

volume 1 - Hackers Exposed

zxcvbnm,. /12567890-

Section 1: Goals - Learning Objective

- One of the best ways to learn is to learn to teach someone else.

If you have in your mind that you need to teach what you are learning to someone else after or actually

do teach someone else, that will really help you retain what you learn.

- ✓ Master the fundamental building blocks of security & privacy
- ✓ Understand the online threat and vulnerability landscape
- ✓ Perform threat modeling and risk assessments
- ✓ Determine personal threats and adversaries
- ✓ Build test environments in Virtualbox and VMWare
- ✓ Master encryption
- ✓ Understand Windows, MacOS, Linux security & privacy features
- ✓ Be able to mitigate social engineering attacks
- ✓ Use isolation and compartmentalization effectively

This is for:

- Technically minded people
- If you are concerned about hackers, cyber criminals, malware and viruses
- If you share information anonymously
- If you want to keep communication and personal information private
- Interest in technology and the Internet
- Security professionals
- Students studying IT or security
- Freedom fighters
- Political or religious dissidents
- Journalists
- Businessmen or women where security, privacy and anonymity matters
- Law enforcements officers and agents
- High profile individuals
- Concerned about government and corporate spying
- Whistle blowers
- Anonymous bloggers
- Anyone who has an interest in security, privacy and anonymity

STAT
THE PRACTICAL

Setting up WireTrap (CanaryToken)

- What hackers are looking for:

HERE ARE WHAT HACKERS ARE LOOKING FOR TO GIVE YOU SOME IDEAS FOR THE SORT OF TOKENS YOU CAN CREATE!

Personal

- Passwords and credentials
- Photos
- Email accounts
- Email contacts
- General contact information
- Operating system and application license keys

Business

- Trade secrets
- R&D data
- Customer lists
- Strategic plans
- Insurance numbers
- Employee tax information
- Corporate email accounts

Financial

- Credit card data
- PayPal and payment service accounts
- Bank account data
- Stock trading accounts
- Mutual funds
- Skype/VoIP credit

File Hosting Accounts

- Google Docs
- MS drive
- Dropbox
- Onedrive
- Box
- Apple

Other Accounts

- eBay accounts
- Macys
- Amazon
- Walmart
- Spotify
- Hulu+
- Netflix
- ITunes
- Skype
- Bestbuy

Social Media Accounts

- Facebook
- Twitter
- LinkedIn
- Google+
- Tumblr

Gaming

- PC game and online gaming license keys
- Online gaming characters
- Origin
- Steam
- Crossfire

- To alert if someone was attempted to hack into your system.



You'll be familiar with web bugs which track when someone opens an email. Imagine doing that, but for file reads, database queries or process executions. A more comprehensive explanation can be found [here](#).

Email that you wanted the alert to be sent

Generate your Canarytoken here

Enter your Email Address

Enter a brief Comment to remind you where you used this Token

Got Webhooks?

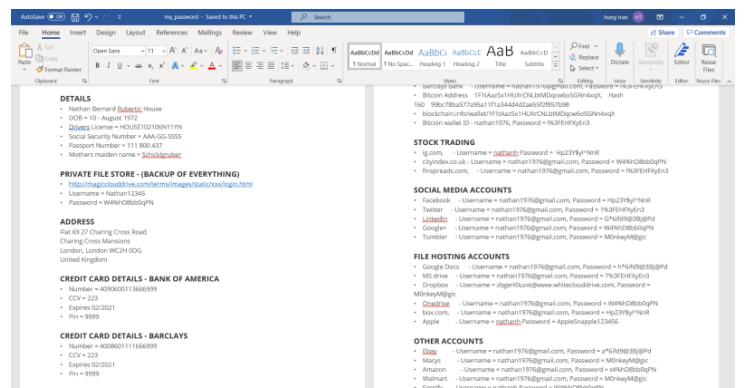
DNS/HTTP Browser Scanner Cloned site Imgur
 LinkedIn Bitcoin

I accept the Terms and Conditions

- To get alert → enter your email

- What this does is, it will alert if someone click on that “file trap” on your system, and obviously it will be triggered and send you an mail alert

- The file is should be named as something interesting to attract the hackers



Result: As if someone enumerating on your system and click on the file → it will alert

"ALERT - StationX Canarytoken Triggered" ➔ Inbox ✎

StationX Canarytokens

One of your canarydrops was triggered. Channel: HTTP Time : 2021-06-08 17:14:26.471120 Memo : Word document in a data folder on laptop Source IP: 2603:9000:ec02

StationX Canarytokens <canarytokens@whiteclouddrive.com>

to me ▾

One of your canarydrops was triggered.

Channel: HTTP

Time : 2021-06-08 17:16:30.006520

Memo : Word document in a data folder on laptop

Source IP: 2603:9000:ec02:700:54d8:336d:42cf:16f8, 172.70.82.162

...

CyberSecurity Career

<https://stationx-public-download.s3.us-west-2.amazonaws.com/A-Guide-To-Starting->

Section 2: Threat and Vulnerability Landscape

The objective of this section is to

- Get an understanding of the foundation principles of **security, privacy, and anonymity**.
- How these principles apply to any given situation, and yours personally so you can assess, select, implement,
 - and monitor appropriate security controls to reduce risk.

Protect what you value

- Time, money, and our resources are precious to us, so we want to spend as little of our resources as possible on security.

Security is not the end goal.

- We want to optimize our use of our resources so that they optimally protect our assets.
- I want you to get your best return on investment in terms of your resources when it comes to applying security.
- So the aim should be to protect what you value most and apply enough security so that you can do the things that you want to do safely online or so the business can function within acceptable levels of
- Protect what you value the most

Thought Experiment

Self / Family
Organization
Service
Application

- What is most confidential?
- What can't you afford to lose?
- What is irreplaceable?
- What would cause the most damage?
- What might impact your reputation?

Example Security Assets

- Photos
- Credit card details
- Bank account details
- Personal Identifiable Information (PII)
- Account information – Linkedin, Facebook, Amazon, Paypal
- Primary Email
- Bitcoin wallet / Crypto currency
- Browser history
- Secret files
- Password information
- Financial records



→ Most valuable things need to protect are:

- Secret files
- Credential details

Definition of Privacy, Anonymity and Pseudonymity

Privacy

- **Privacy** is nobody seeing what you do ⇒ but potentially knowing who you are.
- **Privacy** is about content.

- **Privacy** is about maintaining confidentiality and keeping secrets. → Quyền riêng tư là duy trì tính bảo mật và giữ bí mật.

⇒ **Privacy** is people cannot see what you do, but know you are exist.

Example 1: if you register with a cloud storage provider such as Dropbox, you are not anonymous.

But if you encrypt the files and only you have the key, the data is private.

→ You have **privacy**.

→ You are **private** in your own home as no one knows what you do in your home.

→ You are not anonymous as everyone knows that you live there.

Example 2: You register for an social media account, and you choose to set your account **private**.

→ You have privacy which people cannot see your activity such as what you do

But, people still know that you are existed there.

Anonymity

- **Anonymity** - ẩn danh
- **Anonymity** (an no mi ni tì) is people don't know your true identity, but see what you do.
- **Anonymity** keep your action separate from your true identity
- **Anonymity** means non attribution to your actions to be nameless, to be faceless.

Example:

- You could be under an anonymous using Tor service and contribute to your action such as posting a message

But noone know your identity but your message is received and not private

Pseudo-anonymity

Pseudo-anonymity - bí danh, giả danh

Pseudo-anonymity (Ẩn danh giả) is when you wish to retain a reputation against an identity.

Ẩn danh giả là khi bạn muốn duy trì danh tiếng chống lại danh tính.

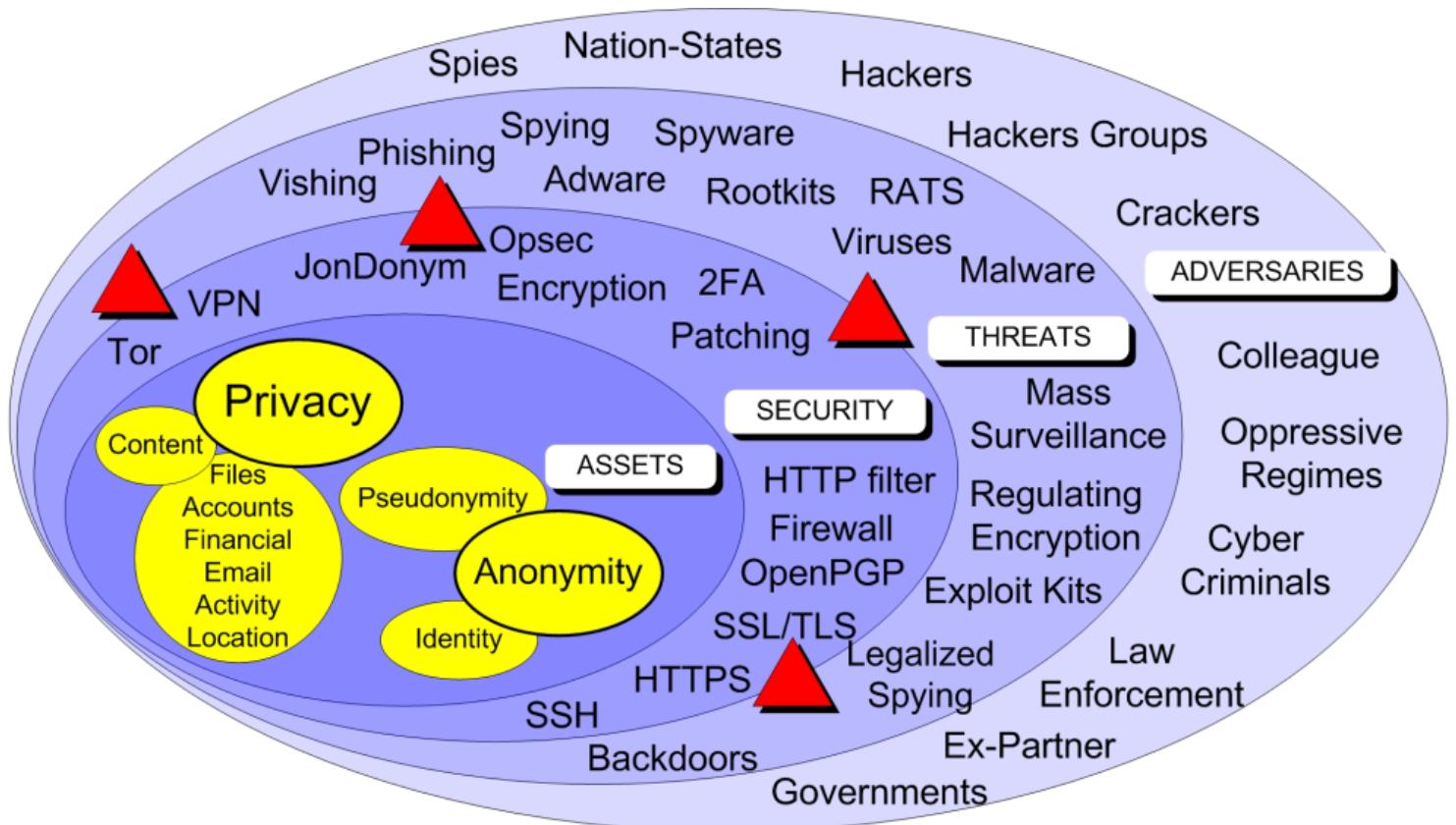
Example: One of the more interesting pseudonyms of modern times is **Satoshi Nakamoto**, the creator of Bitcoin.

Example 2:

A common example is having an alias for social media or for a forum online

Một ví dụ phổ biến là có một bí danh cho mạng xã hội hoặc cho một diễn đàn trực tuyến

Security, Vulnerabilities, Threats and Adversaries



Your **security controls** should be selected based on their ability to mitigate your perceived threats and adversaries and the consequences of that realization.

Risk = (Vulnerability x Threat x Consequences)

Rủi ro = (Lỗi hỏng x Đe dọa x Hậu quả)

Example:

For example, you might select TOR as a security control to help mitigate against mass surveillance the threat of mass surveillance from an oppressive regime. And you might use Tor because the consequences are high in terms of your identity. And once your identity is known, the consequences will be realized.

Ví dụ: bạn có thể chọn TOR làm biện pháp kiểm soát an ninh để giúp giảm thiểu giám sát hàng loạt mỗi đe dọa của sự giám sát hàng loạt từ một chế độ áp bức. Và bạn có thể sử dụng Tor vì hậu quả là rất lớn về danh tính của bạn. Và một khi danh tính của bạn được biết đến, hậu quả sẽ được nhận ra.

→ Dùng Tor để tránh bị giám sát

→ Nhưng hậu quả của việc này là khi bị lộ danh tính

Security control solution: Using Tor to mitigate against mass surveillance

Consequences: high in terms of your identity, once your identity is known, the consequences will be realized.

Asset Selection

As we've discussed, the assets have security controls, possible vulnerabilities, threats and adversaries.



Như chúng ta đã thảo luận, nội dung có các biện pháp kiểm soát bảo mật, các lỗ hổng bảo mật có thể xảy ra, các mối đe dọa và đối thủ.



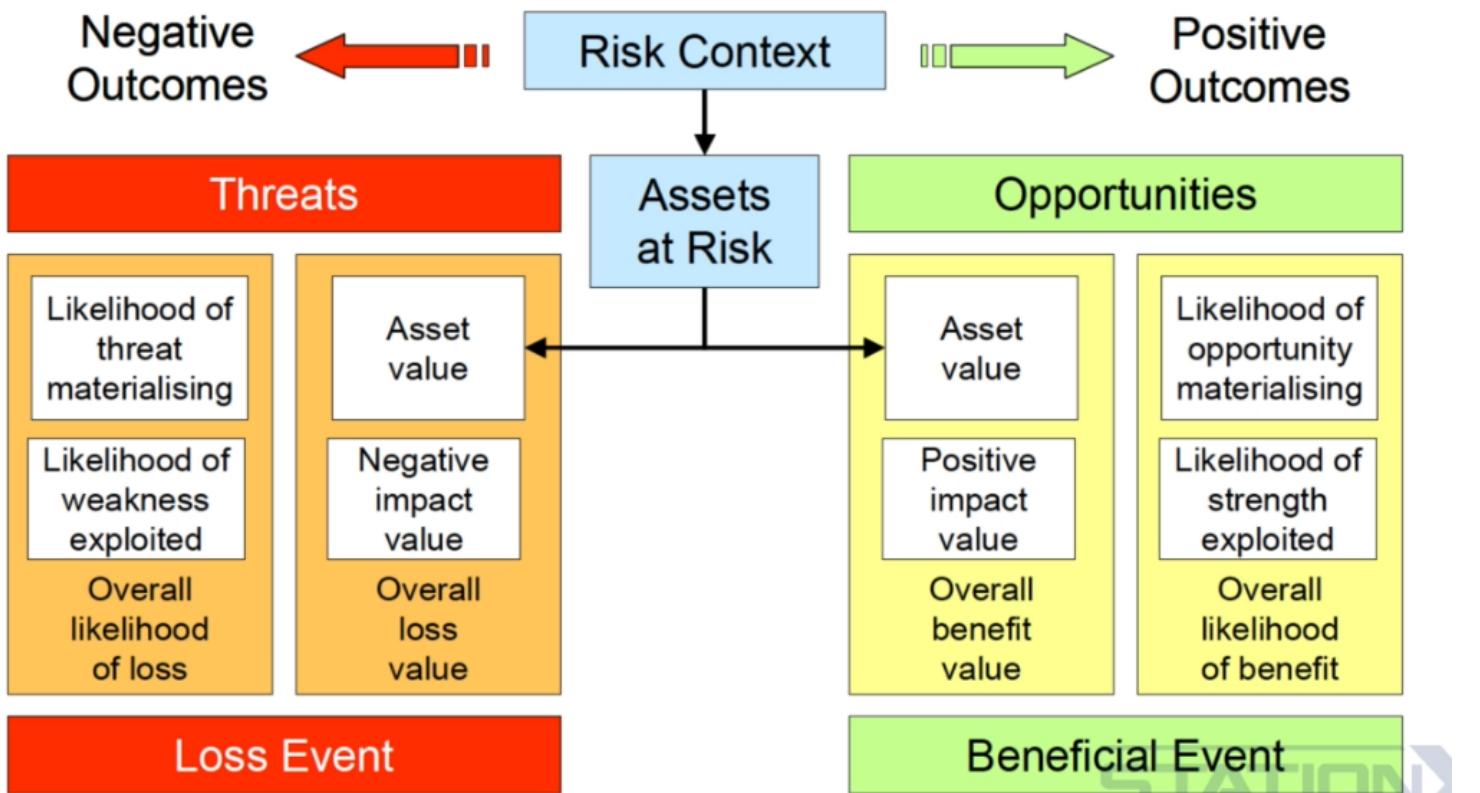
How we define what our assets will depend on the entity you are trying to protect.

So beyond information, data, accounts, devices, you may also want to assign things like functions, departments, processes and other such things as assets to because these things are value too.

Cách chúng tôi xác định tài sản của mình sẽ phụ thuộc vào thực thể bạn đang cố gắng bảo vệ như thế nào.

Vì vậy, ngoài thông tin, dữ liệu, tài khoản, thiết bị, bạn cũng có thể muốn gán những thứ như chức năng, phòng ban, quy trình và những thứ khác như tài sản vì những thứ này cũng có giá trị.

Risk Assessments



STATION
THE CYBER SECURITY COMPANY

We know we can't have 100 percent security.



Chúng tôi biết chúng tôi không thể có 100 phần trăm bảo mật.



So you need to take a risk based approach to applying the right level of security to mitigate the risk without it being overburdensome to the point where the system is unusable.

But only you can choose how big and burdensome your security needs to be to protect your assets.

In order to take a risk based approach to security, you should do basic threat modeling and risk assessments when selecting your security controls.

Vì vậy, bạn cần phải thực hiện một cách tiếp cận dựa trên rủi ro để áp dụng mức độ bảo mật phù hợp để giảm thiểu rủi ro mà không bị quá tải đến mức hệ thống không thể sử dụng được.

Nhưng chỉ bạn mới có thể chọn mức độ lớn và nặng nề mà bảo mật của bạn cần để bảo vệ tài sản của bạn.

Để thực hiện phương pháp tiếp cận bảo mật dựa trên rủi ro, bạn nên thực hiện mô hình hóa mối đe dọa và đánh giá rủi ro cơ bản khi lựa chọn các biện pháp kiểm soát bảo mật của mình.

As you go through the course, select, implement, assess, monitor those security controls that we go through when it comes to select, select security controls, at best, mitigate the risks, for example, of the stolen laptop that we were just talking about.

