/en/antivirus/home-windows/windows-10/october-2019/microsoft-windows-defender-4.18-194015/

Device Security and Privacy

Device Security and Privacy

General Tips

iOS

Android

Windows

Mac

Linux

Securing Networks

General Tips

Set login pin/passwords to more than 8 chars

Encrypt your devices

Don't use the admin account for everyday uses. Set up a standard user account

Review your installed apps/programs

Keep your system updated

Backups! Backups! Backups!

Review which apps can access your personal data

Don’t share your location with apps and audit location services

https://spreadprivacy.com/device-privacy-protection/

iOS

- Enable data erasure after 10 failed logins
  - Be careful if you don’t have solid backups as you can loose everything
- Enable “Limit ad tracking”
- Periodically reset your advertising identifier
- Don’t show notifications in the lock screen for sensitive apps

https://spreadprivacy.com/iphone-privacy-tips/

Android

Audit Google’s data collection

https://myactivity.google.com/myactivity

Block apps from Unknown Sources

Check App Permissions when installing apps

Audit which apps you want syncing with the cloud

Review default apps

Don’t show notifications in the lock screen for sensitive apps

https://spreadprivacy.com/android-privacy-tips/

Mac

- Make sure the firewall is turned on
- Enable stealth mode
- Set the computer to log out after a period of inactivity
- Require an admin password for system-wide changes
- Restrict which types of apps are allowed to run on your Mac
- Stop sending diagnostics and usage data

Linux

- Don’t think your immune because you’re running Linux
- Activate your screensaver when idle with screen lock
- Lock down remote connection settings
- Turn off listening services you don’t need
- Make sure you have a firewall running
- Restrict privileged access with SELinux or AppArmor

https://spreadprivacy.com/linux-privacy-tips/

Windows General Advice

Seriously! Don’t use your admin account for daily usage

- **92%** of all critical vulns are mitigated by standard accounts

Use EMET(EOL) on Win7/8/8.1 or Process Mitigation Management Tool on Win10

- Prevent exploitation before they happen

https://www.avecto.com/news-and-events/news/removing-admin-rights-mitigates-92-percent-of-critical-microsoft-vulnerabilities
https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/exploit-protection-exploit-guard

Windows 7

END OF LIFE IS 14/01/2020

You will no longer receive security updates and be able to adequately secure the platform unless a catastrophic wormable Zero Day such as Wannacry

https://support.microsoft.com/en-us/help/4057281
https://www.wired.com/story/microsoft-windows-xp-patch-very-bad-sign/

Windows 7/8/8.1

- Opt out of the Customer Experience Improvement Program
- Turn off Remote Assistance and Remote Desktop
- Remove tracking and data collection updates
- If Sharing a device with others;
    - Check the sharing options for your account profiles
    - Keep certain files and folders private

https://spreadprivacy.com/windows-7-privacy-tips/

Windows 10

You don’t have to link your PC with a Microsoft account

Randomize your hardware address on WiFi

Don’t automatically connect to open WiFi networks

Disable Cortana to keep voice data private

Watch out for system updates changing your privacy settings

Don’t share your advertising ID with apps on your system

https://spreadprivacy.com/windows-10-privacy-tips/

Windows 10

- Stop your speaking and typing being sent to the cloud
- Keep your account info private
- Restrict the apps that can send or receive messages
- Decide whether apps can control radios such as Bluetooth
- Control apps' ability to sync with non-pairing devices
- Limit the feedback and usage data that is sent to Microsoft

https://spreadprivacy.com/windows-10-privacy-tips/

Securing Networks

- Change the default admin password
- Change the default name of your wireless network
- Only use WPA2 or WPA3
- If you use a guest network, secure it the same way
- Disable WPS(Wi-Fi Protected Setup)

Advanced Topics

Preventative Measures

- Have Signal Installed and ready to go
  - Verify keys with ICE individuals for emergency situations
- Have internet tunnel installed and ready to go
  - Either Tor or a VPN
  - You can’t always install it when you might need it

Helping Others

Expectations

My mam wants to take this seriously and I can help her!

Sets up;

- New email account
- On her new tablet
- Uses a password manager
- Uses ok-ish password 10 chars long

This is gona be great! She’ll never get hacked!

Reality

My mam;

- Forgets the password to her email
- Never stored any passwords in the password manager
- Is essentially locked out of her shiny new tablet...


double facepalm

Lessons learned?

Most people are completely technologically illiterate and as much as they try, they will fail

We need to give them simple advice and let technology handle the rest

Keep it simple stupid

- Do the heavy lifting
- Give basic advice they will understand

Advice to give

- Patch! Patch! Patch!
- Backup! Backup! Backup!
- Social Engineering
- Give some of the Password advice
- Use some of the above protective measures

Sources and Resources

Sources

DuckDuckGo Privacy Blog

https://spreadprivacy.com/

SANS Ouch! Newsletter

https://www.sans.org/security-awareness-training/ouch-newsletter/

EFF Surveillance Self-Defense

https://ssd.eff.org/

Good reading

Threat Modeling by Adam Shostack

https://threatmodelingbook.com/

Smart Girls Guide to Privacy by Violet Blue

https://nostarch.com/smartgirlsguide

Social Engineering by Christopher Hadnagy

https://www.wiley.com/en-ie/Social+Engineering%3A+The+Art+of+Human+Hacking-p-9781118029718

Q&A