- You could select whole disk encryption using looks and encrypted boot sector and Priebeke authentication as some of your security controls that mitigate that threat, then implement those controls.

- You install looks, hold this encryption and configure it, then assess assess the controls you have selected for their effectiveness.

- Check that the whole disk encryption is working and the data is actually encrypted.

- Then monitor, monitor the effectiveness of the security controls, check for security updates, for example, and vulnerabilities in looks and so on.

If a weakness is discovered, you go back to the select stage again. So that's a threat modeling and risk assessment.

X

Khi bạn thực hiện khóa học, hãy chọn, thực hiện, đánh giá, giám sát các biện pháp kiểm soát bảo mật mà chúng tôi thực hiện khi lựa chọn, chọn các biện pháp kiểm soát bảo mật, tốt nhất là giảm thiểu rủi ro, chẳng hạn như, của chiếc máy tính xách tay bị đánh cắp mà chúng ta vừa nói đến.

☆

- Bạn có thể chọn mã hóa toàn bộ ổ đĩa bằng cách sử dụng giao diện và khu vực khởi động được mã hóa và xác thực Priebeke như một số kiểm soát bảo mật của bạn để giảm thiểu mối đe dọa đó, sau đó thực hiện các kiểm soát đó.

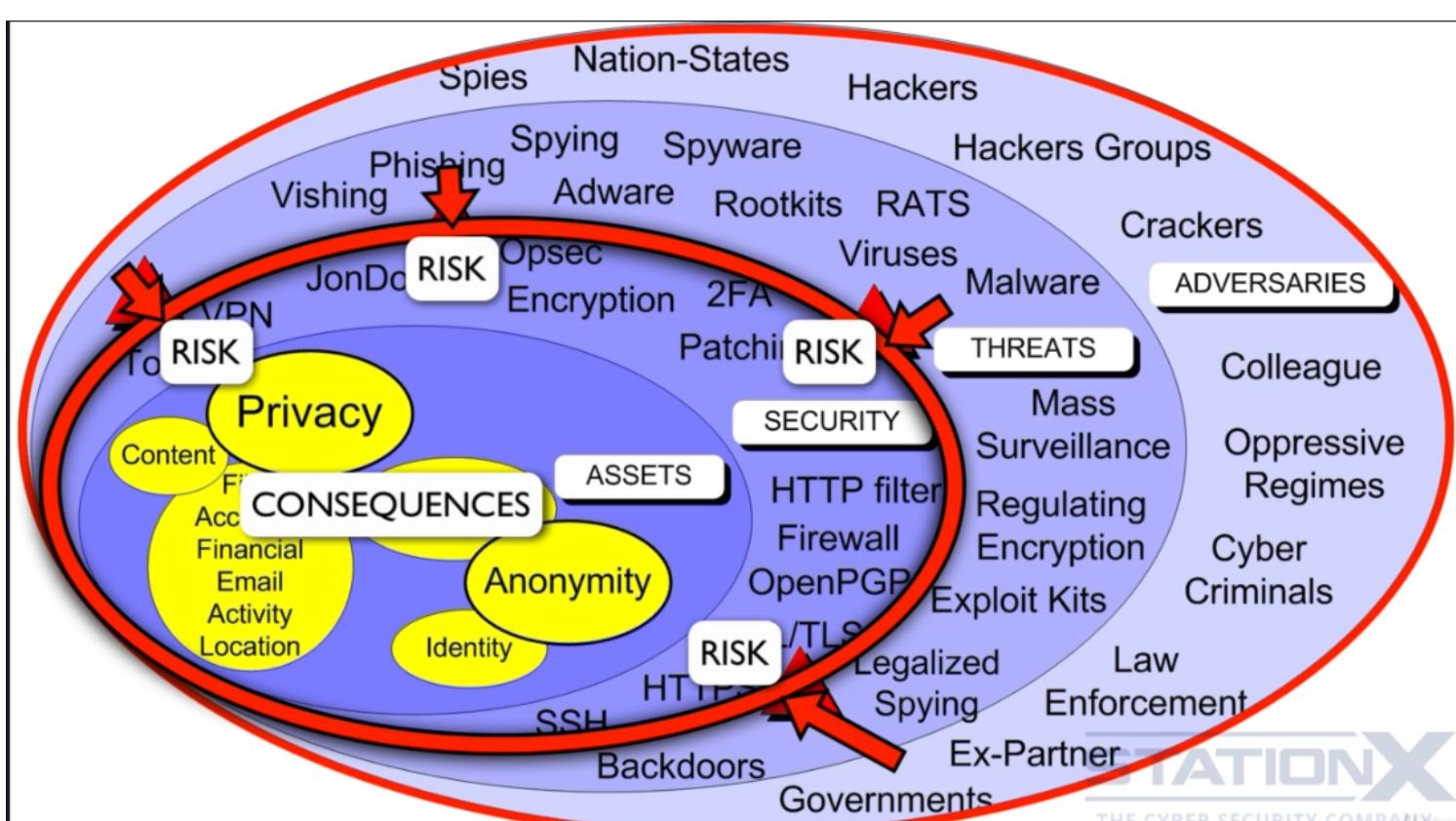
- Bạn cài đặt giao diện, giữ mã hóa này và cấu hình nó, sau đó đánh giá đánh giá các điều khiển bạn đã chọn về hiệu quả của chúng.

- Kiểm tra xem mã hóa toàn bộ ổ đĩa đang hoạt động và dữ liệu thực sự được mã hóa.

- Sau đó theo dõi, giám sát tính hiệu quả của các biện pháp kiểm soát bảo mật, kiểm tra các bản cập nhật bảo mật, ví dụ, và các lỗ hổng trong giao diện, v.v.

Nếu một điểm yếu được phát hiện, bạn quay lại giai đoạn chọn một lần nữa.

Vì vậy, đó là mô hình mối đe dọa và đánh giá rủi ro.



Security vs Privacy vs Anonymity

Can we have it all?

The answer is depends on your purpose activity on the Internet.

For example, if you are a political fighting for a right, then you might need be anonymous (total privacy and anonymity)
as to protect your life.

If you're an average Internet user in the West, you might not want your emails exposed and your surfing history revealed and find that to be an imposition.

the more privacy and anonymity, the more security controls.

As we go through the court and you choose what security controls that you want and need to apply.

X

Khi chúng tôi tiến hành phiên tòa và bạn chọn những biện pháp kiểm soát an ninh nào bạn muốn và cần áp dụng.



- I'll say that again, the amount of privacy and anonymity you require is directly proportional to the amount of security that you need.

==> The more privacy and anonymity, the more security controls.

- Tôi sẽ nói lại lần nữa, mức độ riêng tư và ẩn danh mà bạn yêu cầu tỷ lệ thuận với mức độ bảo mật mà bạn cần.

==> Càng nhiều quyền riêng tư và ẩn danh, càng có nhiều kiểm soát bảo mật.

CIA - Confidentiality, Integrity and Availability

Confidentiality - Integrity - Availability (CIA)

Confidentiality: Defines the solution of security control in the order to protect the asset of the company.

Integrity: Defines the term of untouchable, could the asset be modified unintentionally or get accessed unauthorized.

Availability: Define the availability of security when things happen → Is it always available in emergency situation?

Confidentiality.(Sự bảo mật)

Do we not want the asset disclosed to anyone, i.e. that the asset is not disclosed to unauthorized individuals, entities and processes? If that is true for the asset that defines the sort of security controls we need for that asset, the

Integrity. (Sự toàn vẹn)

Do we not want the asset unintentionally altered?
Do we want to maintain and assure the accuracy and completeness of the asset over its entire lifecycle.
This means that the asset cannot be modified in an unauthorised or undetermined manner.

Availability.(Sự sẵn sàng)

Do we not want it destroyed, i.e. for any asset to serve its purpose?
It must be available when it is needed.
This means the systems used to store and process the asset, the security controls used to protect it.

Bảo mật. (Sự bảo mật)

Chúng ta không muốn tài sản được tiết lộ cho bất kỳ ai, tức là tài sản đó không được tiết lộ cho các cá nhân, thực thể và quy trình trái phép?

Nếu điều đó đúng với nội dung xác định loại kiểm soát bảo mật mà chúng ta cần cho nội dung đó, thì

Chính trực. (Toàn vẹn)

Chúng ta không muốn tài sản bị thay đổi một cách vô ý?
Muốn duy trì và đảm bảo tính chính xác và đầy đủ của tài sản trong toàn bộ vòng đời của nó.
Điều này có nghĩa là nội dung không thể được sửa đổi theo cách trái phép hoặc không xác định.

Sự sẵn sàng. (Sự sẵn sàng)

Chúng ta không muốn nó bị phá hủy, tức là đối với bất kỳ tài sản nào phục vụ cho mục đích của nó?
Nó phải có sẵn khi cần thiết.
Điều này có nghĩa là các hệ thống được sử dụng để lưu trữ và xử lý tài sản, các biện pháp kiểm soát an ninh được sử dụng để bảo vệ tài sản đó.

Example:

So let's get a little bit more tangible here with some examples.

So if something is encrypted, this can provide confidentiality.

If something is hashed, this can provide integrity.

If something is digitally signed, this can also provide authentication, non-repudiation and integrity.

If something is encrypted and digitally signed, this can also provide confidentiality, authentication, non repudiation and integrity.

So you can see that how we've gone from an asset to an asset, having security attributes to then having the security controls such as encryption and hashing and digital signatures that then meet those security attributes.

Vì vậy, chúng ta hãy hiểu rõ hơn chút ở đây với một số ví dụ.

Vì vậy, nếu một cái gì đó được mã hóa, điều này có thể cung cấp tính bảo mật.

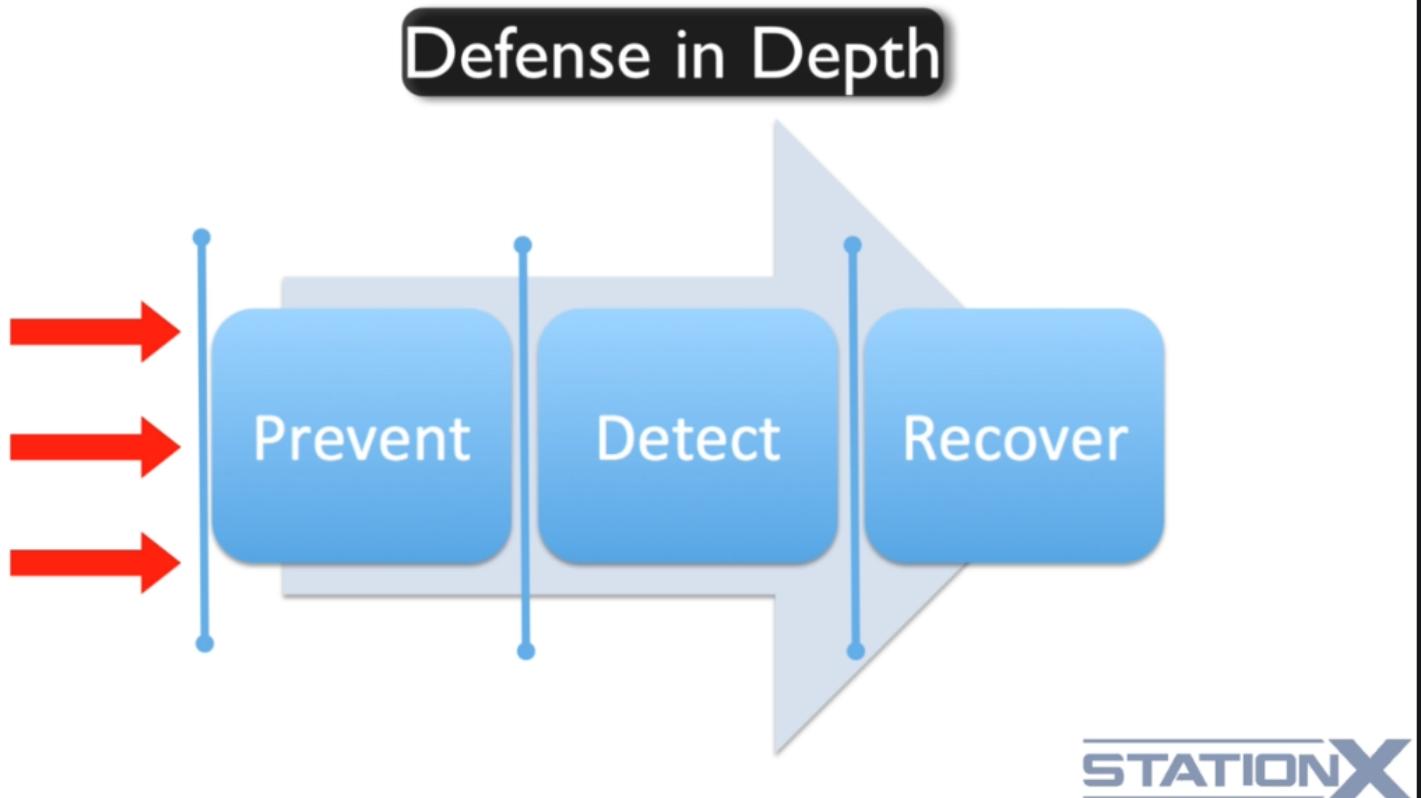
Nếu một cái gì đó được băm, điều này có thể cung cấp tính toàn vẹn.

Nếu một cái gì đó được ký kỹ thuật số, điều này cũng có thể cung cấp xác thực, không từ chối và tính toàn vẹn.

Nếu một thứ gì đó được mã hóa và ký điện tử, điều này cũng có thể cung cấp tính bảo mật, xác thực, không từ chối và tính toàn vẹn.

Vì vậy, bạn có thể thấy rằng cách chúng tôi đã chuyển từ tài sản sang tài sản, có các thuộc tính bảo mật rồi có các kiểm soát bảo mật như mã hóa và băm và chữ ký số đáp ứng các thuộc tính bảo mật đó.

Defense in Depth



Prevention:

This, for example, if you encrypt your files; make sure the key or password isn't available to prevention defense to stop people compromising those files and accessing confidential information.



Điều này, chẳng hạn, nếu bạn mã hóa các tệp của mình; đảm bảo rằng khóa hoặc mật khẩu không có sẵn để bảo vệ ngăn chặn người khác xâm phạm các tệp đó và truy cập thông tin bí mật.

Detection:

Detection could be you set up something called a canary, which is planting a deliberate trap so that a hacker or malware triggers this canary or trap.
So you're notified that something is amiss.



Việc phát hiện có thể là bạn thiết lập một thứ gì đó gọi là chim hoàng yến, đang giăng một cái bẫy có chủ ý để tin tặc hoặc phần mềm độc hại kích hoạt con chim hoàng yến hoặc cái bẫy này.
Vì vậy, bạn được thông báo rằng có điều gì đó không ổn.

Recovery:

Recovery is like backup or having the ability to recover a lost file or a lost account.

×

Phục hồi giống như sao lưu hoặc có khả năng khôi phục tệp bị mất hoặc tài khoản bị mất.

The principle is:

- What you cannot prevent.
- You detect what you cannot detect.
- You recover from through the course.

Defence In Depth

Prevent

Known Threats

- Blacklists
- Reputation systems
- Threat intelligence
- Signature based network and endpoint methods
- Intrusion Prevention Systems (IPS)
- File and disk encryption
- Virtual keyboards
- URL-blockers
- Content filtering
- Host Based Firewalls
- Parental controls

Unknown Threats

- Exploit prevention
- Sandboxes
- Isolation and compartmentalization
- Application white listing
- Application control / Known good
- Host based firewalls

- Host based firewalls
- File and disk encryption
- Secure deletion
- Access Control Lists (ACL)
- User Access Control (UAC)
- Software Restriction Policies (SRP)

Detect

Known Threats

- Anti-virus
- Intrusion Detection Systems (IDS)
- Web Application Firewall (WAF)
- OSquery
- Credit monitoring
- Vulnerability scanning
- Traffic monitoring
- Anti-spam
- EDR technology

Unknown Threats

- Behavioral analysis
- Anomaly detection
- Binary Analysis
- Machine learning

- Heuristic detection
- OSquery
- EDR technology
- CanaryPi
- Canary Tokens

Respond / Recover

- Anti-virus
- Automated response and remediation
- Backups

- Snapshots
- Re-imaging
- Roll back
- EDR technology

The Zero Trust Model

Say you want to store files online, you want to sink your files online, you need to select a provider that offers the sinking service.

Dropbox is a popular choice that many people use.

- You should not trust that they will not get hacked.
- You should not trust that they won't view your files.
- You should not trust that they will not lose or change your files.

Zero Trust Model basically is you should not trust in any type of application or online service from keep your privacy.

<p>Applications can have secret back doors. You may choose to run an application in an isolated virtual machine to stop it.</p> <p>Being able to communicate out applications can have malware again.</p> <p>You may sandbox that application instead of trusting it. You're evaluating your mitigating the risk. You're distributing the trust.</p>	<p>Các ứng dụng có thể có cửa sau bí mật. Bạn có thể chọn chạy một ứng dụng trong một máy ảo riêng biệt để ngăn chặn nó.</p> <p>Việc có thể giao tiếp các ứng dụng có thể lại có phần mềm độc hại.</p> <p>Bạn có thể hộp cát ứng dụng đó thay vì tin tưởng nó. Bạn đang đánh giá việc giảm thiểu rủi ro của mình. Bạn đang phân phối sự tin tưởng.</p>
<p>Krypton and Encrypt are examples of what are called zero knowledge systems.</p> <p>Zero knowledge is when the provider literally has zero knowledge about what it is that they are hosting for their clients.</p> <p>So zero knowledge system goes some way towards providing a system that you don't necessarily need to trust too much in terms of confidentiality and privacy. You still would have to trust them to keep your files available and to not change them if they were indeed hosting files as an example of a zero knowledge service.</p> <p>If your files are extremely sensitive, I still wouldn't trust a claim of a zero nine system because they could always change something.</p> <p>They could recode it as they have control over the application.</p> <p>If it was important, I would always add an extra layer of encryption.</p>	<p>Krypton và Encrypt là những ví dụ về những gì được gọi là hệ thống tri thức không.</p> <p>Không có kiến thức là khi nhà cung cấp thực sự không có kiến thức về những gì họ đang lưu trữ cho khách hàng của họ.</p> <p>Vì vậy, hệ thống kiến thức không đi theo một cách nào đó hướng tới việc cung cấp một hệ thống mà bạn không nhất thiết phải tin tưởng quá nhiều về tính bảo mật và quyền riêng tư. Bạn vẫn phải tin tưởng họ để giữ các tệp của bạn có sẵn và không thay đổi chúng nếu họ thực sự đang lưu trữ tệp như một ví dụ về dịch vụ không có kiến thức.</p> <p>Nếu các tệp của bạn cực kỳ nhạy cảm, tôi vẫn sẽ không tin tưởng tuyên bố về hệ thống không chính xác vì chúng luôn có thể thay đổi điều gì đó.</p> <p>Họ có thể mã hóa lại nó vì họ có quyền kiểm soát ứng dụng.</p> <p>Nếu nó quan trọng, tôi sẽ luôn thêm một lớp mã hóa bổ sung.</p>

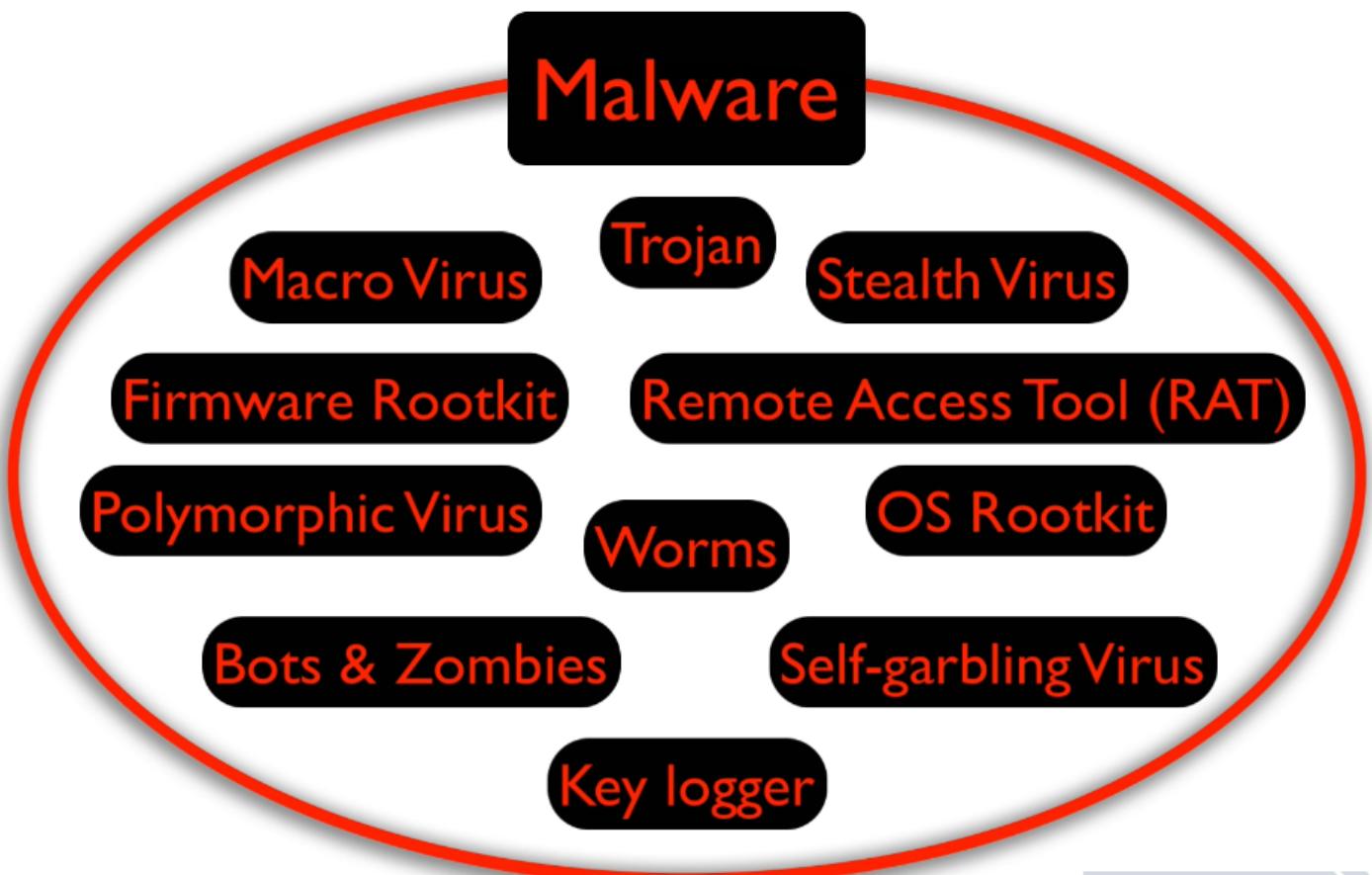
Section 3: The Current Threat and Vulnerability Landscape

Secure yourself online!

- Cyber security is an arms race between offensive and defensive capabilities.
Unfortunately, we are losing this battle as users, we want better technology, doing cooler things, enabling us to do more.
But the more we have, the more we rely on it and the more complex the systems become.

Complexity is the **enemy of security**.

Malware - Virus - Rootkit - RATS



STATIONX
THE CYBER SECURITY COMPANY

Malware

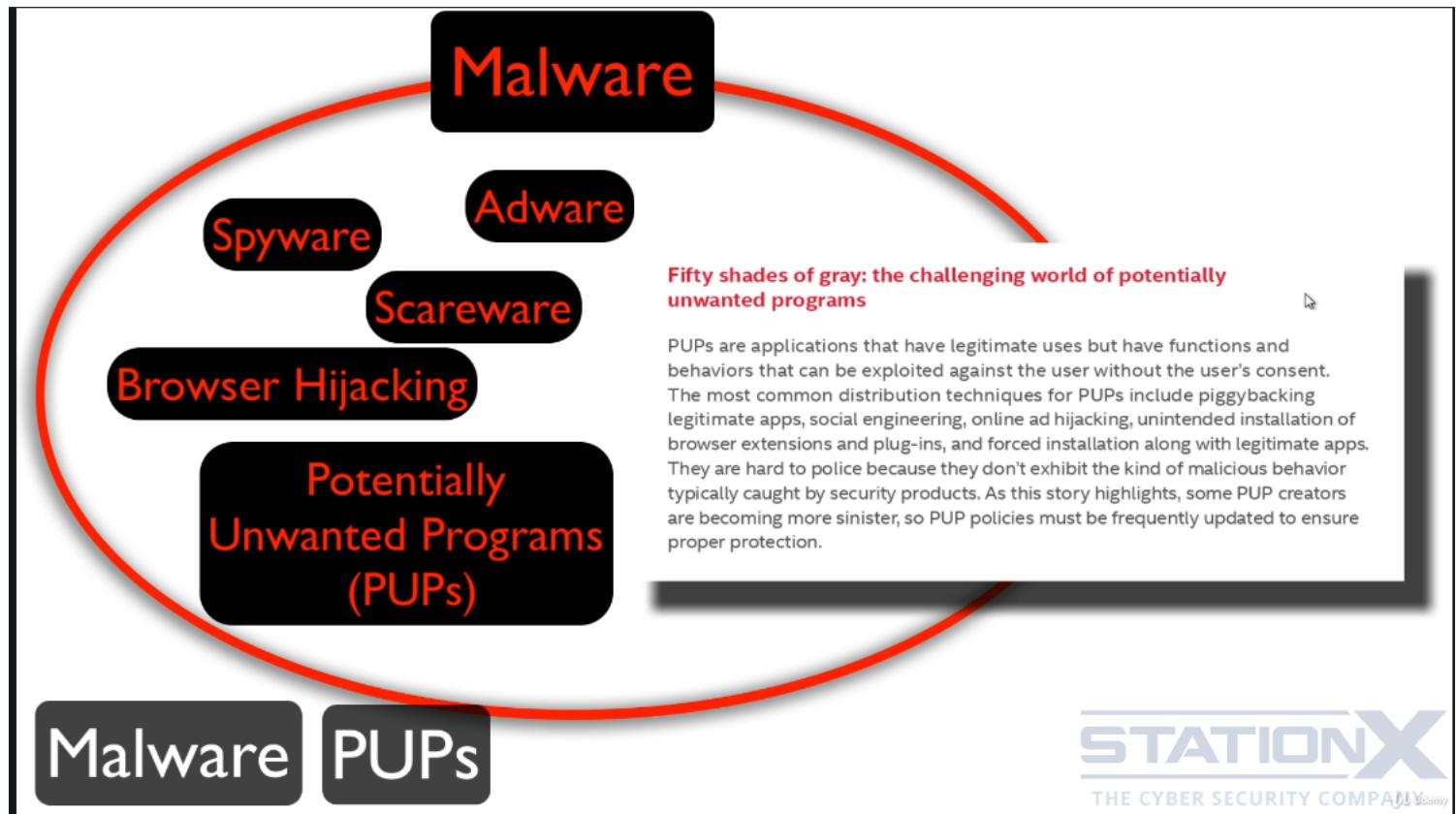
Stealth viruses: A virus that hides the modifications it makes tries to trick antivirus software by intercepting its request to the operating system and providing false and bogus information.

Polymorphic viruses: It produces very operational copies of itself.

A polymorphic virus may have no parts that remain identical between infections, making it very difficult to detect directly.

However, it is not necessary to know all type of malware

Adware, Spyware, Hijacking Browser



Browser hijacking: When an adware or malware takes over your browser in this way.

ScareWare: It is a type of social engineering attack to trick a person into believing in a threat that isn't really real.

So a common example is fake security software claiming that you have malware infections or something like that.

Potentially unwanted program (PUPs): is software that a user may perceive as unwanted. It is used as a subjective tagging criterion

by security

and parental control products.

Phishing, Vishing - SMSing

Phishing: It is a type of attack that typically attempts to trick the victim into clicking on a link or executing malware in some way.

Phishing is typically carried out by sending fake emails or instant messages as well that direct the

victim to a fake site that often resembles a legitimate site. It is a form of social engineering, or in other words, it's an attack against human weaknesses.

Subdomains & Misspelt

<http://www.google.com/stationx.net>

<http://stationx.net/sa/google.com/support/>

<http://www.rnicrosoft.com>

IDN homograph attack

<http://www.g00gle.com>

<http://www.goog1e.com>

The **hidden URLs** is using the HTML tags to hide the real you URL.

So you can see here we've got click here so you don't know what's behind it.

But if you look down there at the bottom, you can see that it's going to Google.com.station,

Hidden URLs

[Click Here](#)

<https://www.google.com/>

google.com.stationx.net

```
<h4>Subdomains & Misspelt</h4>
<a href="http://google.com.stationx.net">http://www.google.com.stationx.net</a><br>
<a href="http://www.stationx.net/sa/google.com/support/">http://stationx.net/sa/google.com/support/</a><br>
<a href="https://www.rnicrosoft.com">http://www.rnicrosoft.com</a>

<h4>IDN homograph attack</h4>
<a href="https://www.g00gle.com">http://www.g00gle.com</a><br>
<a href="https://www.google.com">http://www.google.com</a>

<h4>Hidden URLs</h4>
<a href="http://google.com.stationx.net">Click Here</a> <br>
<a href="http://google.com.stationx.net">https://www.google.com/</a>
```

<http://www.google.com.stationx.net>
<http://stationx.net/sa/google.com/support/>
<http://www.rnicrosoft.com>

IDN homograph attack

<http://www.g00gle.com>
<http://www.goog1e.com>

Hidden URLs

[Click Here](#)
<https://www.google.com/>



XSS Attack

So it is possible that you might get sent a link to a real site and the real site is being manipulated to attack you in some way.

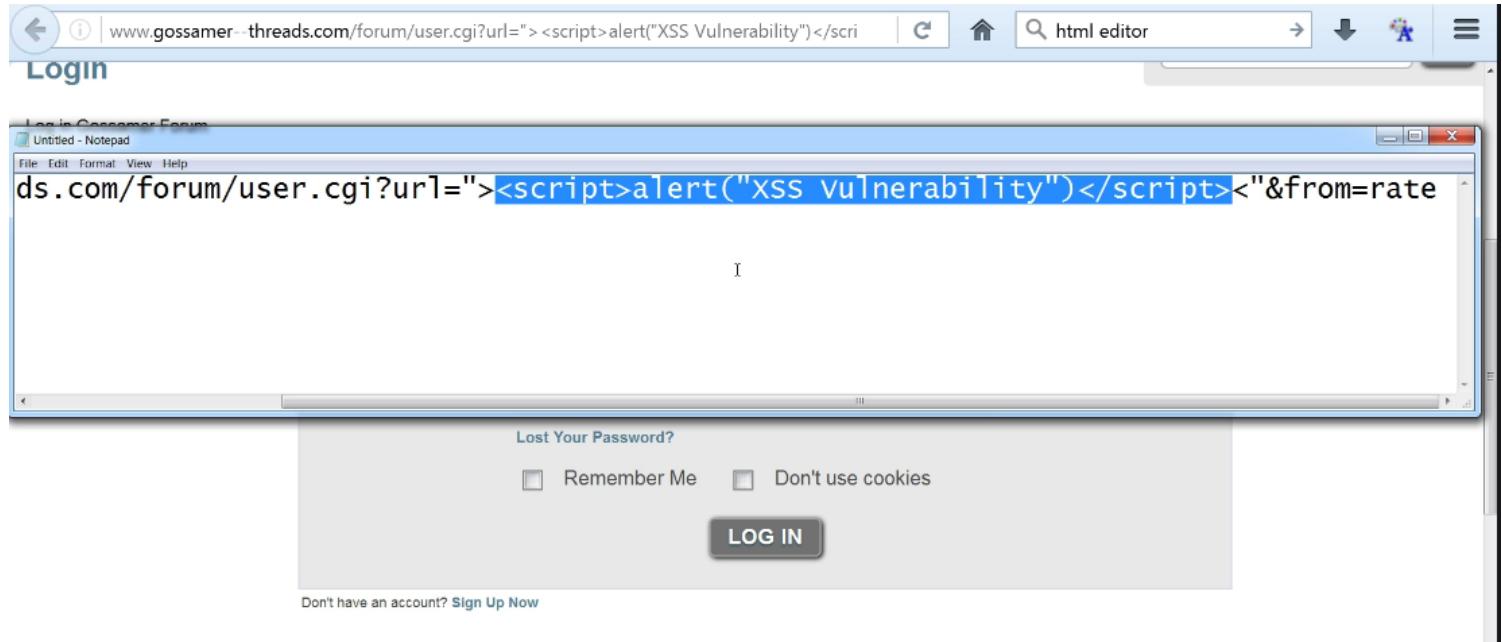
So the attacker can or possibly has found a flaw in the real site and is using a technique like open redirect or as I've just mentioned, the cross site scripting and the cross site request forgery vulnerabilities in order to attack you.

So this has happened to PayPal and many others.

So let me give you an example, because this, you know, obviously won't be clear of a reflected cross site scripting vulnerability that could be used in a phishing attack.

That site should not let me put in my own scripts into your URLs and process it, because what that means is that I am then able to act as that website under the security context of that website, which

means I then have access to your cookies.



Cryptomining Malware

<https://thehackernews.com/2018/01/cryptocurrency-mining-malware.html>

<https://thehackernews.com/2018/02/cryptojacking-malware.html>

Cryptojacking is malicious cryptomining that happens when cybercriminals hack into both business and personal computers, laptops, and mobile devices to install software.

This software uses the computer's power and resources to mine for cryptocurrencies or steal cryptocurrency wallets owned by unsuspecting victims.

Mitigations (Phòng tránh, giảm nhẹ)

Well, you'll need to monitor your CPU usage and see if any process looks like it's running too high.

You will most often notice this from your browser processors due to the JavaScript based attacks from websites Firefox, Chrome, etc..

⇒ Close the browser tab or window that is running up.

⇒ Install AdBlocker

- Installing an ad blocker like you Block-origin that you can see here can help to prevent these crypto minors.

Note: The high process is hard to say what normal CPU usage looks like since computer processing, power and applications people run vary so much.

But a suddenly elevated level of CPU usage would indicate an abnormal increase in demand for processingpower.

Darknets - Dark Market - Exploit kits

Darknets

Darknets is used by government, military, companies and criminal who values their privacy.

→ In some sense, darknets is a tool to maintain anonymity and security

Darknets included:

- RetroShare which is a file sharing peer to peer or friend to friend.
- Ganu Net Framework
- NetProject

Through the **darkness**, you can access dark markets and hacker forums, they sell every sort of good and service from assassination to drugs and of interest towards things like **malware**, **remote access**, **tool rats**, **hacking tools**, **exploit kits** and so on.

Government Secret

NSA secret spying weapon: <https://nsa.gov1.info/dni/nsa-ant-catalog/>

→ These are from circa 2008, 2009, imagine what they might have now if your government is an active threat agent to you or anyone of sufficient means, motive and opportunity, then I hope you can see that if you are a target, the only way to be anonymous online is to be anonymous offline as well.

Five Eyes: Their focus is to gather and analyze intelligence globally, which includes using the Internet for mass surveillance to avoid breaking domestic laws by spying on their own citizens.

Five Eyes

1. Australia
2. Canada
3. New Zealand
4. United Kingdom
5. United States of America

Nine Eyes

6. Denmark
7. France
8. Netherlands
9. Norway

Fourteen Eyes

10. Belgium
11. Germany
12. Italy
13. Spain
14. Sweden

- To give you some concrete examples of how this could include you,

Governments: • Can listen in on your cell satellite and mobile phones.

- Use voice recognition to scan mobile networks, read your emails and text messages, censor web pages.
- Track a citizen's movement using GPS or their mobile phone or the mobile network and can even change email content

while it's en route to you.

- They can secretly turn on webcams built into personal computers, turn on microphones in mobile and cell phones that are not in use.

And all this information is filtered and organized on such a massive scale that it can be used to spy on every person in the entire country. And actually, there's a new facility known as the Utah Data Center, which has been built for storing the enormous amounts of data the structure provides.

x

Và tất cả thông tin này được lọc và sắp xếp trên một quy mô lớn đến mức nó có thể được sử dụng để theo dõi mọi người trên toàn quốc. Và trên thực tế, có một cơ sở mới được gọi là Trung tâm Dữ liệu Utah, được xây dựng để lưu trữ lượng dữ liệu khổng lồ mà cấu trúc cung cấp.

☆

- **Tools for passive and active surveillance** are sold by security companies to governments.

If the governments don't develop themselves or even if they do, if they want to buy extra tools. There is a large and very active market in such tools.

1. Passive RF Retro Ultra High Frequency Reflector:

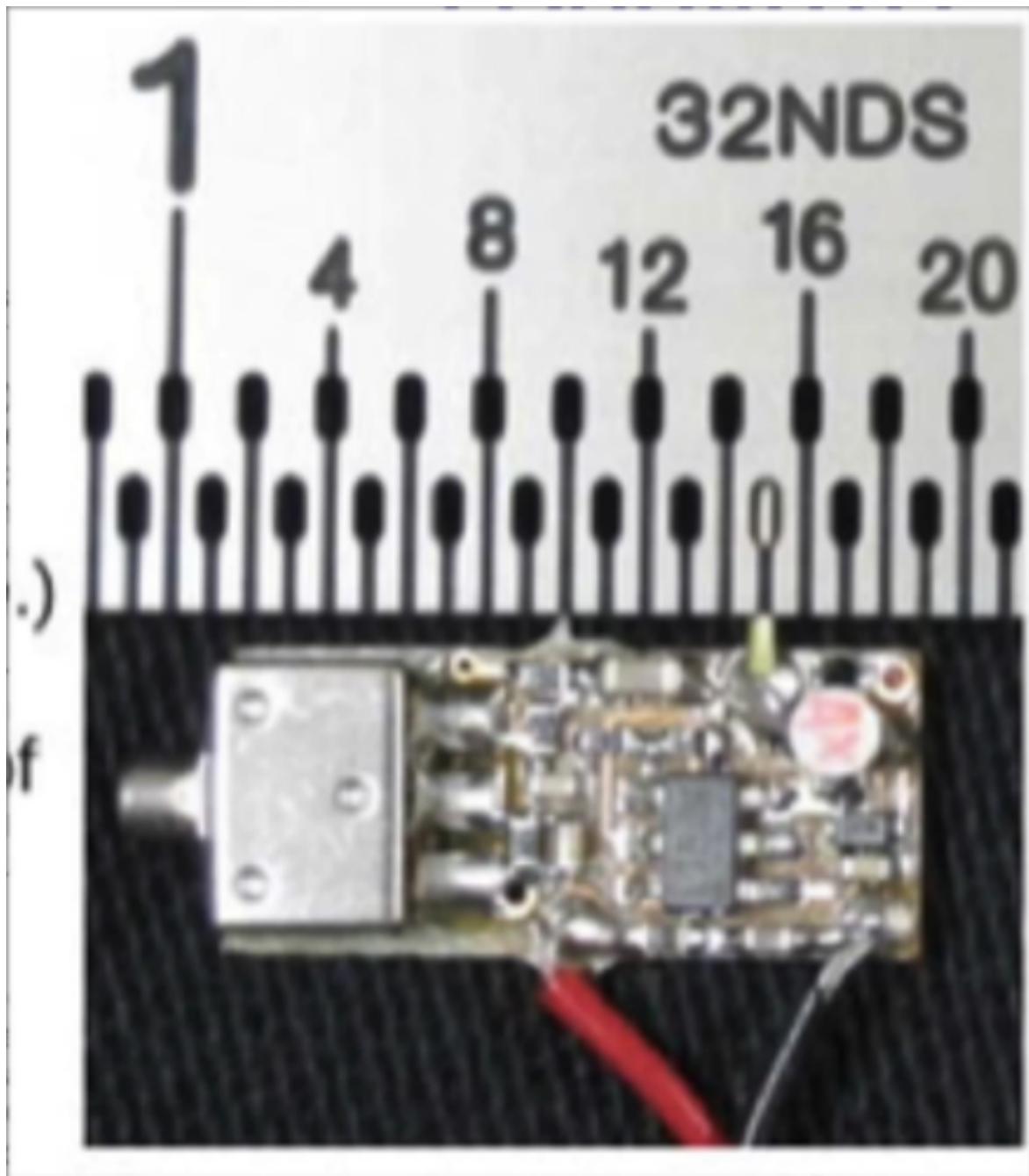
These can be extremely small electronic devices that need only micro amps of power or in some cases need no power at all, meaning that they can remain active for years.

And we can see here audio based RF Retro Reflector provides room audio from targeted space using radar and basic post-processing. So what that means is in order to listen to this device, a person needs to be at a distance somewhere and then send a focused beam of radio frequency energy targeted at that retro reflector. They are then able to listen to the room's audio. The device is only active when it radiates back to the sender.

x

Và chúng ta có thể thấy ở đây Bộ phản xạ âm thanh dựa trên RF Retro cung cấp âm thanh trong phòng từ không gian được nhắm mục tiêu bằng cách sử dụng radar và xử lý hậu kỳ cơ bản. Vì vậy, điều đó có nghĩa là để nghe thiết bị này, một người cần ở khoảng cách xa ở đầu đó và sau đó gửi một chùm năng lượng tần số vô tuyến hội tụ nhắm vào thiết bị phản xạ ngược đó. Sau đó, họ có thể nghe âm thanh của căn phòng. Thiết bị chỉ hoạt động khi nó tỏa ra trở lại người gửi.

☆



Avoiding Government tracking

Look at **WikiLeaks** for government spying type information.

<https://wikileaks.org/-Leaks-.html>

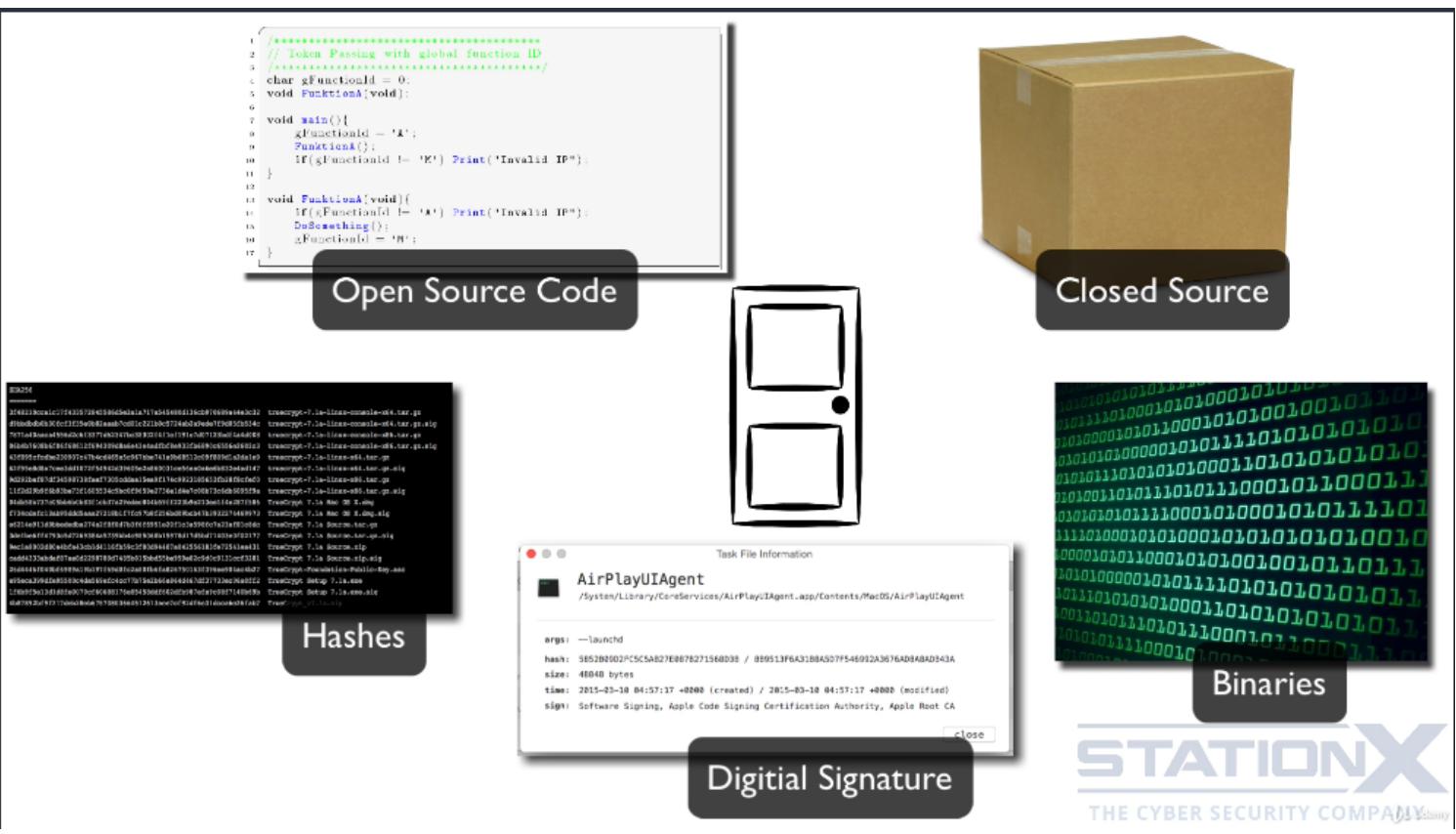
For me, the issue of mass surveillance is about giving away too much power to a government. Key questions to consider and to ask, can you trust all the people, government offices, agencies, companies and contractors with your personal and private data gathered through this mass surveillance? Can you trust that they will always have your best interests at heart and that they

will act justly with this power, this new power that they will have and not just now, but in the future and with your children, because your children will inherit a watched world, this data will be kept and any slight deviation from what is considered acceptable could be used against you.

For me, the issue of mass surveillance is about giving away too much power to a government. Key questions to consider and to ask, can you trust all the people, government offices, agencies, companies and contractors with your personal and private data gathered through this mass surveillance? Can you trust that they will always have your best interests at heart and that they will act justly with this power, this new power that they will have and not just now, but in the future and with your children, because your children will inherit a watched world, this data will be kept and any slight deviation from what is considered acceptable could be used against you.

Đối với tôi, vấn đề giám sát hàng loạt là trao quá nhiều quyền lực cho chính phủ. Các câu hỏi chính cần xem xét và hỏi, liệu bạn có thể tin tưởng tất cả mọi người, văn phòng chính phủ, cơ quan, công ty và nhà thầu với dữ liệu cá nhân và riêng tư của bạn được thu thập thông qua giám sát hàng loạt này không? Bạn có thể tin tưởng rằng họ sẽ luôn dành lợi ích tốt nhất cho bạn và họ sẽ hành động chính đáng với sức mạnh này, sức mạnh mới này mà họ sẽ có và không chỉ bây giờ, mà trong tương lai và với con cái của bạn, bởi vì con bạn sẽ thừa hưởng một thế giới đã theo dõi, dữ liệu này sẽ được lưu giữ và bất kỳ sai lệch nhỏ nào so với những gì được coi là có thể chấp nhận được đều có thể được sử dụng để chống lại bạn.

OS System - Backdoor Trust?



Software is fundamentally a mathematical system.

⇒ Therefore, you can prove the correctness of a system through testing and proving properties of that system.

Unfortunately, currently only the most critical software goes through formal methods like air transportation or process control systems. Formal process is still too time consuming and cost prohibitive for most systems. So most software testing today doesn't provide complete evidence of correctness proven mathematically. So we have to accept the risk of security vulnerabilities and bugs and mitigate accordingly because we know security vulnerabilities and bugs will exist.

X

Thật không may, hiện tại chỉ có phần mềm quan trọng nhất đi qua các phương pháp chính thức như vận tải hàng không hoặc hệ thống kiểm soát quy trình. Quá trình chính thức vẫn còn quá tốn thời gian và chi phí cao đối với hầu hết các hệ thống. Vì vậy, hầu hết các thử nghiệm phần mềm ngày nay không cung cấp bằng chứng đầy đủ về tính đúng đắn đã được chứng minh bằng toán học. Vì vậy, chúng tôi phải chấp nhận rủi ro về các lỗ hổng bảo mật và lỗi và giảm thiểu tương ứng vì chúng tôi biết các lỗ hổng bảo mật và lỗi sẽ tồn tại.



Section 4: Encryption

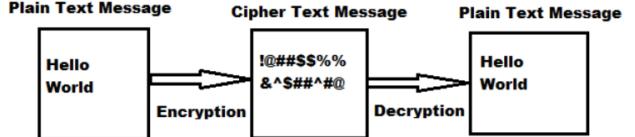
Symmetric Encryption

- **1 Keys Encryption**

- **Symmetric-key** algorithms are algorithms for cryptography that **use the same cryptographic keys** for both the encryption of plaintext and the decryption of ciphertext. The keys may be identical, or there may be a simple transformation to go between the two keys.



- **Encryption** is a method of transforming readable data called plain text into a form that is unreadable is a method of transforming readable data called plain text into a form that is



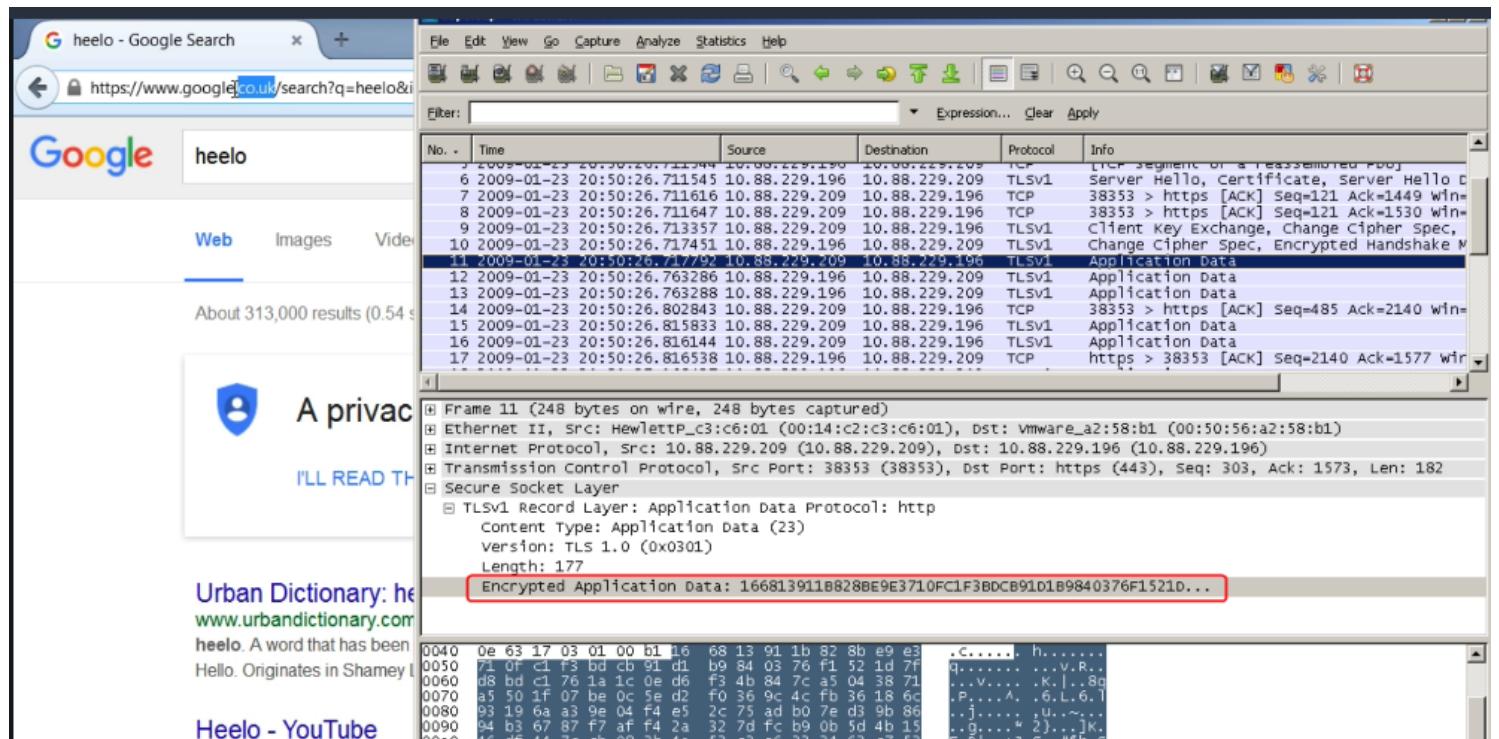
Example:

- If you do a quick search on Google, the content of that webpage is encrypted and the middle-man only knows your destination which is the domain, but not the content

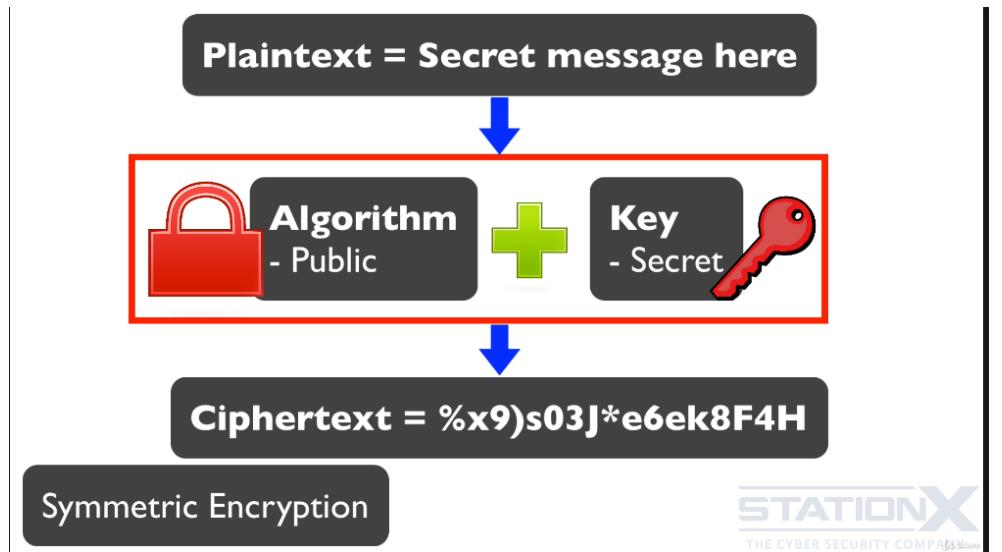
→ So that means that your Internet service provider or your government, maybe they can only see the destination domain.

→ Anybody who's sat between me and Google would only know that I was going to Google.

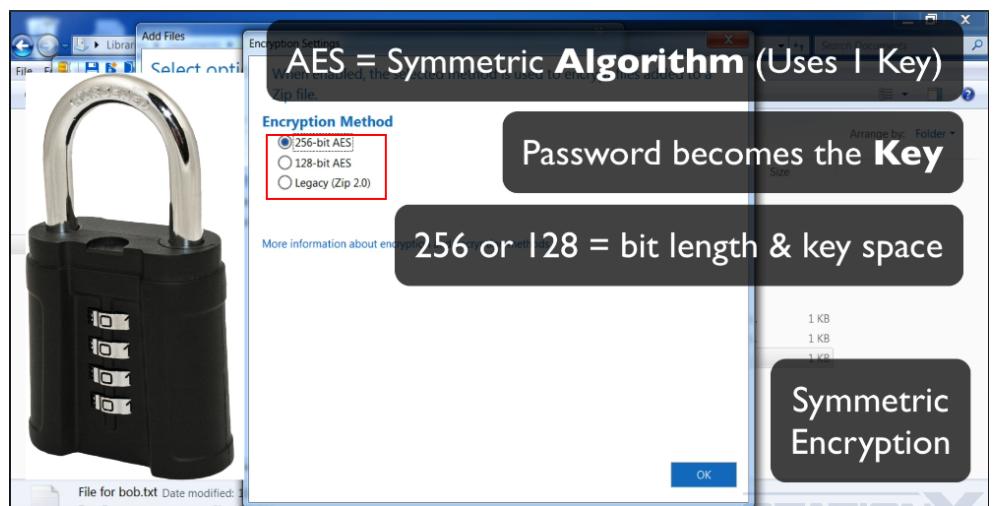
They would not know what I was searching for because this is end to end encryption between my browsers application and the server to simplify things.



Encryption Component



STATIONX
THE CYBER SECURITY COMPANY



The Most Common Word Selections in 10 Million Passwords

Most Used Base Phrase (4+ characters)	Most Used Noun (1,000 most common)	Most Used Verb (1,000 most common)	Most Used Colors (Used with numbers)
1. password 2. qwerty 3. qwer 4. dragon 5. qazwsx 6. alex 7. love 8. monkey 9. master 10. shadow	1. master 2. football 3. killer 4. angel 5. summer 6. money 7. freedom 8. access 9. green 10. silver	1. welcome 2. enter 3. please 4. flash 5. chase 6. catch 7. express 8. enjoy 9. remember 10. rescue	1. red 2. blue 3. black 4. green 5. white 6. pink 7. orange 8. brown 9. purple 10. yellow
Animals	Fruits	I love...	My...
1. fish 2. bear 3. monkey 4. tiger 5. wolf 6. bird 7. eagle 8. lion 9. fox	1. apple 2. orange 3. banana 4. peach 5. lemon 6. cherry 7. mango 8. kiwi 9. grape	1. iloveyou 2. iloveU 3. iloves*x 4. iloveme 5. ilovegod 6. ilovehim 7. iloveit 8. iloveher 9. ilovep*rn	1. mylove 2. mypass 3. myself 4. mybaby 5. mylife 6. myname 7. mypassword 8. mygirl 9. mykids

Asymmetric Encryption



- **2 Keys Encryption**

Public-key cryptography (asymmetric cryptography): is a cryptographic system that uses pairs of keys: **public keys**, and **private keys**.

The generation of such key pairs depends on cryptographic algorithms which are based on mathematical problems termed one-way functions.

If you encrypt with the **private** you need the **public** to decrypt
If you encrypt with the **public** you need the **private** to decrypt

Asymmetric

- Better key distribution
- Scalability
- Authentication and nonrepudiation
- Slow
- Mathematically intensive

Asymmetric /
Public & Private key

Symmetric

- Fast
- Strong

Asymmetric

- Better key distribution
- Scalability
- Authentication and nonrepudiation
- Slow
- Mathematically intensive

Asymmetric /
Public & Private key

Symmetric

- Fast
- Strong

- 1024-bit RSA keys are equivalent in strength to 80-bit symmetric keys
- 2048-bit RSA keys are equivalent in strength to 112-bit symmetric keys
- 3072-bit RSA keys are equivalent in strength to 128-bit symmetric keys
- 15360-bit RSA keys are equivalent in strength to 256-bit symmetric keys

INX
THE CYBER SECURITY COMPANY

Hash Function

- **Hash functions** are extremely useful and appear in almost all information security applications.
- **Hash function** is a mathematical function that converts a numerical input value into another compressed numerical value.

The input to the hash function is of arbitrary length but output is always of fixed length.

- **Hash function** is also used to identify what you have just downloaded to see if it is the

authentic one

⇒ This is called **Data Integrity Check**

Data integrity check is a most common application of the hash functions.

It is used to generate the checksums on data files. **This application provides assurance to the user about correctness of the data.**



Digital Signature

Digital signature: It is a mathematical scheme for **verifying the authenticity of digital messages or documents.**



So a hash value that has been encrypted with the sender or issue is private key. ⇒ That is a **digital signature**.

It provides authentication, repudiation and integrity.

And if you encrypt something and also provide a digital signature, then you're also going to get confidentiality along with authentication or repudiation and integrity.

Digital signatures ensure that the software or whatever it is that you've got came from that person or that publisher, and it protects that software or that message from alteration after it has been published or sent.

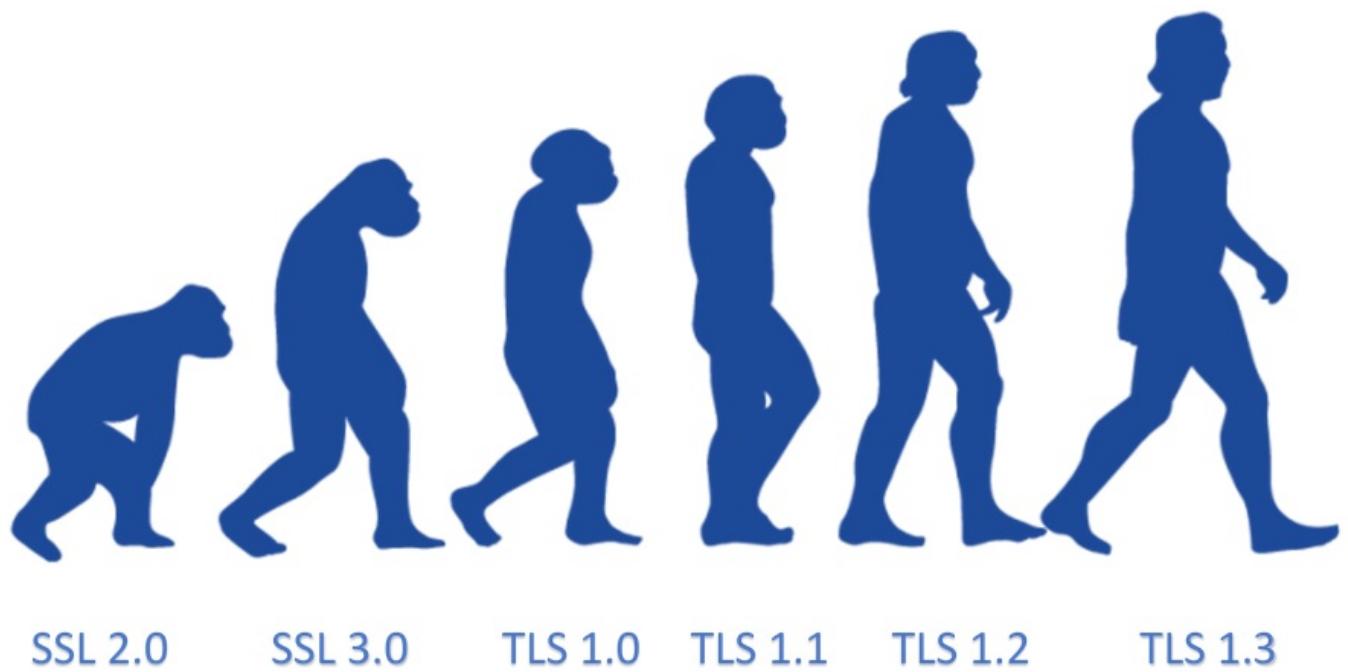
SSL - TLS

- **SSL** and **TLS** are both cryptographic protocols that provide authentication and data encryption between servers, machines, and applications operating over a network (e.g. a client connecting to a web server).
- **TLS** is way better and more secured'

TLS 1.1 came out seven years later in 2006, replaced by TLS 1.2 in 2008. That hurt TLS 1.1 adoption as many websites simply upgraded from 1.0 to TLS 1.2. We are now at TLS 1.3, which was finalized in 2018 after 11 years and nearly 30 IETF drafts.

TLS 1.3 makes significant improvements over its predecessors and right now major players around the internet are pushing for its proliferation. Microsoft, Apple, Google, Mozilla, and Cloudflare all announced plans to deprecate both TLS 1.0 and TLS 1.1 in January 2020, making TLS 1.2 and TLS 1.3 the only game in town.

At any rate, we've been using TLS for the past couple decades. At this point, if you're still using SSL you're years behind, metaphorically living in a forlorn era where people still use phone lines to dial on to the internet.



SSL Stripping

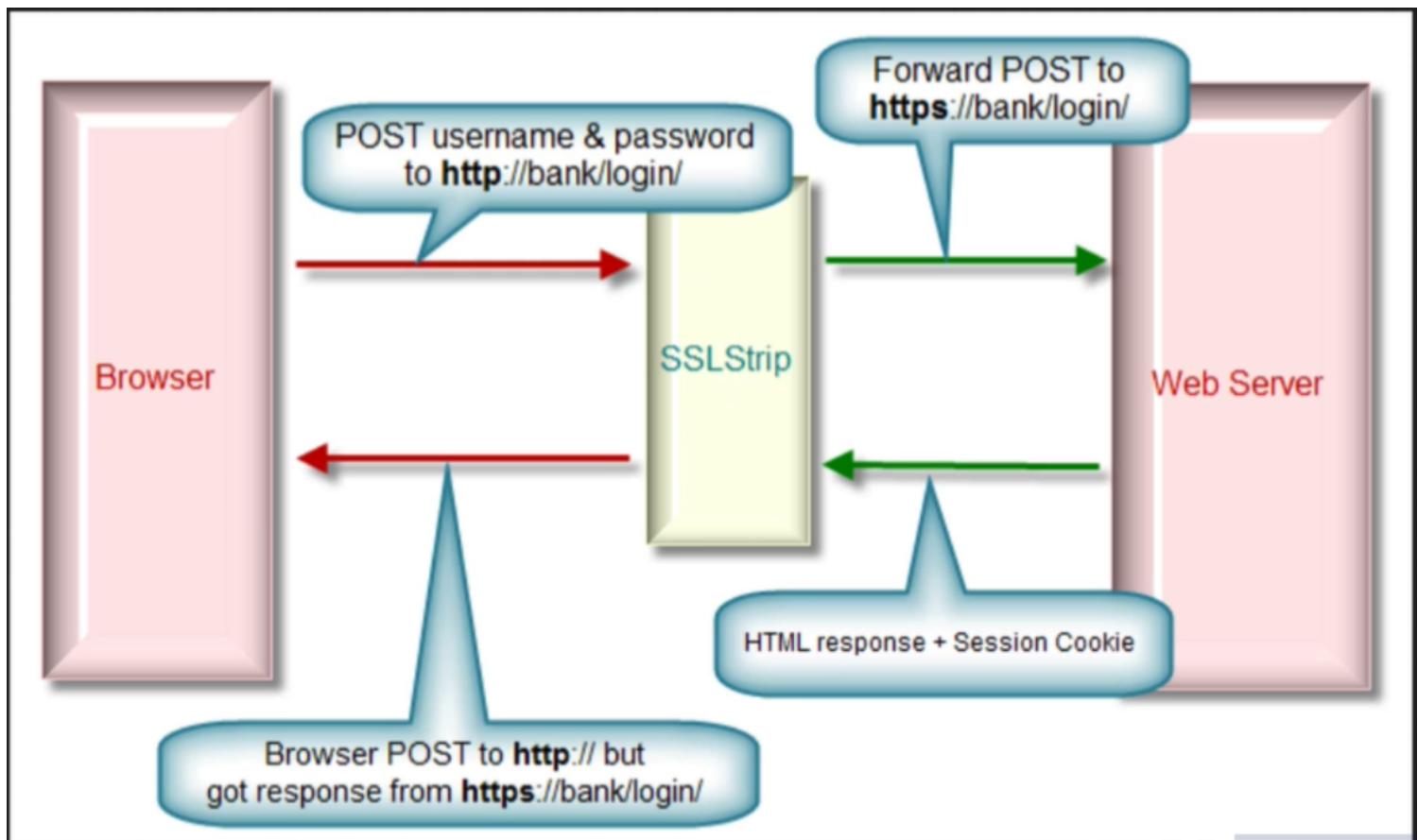
Explain: <https://www.https.in/ssl-security/how-ssl-strip-work/>

Tool: <https://shop.hak5.org/products/wifi-pineapple>

You take this to a airport or somewhere busy, switch it on, switch on an open network saying ⇒ **Free Wi-Fi** or something like that, and you'll be amazed at the **number of passwords** you'll get for Facebook and Google and **all the rest of the websites** by **stripping out the SSL**.

People just do not notice.

It's probably worth pointing out, actually, that **when you do strip SSL, it means the connection is no longer encrypted** and therefore you can see all of the content and therefore **you be able to steal usernames and passwords and just see everything that the person is actually doing.**



SSL Tool

Digital Certificate

A **digital certificate**, also known as a public key **certificate**, is used to cryptographically link ownership of a public key with the entity that owns it.

The screenshot shows the Mozilla Firefox 'Page Info' dialog for the URL support.mozilla.org. The left pane displays general information, media files, and permissions. The right pane is titled 'Certificate Hierarchy' and shows a tree structure of certificates, with the leaf node 'support.mozilla.org' highlighted by a red box. Below this is the 'Certificate Fields' section, which lists various X.509 fields. The 'Certificate Signature Algorithm' field is selected and highlighted with a blue background. The 'Field Value' section shows the value 'PKCS #1 SHA-256 With RSA Encryption'. Several fields in the certificate list are also highlighted with red boxes.

Website Identity

Website: support.mozilla.org

Owner: Mozilla Foundation

Verified by: DigiCert Inc

Privacy & History

Have I visited this website prior to today?

Is this website storing information on my computer?

Have I saved any passwords for this site?

Technical Details

Connection Encrypted (TLS_ECDHE_RSA)

The page you are viewing was encrypted with TLS_ECDHE_RSA. Encryption makes it difficult for others to intercept your communications with this computer. It is therefore unlikely that your connection will be monitored or tampered with.

Certificate Hierarchy

- DigiCert High Assurance EV Root CA
- DigiCert SHA2 Extended Validation Server CA
- support.mozilla.org

Certificate Fields

- Extended Key Usage
- CRL Distribution Points
- Certificate Policies
- Authority Information Access
- Certificate Basic Constraints
- Object Identifier (1 3 6 1 4 1 11129 2 4 2)
- Certificate Signature Algorithm**
- Certificate Signature Value

Field Value

PKCS #1 SHA-256 With RSA Encryption

Certificate Authorities and HTTPS

If someone can issue a fake certificate that your browser TROs, you'll have no idea that the HTTP can be intercepted and read.

The https that you associate within the URL will still be there.

The padlock will still appear as normal, the traffic will be sent encrypted as normal, and the certificate will look valid and everything will look fine.

⇒ Whoever issued the fake certificate can decrypt the traffic as they know the private key.

Mitigation

1. Stay anonymous

Another method is to be **anonymous** in the first place. So if you're concerned about somebody reading your traffic.

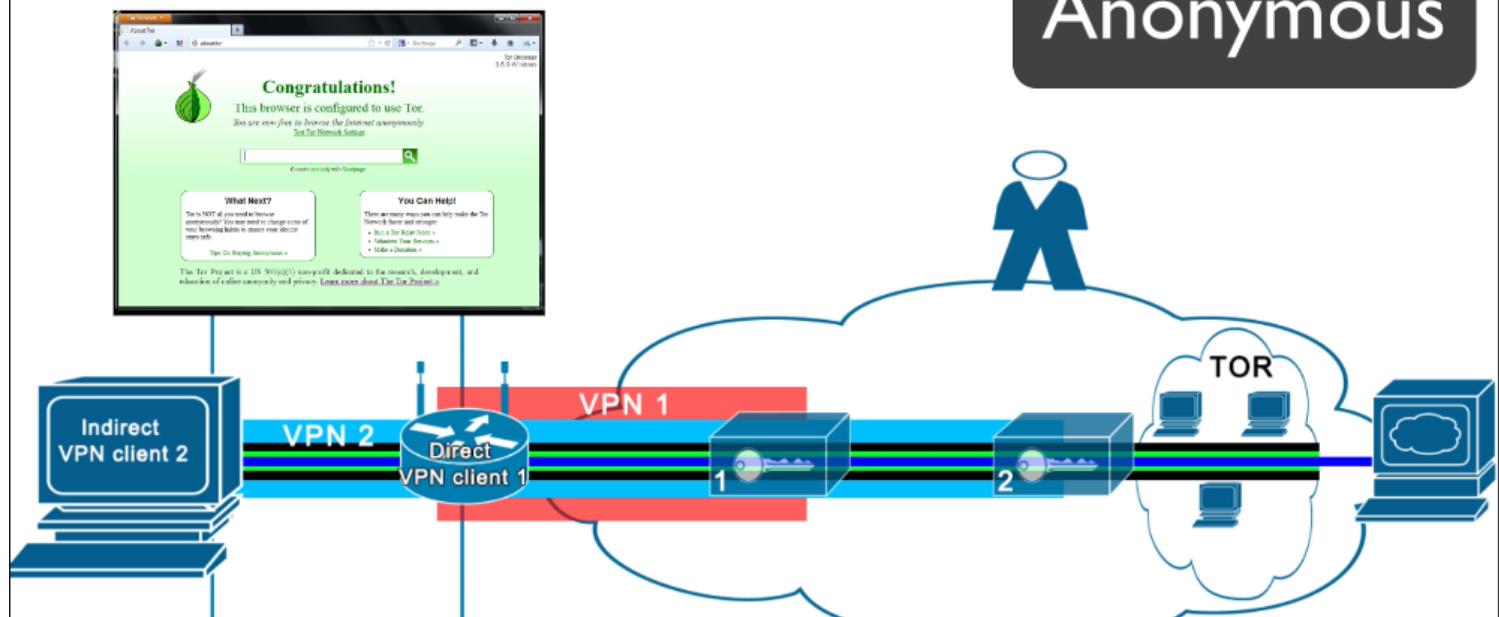
Then if you're **anonymous**, they won't be able to attribute that traffic to you even if they can read it, if this makes sense.

For example: If you are using an anonymizing method, so perhaps a VPN or Tor or something like that, if they then issue a fake certificate and are able to read it.

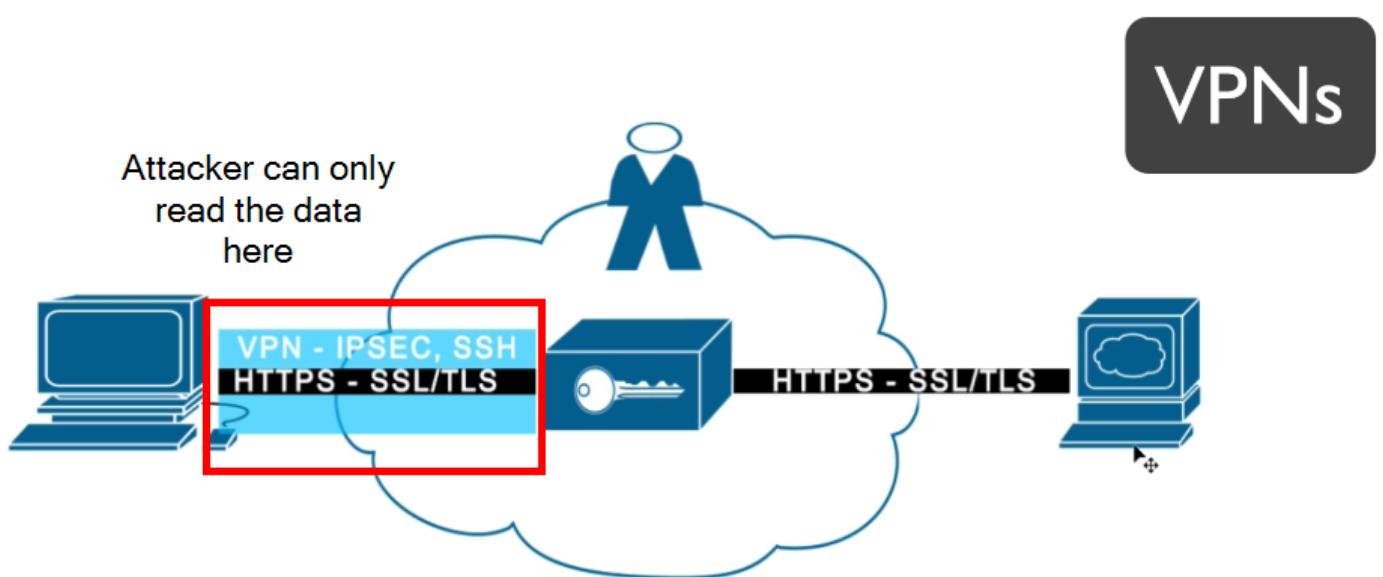
⇒ They may not then be able to associate that back to you to all depends on whether or not you care about them reading the data or you care about them associating that data to you.

Being anonymous is another method and you can also use VPN to.

Anonymous



2. VPNs



Now if you've got an **attacker** there is only able to get in the middle here is going to prevent them from being able to change the certificate.

⇒ If they can get to the traffic here and obviously they can change the certificate.

An example where this might be useful. So say you're in China and you care about the Chinese government swapping out a fake certificate. What you can do is you can VPN out of China and then connect to your server again, which will need to be out of China. And then you can more guarantee that your connection is end to end secure because you know that they've not been able to change the certificate while it's been in China. Now, if you want to connect to a server that's within the domain of influence of your threat agent and even a VPN can be a problem because once you break out of the VPN, then they can decrypt the traffic. So that certificate authorities and ISPs and the issues that you have with them, your main line of defense is to have defense in depth.



Một ví dụ mà điều này có thể hữu ích. Vì vậy, giả sử bạn đang ở Trung Quốc và bạn quan tâm đến việc chính phủ Trung Quốc đổi chứng chỉ giả. Những gì bạn có thể làm là bạn có thể VPN ra khỏi Trung Quốc và sau đó kết nối lại với máy chủ của bạn, máy chủ này sẽ cần phải ở ngoài Trung Quốc. Và sau đó, bạn có thể đảm bảo hơn rằng kết nối của bạn kết thúc để kết thúc an toàn vì bạn biết rằng họ không thể thay đổi chứng chỉ khi nó ở Trung Quốc. Bây giờ, nếu bạn muốn kết nối với một máy chủ nằm trong phạm vi ảnh hưởng của tác nhân đe dọa của bạn và thậm chí VPN có thể là một vấn đề vì một khi bạn thoát ra khỏi VPN, thì chúng có thể giải mã lưu lượng. Vì vậy, cơ quan cấp chứng chỉ và ISP cũng như các vấn đề mà bạn gặp phải với họ, tuyến phòng thủ chính của bạn là bảo vệ theo chiều sâu.



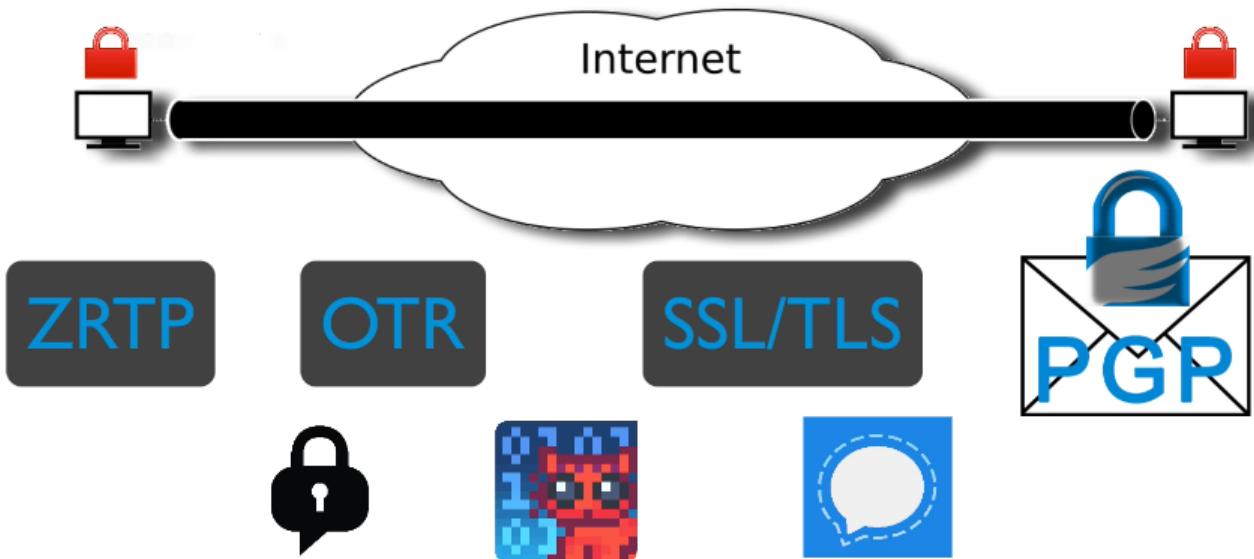
This is a desired form of encryption for data in transit, for maximum protection of the data if you wish to avoid tracking global mass surveillance, hackers and so on.

End-To-End Encryption

This is a desired form of encryption for data in transit, for maximum protection of the data
 ⇒ if you wish to avoid tracking global mass surveillance, hackers and so on.

If everyone used end to end encryption for all traffic, everyone's traffic would look the same when only some people use end to end encryption.

Those people that use into an encryption stand out as different and own encryption offers protection



End-to-End Encryption (E2EE)

STATION X
THE CYBER SECURITY COMPANY

Steganography

Tools: https://embeddedsw.net/OpenPuff_Steganography_Home.html

<https://www.spammimic.com/>

<http://www.jitc.com/Steganography/tools.html>

Steganography is the practice of concealing information or files within other non secret text or data.

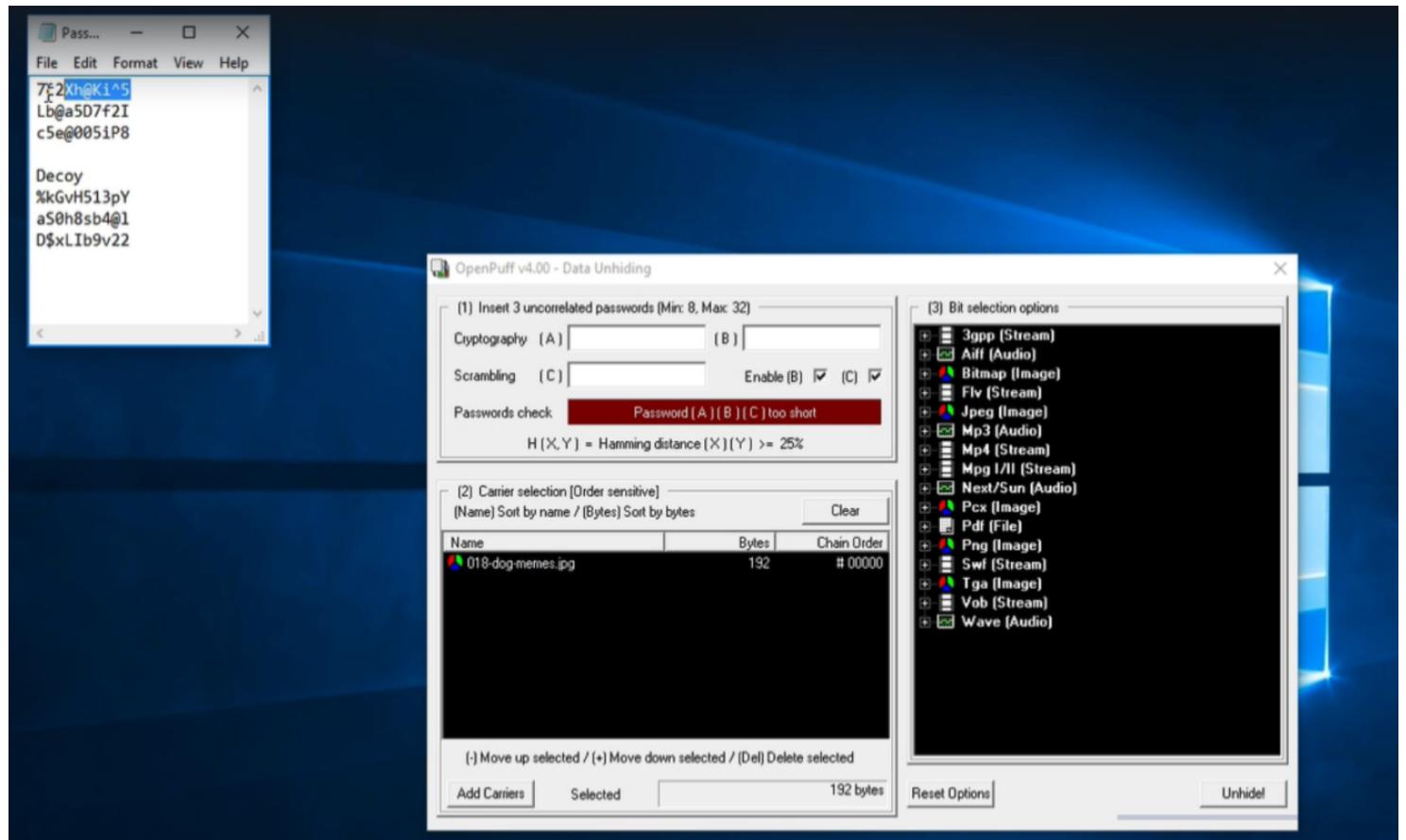
⇒ It is called hiding data in plain sight.

For example, hide a text file containing secret information within an image file.

⇒ If you use this, make sure to modify the carrier such images by resizing and photoshop it.

Because if you just do a quick search for something on the Internet, download that file because you want to use it as a carrier, somebody can then just do the same thing. They do a quick search, try to find it, use Google quite easy to find images using Google and Google images.

And they compare it and they can see that some changes have been made and to be able to see if it's steganography.



End in brief

Good encryption is often the strongest link as human beings are usually the weakest link in the section on OPSEC or operational security.

Human weaknesses in security and what to do to prevent them.

- ⇒ If you put lots of effort into your security **but missed something big**, like not patching your **browser** or using poor passwords,
- ⇒ You're just as insecure as if you had done nothing. **This is the problem.**

Make sure you mitigate your weakest links first before you concern yourself over detail.

Your **security engine** needs to be running first before you even attempt to tune the engine.

Section 5: Operating System Security & Privacy

- **The operating system** has full control of all actions on a device.

OS Security Features and Functionality

- **Window** - has the most security features and third party security applications available.
- **Mac OS** - has the least security features and third party security applications available.
- **Linux** (most secured system) - is where the security focus.
 - **Android** is a more open operating system, mean you're allowed to do more with it and you can do more with it, which is great. But this isn't good for security, though.
 - **iOS** is a closed system restricting what you can do so you can do less on it than you can on Android. But because it's a restricted operating system, a closed operating system. This is good for security.

Security Bugs and Vulnerabilities

- **Critical security vulnerabilities** would be something like a remote code execution bug

where you can remotely take over a device by sending a specially crafted packet or data.

CVE Details

The ultimate security vulnerability datasource

(e.g.: C

[Log In](#) [Register](#)

[Switch to https://](#)

[Home](#)

Browse :

[Vendors](#)

[Products](#)

[Vulnerabilities By Date](#)

[Vulnerabilities By Type](#)

Reports :

[CVSS Score Report](#)

[CVSS Score Distribution](#)

Search :

[Vendor Search](#)

[Product Search](#)

[Version Search](#)

CVSS Score Distribution For Top 50 Vendors By Total Number Of "Distinct" Vulnerabilities

	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities										Weighted Average
			0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+	
1	Microsoft	7800	2	105	563	220	1415	862	694	1789	25	2125	7.10
2	Oracle	7621	2	137	367	536	2308	2135	887	649	29	571	5.90
3	Google	6119	38	447	54	1634	618	1018	1186	34	1090		6.80
4	Debian	5203	68	274	135	1447	1066	999	961	14	239		6.20
5	IBM	5147	2	63	337	916	1386	979	516	529	26	393	5.80
6	Apple	5041	1	54	338	47	925	640	1381	728	15	912	6.80
7	Cisco	4020	2	6	87	167	881	877	541	949	41	469	6.70
8	Redhat	3922	62	313	169	1024	710	599	696	13	325		6.20

- **Security researchers** can get paid for finding security bugs called **bug bounties**, which incentivizes security researchers to look at specific products. And particularly, they're not going to be looking at open source products because they tend to not have bug bounties offering money.

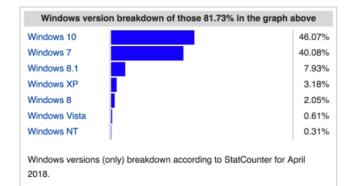
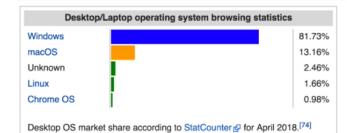
Usage Share

The **usage share of operating systems** is the percentage of computing devices that run each operating system (OS) at any particular time.

All such figures are necessarily estimates because data about operating system share is difficult to obtain;

→ there are few reliable primary sources – and no agreed methodologies for its collection.

Operating System Usage Statistics



- Cyber criminals, like any budding entrepreneur, wants to get the best return on investment in time and effort.

→ Therefore, it makes much more sense to target the largest demographic of users, which is **Windows**.

Generally, malware is written for a single type of operating system.

So because Windows still has the greatest market share, that's where they're going to aim.

That's where the money is.

Privacy & Tracking

- **Windows 10** is a cloud based operating system with cloud functionality like synchronization sharing.

- **Window 10** data synching is the default setting

→ This includes websites that are open your browsing history, software settings, Wi-Fi, hotspot names and passwords, etc..

- The sort of data you're going to have collected and shared with third parties if you read these documents here.

- So we're talking about your name, your email address, your postal address, phone number, passwords, password related information, account access information, teams that you might follow, stocks that you might be interested in, your favorite places and cities, your age, gender, preferred language, payment information such as credit cards, security codes, features you use, the items you purchase, the websites that you visit, the search terms that you enter, contacts in your relationships to them, location information.

Window 10 - Disable Tracking

- Before you install any privacy application.

→ So you have to think about trust.

→ Can you trust these people to have developed this software with your security and privacy in mind?

- If they are open source and you understand the language they are written in, you can verify the software.

This is why it's best to go with open source as a tool for this, because these are from untrusted sources.

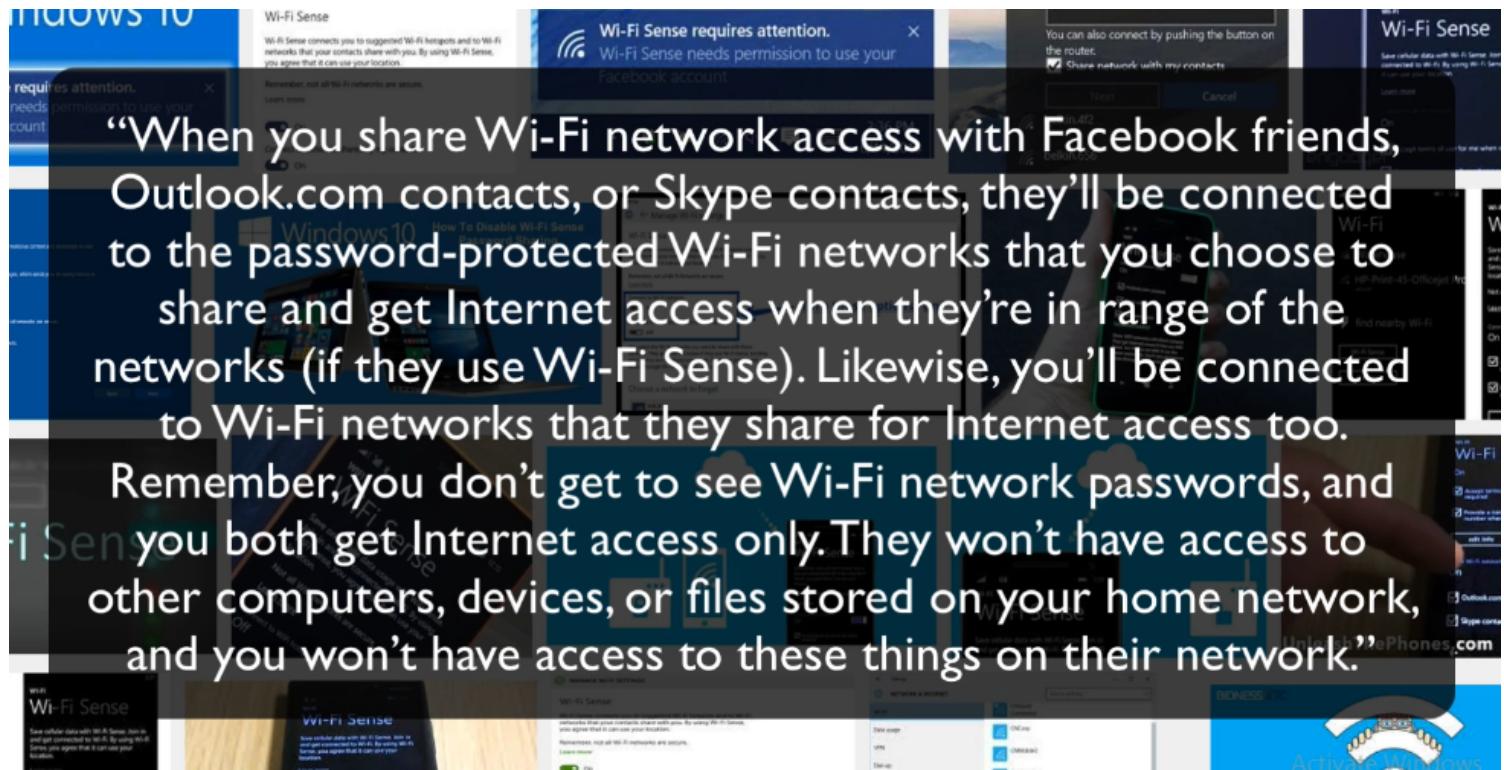
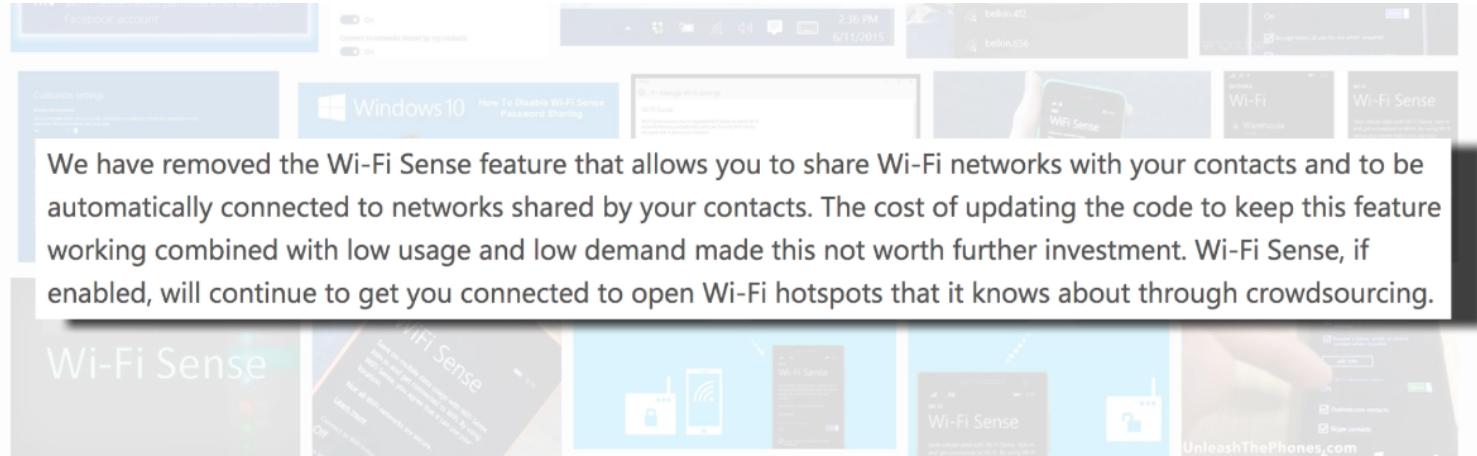
You have no idea who has written some of these and you don't know what extra bits of crap they put into them, which could be counter to your security or privacy, which is why I go with an open source option.

Tool

Privacy Setting

So Windows 10 assigns each instance of the operating system a unique advertising I.D. This is used to customize ads that are sent to you by third party companies such as ad networks and advertisers. So do not need that privacy issue.

WiFi Sense



Window 7 & 8 - 8.1 Privacy & Tracking

Operation System Choices

Linux and Unix

- **Subgraph:** <https://subgraph.com/sgos/>
- **Qubes OS:** <https://www.qubes-os.org/> (Recommended)
- **Hardended Gentoo Linux:** <https://wiki.gentoo.org/wiki/Project:Hardened>
- **Trisquel GNU/Linux :** <https://trisquel.info/>
- **PureOS:** <https://www.pureos.net/>
- **Astra Linux:** It's a Russian Linux based computer operating system developed to meet the needs of the Russian armed forces and intelligence agencies. <https://astralinux.ru/>
- **Security Enhancement SELinux:** <https://github.com/SELinuxProject>

Pure Security Focused OS

General Use OS

- **Windows**
 - Microsoft is fast to respond to fix security vulnerabilities, which is great.

- Security is okay.
- Privacy is okay.

If you trust Microsoft on the negative, they're not really good for anonymity.

That's not really what they're designed for. So don't use Tor on those platforms.

- **Mac OS**

- Apple's desktop and laptop operating system on the positive, it's easy to use and also good.

- Most malware and hackers are not targeting this platform because it's got a low market share.

- Apple is fast to respond also to fix security vulnerabilities, which is great, and there's moderate security features within the operating system itself.

- On the negative, there is a limited security software available for it, so you won't find much in the way of endpoint protection.

General Use OS with security and privacy

- **Debian** (For general use if security and privacy is priority)
- **Arch Linux**
- **OpenBSD**

Anonymity Focused OS

- **Tails**: is specifically resistant to local forensic examination, so no one will know what you've actually been doing on it once you finish using it.

- **Whonix:**

As you know, Unix implement security through isolation and Unix particularly has a focus on anonymity

X

Như bạn đã biết, Unix thực hiện bảo mật thông qua cách ly và Unix đặc biệt có tập trung vào ẩn danh



và ngăn chặn rò rỉ ra khỏi mạng Tor.

Vì vậy, nó tốt cho an ninh, quyền riêng tư và ẩn danh.

Nó không giảm thiểu chống lại kiểm tra pháp y địa phương, mặc dù

and preventing leaks out of the Tor network.

So it's good for security, privacy and anonymity.

It does not mitigate against local forensic examination, though.

Penetration Testing Focused OS

- **Kali Linux:** <https://www.kali.org/>
- **Parrot GNU/Linux:** <https://www.parrotsec.org/>
- **BlackArch Linux:** <https://blackarch.org/>
- **BackBox Linux:** <https://www.backbox.org/>
- **Pentoo:** <https://www.pentoo.ch/>

Mobile OS Security Focused

Android:

LineageOS: <https://lineageos.org/>

Section 6: Reducing Threat Privilege

- **Restricting privileges** is a standard approach in Linux and UNIX type operating systems

where the admin or root account is rarely used.

Administrative privileges is the default. You simply need to change your account in Windows to be a standard user and use an admin account just for when you need it.

This has surprisingly little administrative burden as you will be prompted for the admin privileges if and when you need them, which is mostly when you're installing applications.

This is a nice, easy win to lock down any attacker or attack, you have to train yourself not to blindly enter the admin password when requested, and question the reason you're being prompted for the admin username and password, and make sure that it is actually genuine.

Đặc quyền quản trị là mặc định. Bạn chỉ cần thay đổi tài khoản của mình trong Windows để trở thành người dùng tiêu chuẩn và sử dụng tài khoản quản trị chỉ khi bạn cần.

Điều này có ít gánh nặng quản trị đáng ngạc nhiên vì bạn sẽ được nhắc về các đặc quyền quản trị nếu và khi bạn cần, chủ yếu là khi bạn đang cài đặt ứng dụng.

Đây là một chiến thắng tuyệt vời, dễ dàng để khóa bất kỳ kẻ tấn công hoặc cuộc tấn công nào, bạn phải huấn luyện bản thân không nhập mật khẩu quản trị viên một cách mù quáng khi được yêu cầu và đặt câu hỏi lý do bạn được nhập tên người dùng và mật khẩu quản trị viên và đảm bảo rằng nó thực sự là chính hãng.

Window 10 - Not using admin

Section 7: Security Isolation

- Physical Security Domain:**

An example of a Physical Security Domain could be that you have one lock down physical machine or laptop, and the operating system and everything in it is configured in a certain way that gives you high security. And you have another physical machine or laptop, and that is for general use.

Một ví dụ về một miền bảo mật vật lý có thể là bạn có một khóa và máy tính xách tay, và hệ điều hành và mọi thứ trong đó được cấu hình theo một cách nhất định cho phép bạn bảo mật cao. Và bạn có một máy vật lý hoặc máy tính xách tay khác, và đó là để sử dụng chung.

- Virtual Security Domain:**

Not necessarily physical, but at least virtual. The level of security you need to maintain high privacy isn't practical for day to day use of the internet. Think about the type of Security Domains that you might want as you go through the course.

Domains you might have in extreme cases could be:

Work Domain, Personal, Banking

Temporary Domain: a Non-persistent Domain that is used temporarily and then it's destroyed, a High Privacy Domain.

All of these are possible in different ways with different techniques and not necessarily that onerous, depending on how you set them up.

Không nhất thiết phải vật lý, nhưng ít nhất là ảo. Mức độ bảo mật bạn cần duy trì quyền riêng tư cao không thực tế cho việc sử dụng Internet hàng ngày. Hãy nghĩ về loại tên miền bảo mật mà bạn có thể muốn khi bạn đi qua khóa học.

Tên miền bạn có thể có trong trường hợp cực đoan có thể là:

Tên miền làm việc, cá nhân, ngân hàng

Tên miền tạm thời: Một miền không bền bỉ được sử dụng tạm thời và sau đó nó bị phá hủy, một miền riêng tư cao.

Tất cả những cách này có thể theo các cách khác nhau với các kỹ thuật khác nhau và không nhất thiết phải có rất nhiều, tùy thuộc vào cách bạn thiết lập chúng.

For example: The network cards within physical devices have unique **MAC addresses** or **hardware addresses**.

If you purchase your secure laptop anonymously, then the MAC, if somebody is able to determine it, cannot be traced back to you.

There are ways to change your MAC address which we can cover if you're using a Virtual form of Security Domain.

To create separate domains you could do things like dual booting, you can use Platform virtualisation software and hypervisors, the likes of VMware, Virtualbox, Vagrant, Hyper-V, VPC. There's also Kernel Virtual Machine, there's Jails or BSD Jails, Zones, Linux Containers, Docker. You can also have hidden operating systems, VeraCrypt and TrueCrypt provide that functionality. You can have separate hard drive partitions that are encrypted and hidden. You can have things like Sandboxes. You can have portable apps. You can have non-persistent operating systems like Tails, Knoppix, Puppy Linux, JonDo Live, Tiny Core Linux. You can have bootable USBs. You can have operating systems that are dedicated to Isolation/Separation like Qubes, which is a very good operating system. So there are lots of ways to create Security Domains through Isolation and Separation.

Để tạo các tên miền riêng biệt, bạn có thể làm những việc như khởi động kép, bạn có thể sử dụng phần mềm áo hóa nền tảng và áo hóa, lượt thích của VMware, VirtualBox, VINGRANT, Hyper-V, VPC. Ngoài ra còn có máy ảo kernel, có tù hoặc nhà tù BSD, vùng, thùng chứa Linux, Docker. Bạn cũng có thể có các hệ điều hành ẩn, Veracrypt và TrueCrypt cung cấp chức năng đó. Bạn có thể có các phân vùng ổ cứng riêng biệt được mã hóa và ẩn. Bạn có thể có những thứ như hộp cát. Bạn có thể có ứng dụng di động. Bạn có thể có các hệ điều hành không bền bỉ như đuôi, Knoppix, Puppy Linux, Jondo Live, Tiny Core Linux. Bạn có thể có USBs có thể khởi động. Bạn có thể có các hệ điều hành dành riêng cho sự cô lập / tách như qubes, đó là một hệ điều hành rất tốt. Vì vậy, có rất nhiều cách để tạo các miền bảo mật thông qua cách ly và tách biệt.

Isolation and Compartmentalization

Isolation Physical and Hardware

So let's start with devices and their hardware serial numbers.

X

Vì vậy, hãy bắt đầu với các thiết bị và số seri phần cứng của chúng.

☆

So devices have hardware serial numbers that can uniquely identify them.

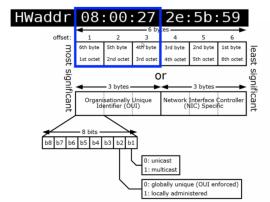
These unique identifiers can then possibly trace back to you through a money trail or potentially other methods, if the hardware wasn't bought anonymously.

Vì vậy, các thiết bị có số seri phần cứng có thể nhận dạng duy nhất chúng.

Sau đó, những số nhận dạng duy nhất này có thể truy ngược lại bạn thông qua đường dẫn tiền hoặc các phương pháp tiềm năng khác, nếu phần cứng không được mua ẩn danh.

If an adversary has access to your machine, they can view the unique MAC.

If they know the unique MAC, that can be potentially traced back to you through the purchasing of that device.



Change MAC addresses

Linux:

```
[root💀kali]-[~]
# sudo ifconfig eth0 down

[root💀kali]-[~]
# ifconfig
          STARK INDUSTRIES
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 12 bytes 640 (640.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 12 bytes 640 (640.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root💀kali]-[~]
# sudo macchanger -r eth0
Current MAC: 00:0c:29:ae:d6:8c (VMware, Inc.)
Permanent MAC: 00:0c:29:ae:d6:8c (VMware, Inc.)
New MAC: f6:5c:8d:01:48:8e (unknown)
```

```
[root💀kali]-[~]
# sudo ifconfig eth0 up

[root💀kali]-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.247.133 netmask 255.255.255.0 broadcast 192.168.247.255
        inet6 fe80::f45c:8dff:fe01:488e prefixlen 64 scopeid 0x20<link>
            ether f6:5c:8d:01:48:8e txqueuelen 1000 (Ethernet)
            RX packets 10 bytes 1732 (1.6 KiB)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 28 bytes 3234 (3.1 KiB)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
            RX packets 12 bytes 640 (640.0 B)
            RX errors 0 dropped 0 overruns 0 frame 0
            TX packets 12 bytes 640 (640.0 B)
            TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

But if you fear a knock at the door, you need to change the virtual MAC through the VM frequently.



Nhưng nếu bạn sợ có tiếng gõ cửa, bạn cần thay đổi MAC ảo thông qua VM thường xuyên.



You don't want a static MAC that ties you to a virtual machine even if it is just a virtual MAC address.

But the best option is to have anonymously purchased hardware like laptops, and network cards, and Wi-Fi, and network dongles; the devices that have MAC addresses.

You could purchase a whole bunch of cheap USB network adaptors and use a MAC changer in combination to mitigate the risk. This would be the best way of MAC mitigation: anonymous hardware plus MAC Changer.

Bạn không muốn một MAC tĩnh ràng buộc bạn với một máy ảo ngay cả khi nó chỉ là một địa chỉ MAC ảo.

Nhưng lựa chọn tốt nhất là có phần cứng được mua ẩn danh như máy tính xách tay, card mạng, Wi-Fi và thiết bị bảo vệ mạng; các thiết bị có địa chỉ MAC.

Bạn có thể mua cả đống bộ điều hợp mạng USB giá rẻ và kết hợp sử dụng bộ thay đổi MAC để giảm thiểu rủi ro. Đây sẽ là cách tốt nhất để giảm thiểu MAC: phần cứng ẩn danh cộng với MAC Changer.

Physical and Hardware Isolation

- So let's start with the CPUs. Almost all modern CPUs **do not** have a software readable serial number.

- **SMBIOS** contains serial numbers

Motherboards often, **but not always**, contain unique identifiers in the system management BiOS, SMBIOS memory.



Bo mạch chủ thường, nhưng không phải lúc nào cũng chứa các số nhận dạng duy nhất trong bộ nhớ quản lý hệ thống BiOS, SMBIOS.

And major OEMs typically have these serial numbers in the SMBIOS, which means an adversary could get access to this and tie it back to the purchaser or you.

In Windows, you can view the hardware information using the Windows Management Instrumentation tool, WMI.
So malware could pretty much do exactly the same.

Và các OEM chính thường có những số sê-ri này trong SMBIOS, có nghĩa là kẻ thù có thể truy cập vào số này và buộc nó lại với người mua hoặc bạn.

Trong Windows, bạn có thể xem thông tin phần cứng bằng công cụ Windows Management Instrumentation, WMI.
Vì vậy, phần mềm độc hại có thể hoạt động giống hệt như vậy.

- This will tell you the name of your BiOS current version and its serial number if there is any.
- This command tells you the system **motherboard name**, **number**, and **its UUID**.

- Motherboard

```

Administrator: C:\Windows\System32\cmd.exe

C:\Users\john\Downloads\demo>wmic bios get name,serialnumber,version
Name                               SerialNumber
Version
PhoenixBIOS 4.0 Release 6.0  VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b d6 70 a
INTEL - 6040000

C:\Users\john\Downloads\demo>wmic csproduct get name,identifyingnumber,uuid
IdentifyingNumber                   Name
Name
VMware-56 4d 0d 76 1a 2b 5a 0c-05 87 de ed 7b d6 70 ab  VMware Virtual Platform 7
4D56-2B1A-0C5A-0587-DEED7BD670AB

C:\Users\john\Downloads\demo>

```

- Hard Drive serial

```

Administrator: C:\Windows\System32\cmd.exe
          Name           NeedsCleaning  NumberOfMediaSupported Partition
s PNPDeviceID          PowerManagement          PowerManagement
abilities PowerManagementSupported SCSIBus SCSILogicalUnit SCSIPort SCSITarget
d SectorsPerTrack SerialNumber Signature Size Status StatusInfo Sys
CreationClassName SystemName   TotalCylinders TotalHeads TotalSectors Total
acks TracksPerCylinder
      512           {3, 4}      {"Random Access", "Supports Writing"} 0
ware, VMware Virtual S SCSI Disk Device
ALSE                         Win32_DiskDrive
LDRIVE0
          SCSI           (Standard disk drives)
      TRUE     Fixed hard disk media
CSI Disk Device  \\.\PHYSICALDRIVE0
      SCSI\DISK&VEN_VMWARE_&PROD_VMWARE_VIRTUAL_S\5&22BE343F&0&000000
      0           0           2           0
      63           -595924089  64420392960  OK
ComputerSystem    WIN-RGCA7VEP057  7832           255           125821080  1997
      255

C:\Users\john\Downloads\demo>wmic diskdrive get serialnumber
SerialNumber
Hard Drive

```

Linux:

Note

This means if you're using, say, Windows or Mac OSX, Microsoft and Apple are aware of your unique hardware IDs, and specifically, usually the motherboard ID is tied to the license in some way. So if you're using Windows or Mac OSX or other operating systems you have purchased and are attempting to be anonymous and your hardware ID is compromised, whoever you purchased it from could link the device back to you. Your adversary may have the power to get this information from the seller. And it's not just operating systems. Also applications can be aware of your hardware serial numbers, which again, through a money trail can be tied back to you.

The next mitigation is to have anonymously purchased the devices that you use. This will mitigate the risk of an adversary deanonymizing you as there is no money trail. Another strong mitigation is using virtual machines for isolation and compartmentalization. Virtual machines have different physical machine IDs and there is no traceable connection to the real physical machine's unique hardware IDs unless there is a breakout to the host, which is unlikely.



Giảm nhẹ tiếp theo là đã mua ẩn danh các thiết bị mà bạn sử dụng. Điều này sẽ giảm thiểu rủi ro bị đối thủ đánh lừa bạn vì không có dấu vết tiền bạc. Một biện pháp giảm thiểu mạnh mẽ khác là sử dụng các máy ảo để cô lập và ngăn cách. Máy ảo có các ID máy vật lý khác nhau và không có kết nối có thể theo dõi được với ID phần cứng duy nhất của máy vật lý thực trừ khi có sự cố đối với máy chủ, điều này khó xảy ra.



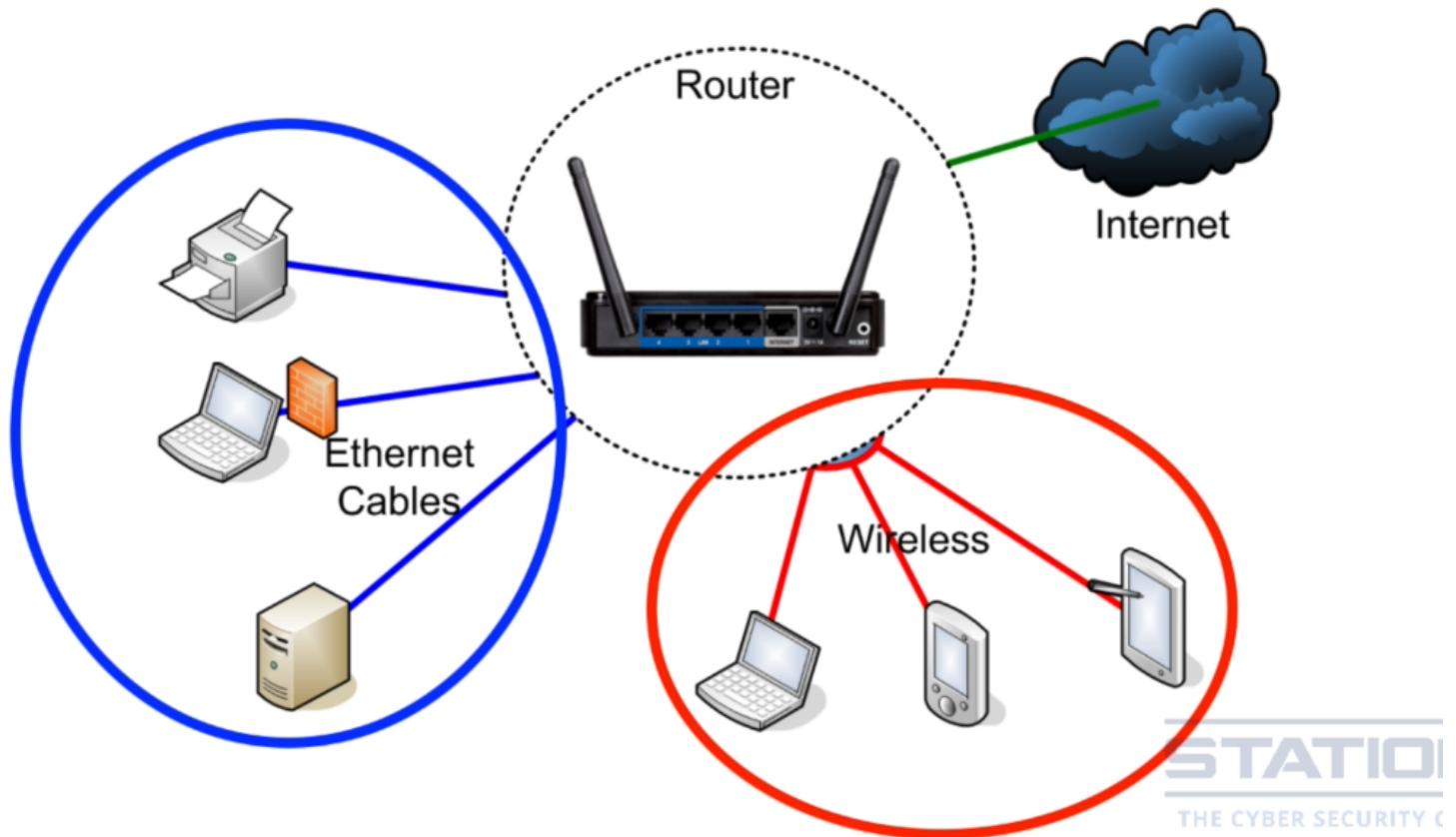
You can store your files, emails, and data physically separate, maybe on an external USB drive, a DVD, or in the Cloud, out of the sphere of influence of your adversary. Law enforcement agencies are having particular problems getting access physically to remote content out of their jurisdiction. You can use security tokens, hardware security modules, and store encryption keys separately. Nitrokey is an example of something you can use to do that. YubiKey is also an example. We'll discuss more on these later. You can store backups offsite for physical isolation. You can do network isolation, separating trusted devices and untrusted devices using LANs, VLANs, utilizing routers, switches and firewalls.



Bạn có thể lưu trữ các tệp, email và dữ liệu của mình riêng biệt về mặt vật lý, có thể trên ổ USB bên ngoài, DVD hoặc trong Đám mây, ngoài phạm vi ảnh hưởng của đối thủ. Các cơ quan thực thi pháp luật đang gặp những vấn đề đặc biệt trong việc truy cập thực tế vào nội dung từ xa ngoài quyền tài phán của họ. Bạn có thể sử dụng mã thông báo bảo mật, mô-đun bảo mật phần cứng và lưu trữ khóa mã hóa riêng biệt. Nitrokey là một ví dụ về một cái gì đó bạn có thể sử dụng để làm điều đó. YubiKey cũng là một ví dụ. Chúng ta sẽ thảo luận thêm về những điều này sau. Bạn có thể lưu trữ các bản sao lưu ngoại vi để cách ly vật lý. Bạn có thể thực hiện cách ly mạng, tách thiết bị đáng tin cậy và thiết bị không đáng tin cậy bằng mạng LAN, VLAN, sử dụng bộ định tuyến, thiết bị chuyển mạch và tường lửa.



- Isolation and compartmentalization can extend to anything physical to create layers of defenses.



STATION
THE CYBER SECURITY C

Virtual Isolation

Portable App

About Portable App:

If you're not familiar, portable apps are standalone applications. They are self contained and don't require an installation.

When you install an application, such as a browser, the application files are stored in various locations over the file system, and changes are made to the registry. With portable apps, all changes are contained to a single folder or file, making the application portable.

So you can literally copy it, paste it somewhere else, and it'll still work. That's not the case with installed applications.

Nếu bạn không quen, các ứng dụng di động là các ứng dụng độc lập. **Chúng hoạt động độc lập và không yêu cầu cài đặt.**

Khi bạn cài đặt một ứng dụng, chẳng hạn như một trình duyệt, các tệp ứng dụng được lưu trữ ở nhiều vị trí khác nhau trên hệ thống tệp và các thay đổi được thực hiện đối với sổ đăng ký. Với ứng dụng di động, tất cả các thay đổi được chứa trong một thư mục hoặc tệp duy nhất, làm cho ứng dụng có thể di động.

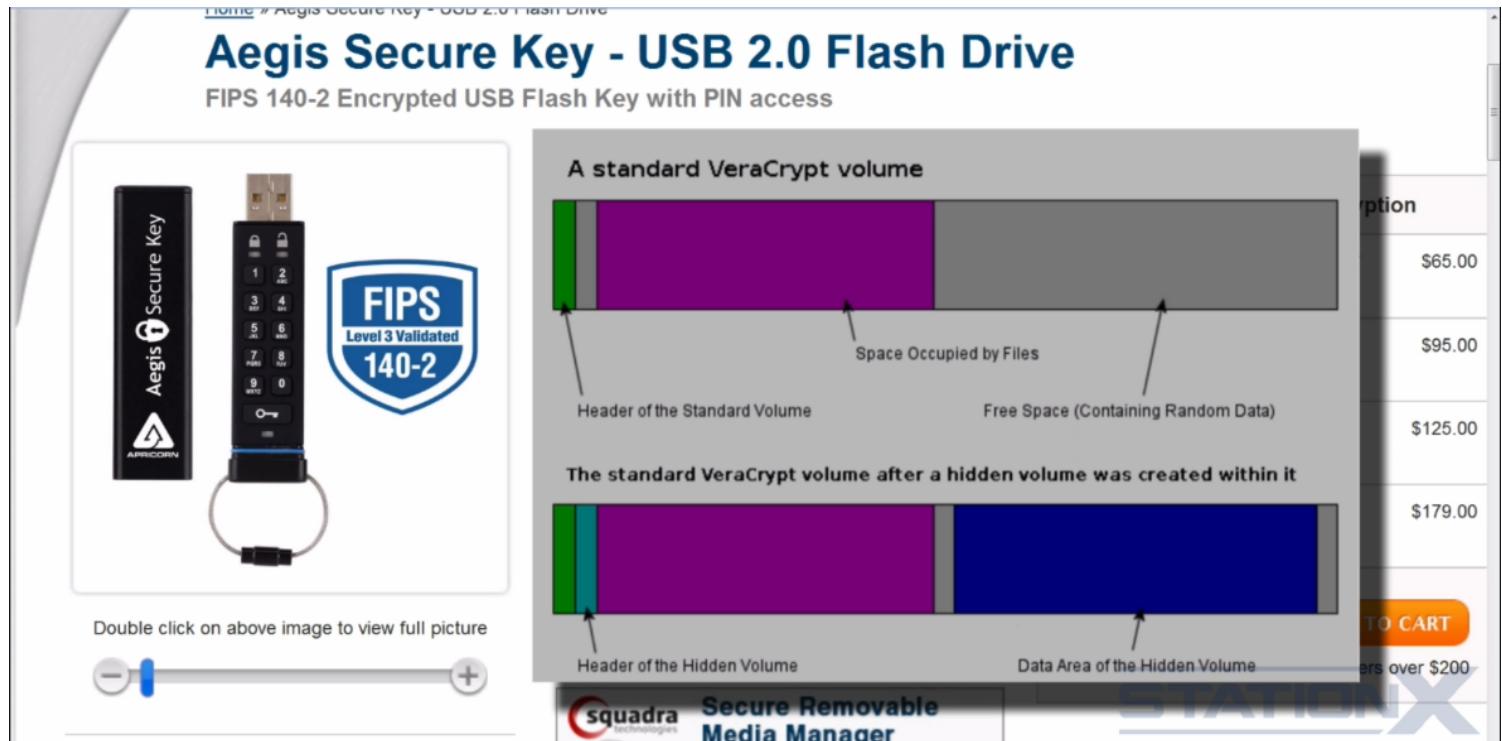
Vì vậy, bạn có thể sao chép nó theo đúng nghĩa đen, dán nó vào một nơi khác và nó sẽ vẫn hoạt động. Đó không phải là trường hợp với các ứng dụng đã cài đặt.

So let's imagine we're using Firefox as a web browser. Data related to the browser history is contained within the portable app. This makes evidence concealment and elimination easier. The application could be placed on a physically secure device, like an encrypted USB such as this one, so that it can be moved, it can be hidden, it can be destroyed. The application can be placed on an encrypted volume or even a hidden encrypted volume. This means that unless it's unencrypted, the application's data is inaccessible. The application could be placed on both a physically secured device like this one, and within this device, put on an encrypted hidden volume making a pretty stealthy app with its data self-contained.

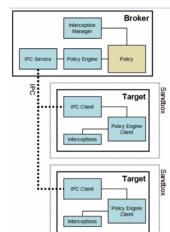
X

Vì vậy, hãy tưởng tượng chúng ta đang sử dụng Firefox làm trình duyệt web. Dữ liệu liên quan đến lịch sử trình duyệt được chứa trong ứng dụng di động. Điều này giúp cho việc che giấu và loại bỏ bằng chứng trở nên dễ dàng hơn. Ứng dụng có thể được đặt trên một thiết bị an toàn vật lý, chẳng hạn như một USB được mã hóa chẳng hạn như thiết bị này, để có thể di chuyển, có thể ẩn, có thể hủy. Ứng dụng có thể được đặt trên một ổ đĩa được mã hóa hoặc thậm chí là một ổ đĩa được mã hóa ẩn. Điều này có nghĩa là trừ khi nó không được mã hóa, dữ liệu của ứng dụng sẽ không thể truy cập được. Ứng dụng có thể được đặt trên cả thiết bị được bảo mật vật lý như thiết bị này và trong thiết bị này, đặt trên một ổ đĩa ẩn được mã hóa tạo thành một ứng dụng khai lén lút với dữ liệu của nó được giữ kín.

→ Use encrypted USB with portable browser could conceal and elimination easier.



Built-in SandBoxes



Sandbox là một kỹ thuật quan trọng trong lĩnh vực bảo mật có tác dụng cô lập các ứng dụng, ngăn chặn các phần mềm độc hại để chúng không thể làm hỏng hệ thống máy tính, hay cài các mã độc nhằm ăn cắp thông tin cá nhân của bạn.

Ví dụ:

Cho vai trò của **Sandbox** chính là trình duyệt web mà bạn sử dụng hàng ngày. Các trang web mà bạn truy cập đều được chạy trong môi trường Sandbox.

Website sẽ bị hạn chế và chỉ được chạy trong trình duyệt cũng như chỉ được can thiệp vào một phần nhỏ trong tài nguyên hệ thống.

Chúng không được phép sử dụng webcam cũng như không thể truy cập được vào các dữ liệu trên máy nếu như bạn không cho phép.

Nếu như các trang web không bị giới hạn trong môi trường Sandbox này, thì khi bạn lỡ truy cập vào các website chứa mã độc, nguy cơ máy tính của bạn bị tấn công là rất cao.

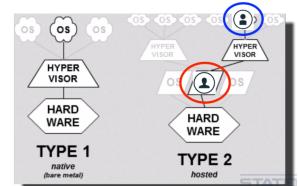
<https://sandboxie-plus.com/downloads/>

Window Sandbox

Linux

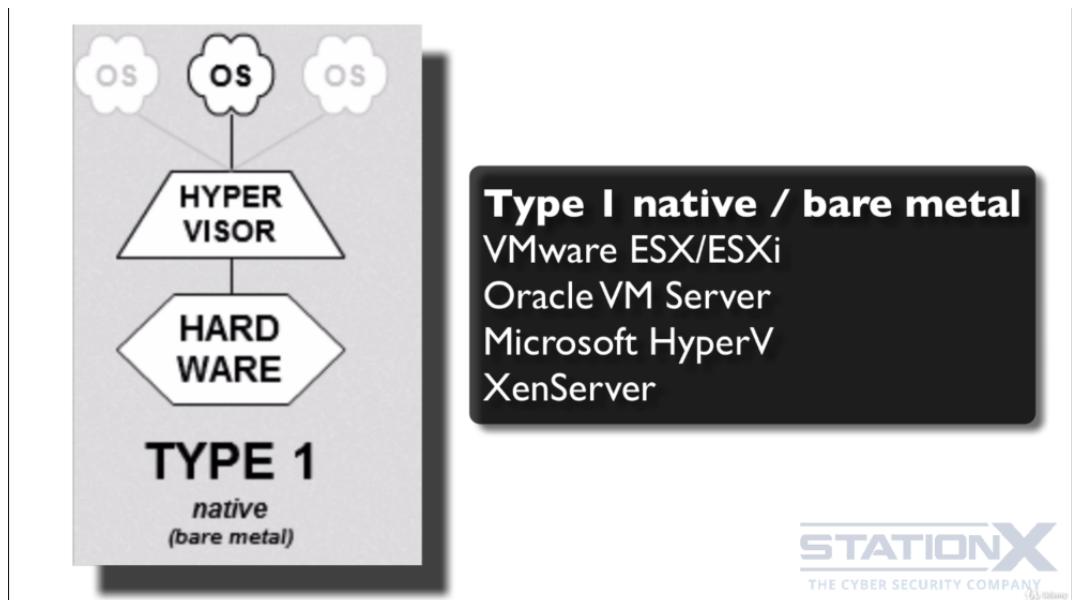
<https://linux.die.net/man/8/sandbox>

Virtual Machines



Type 1 (Hypervisor): Now there's the **Type 1** native hypervisors, also called bare metal hypervisors.

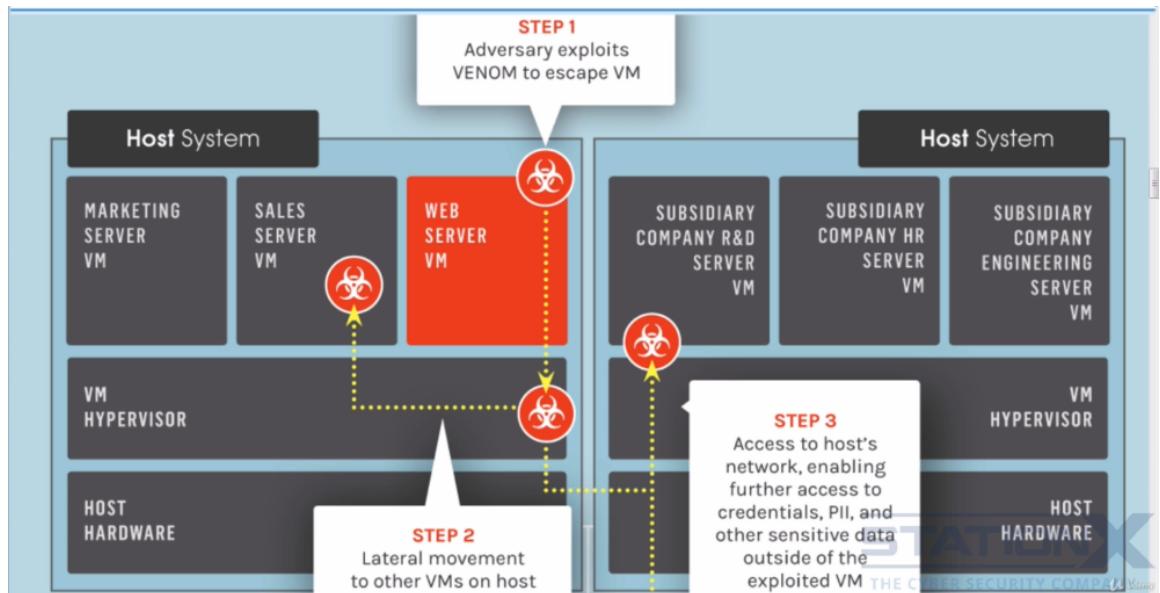
- There is no host operating system.
- The **hypervisor** is really the host operating system.



Weaknesses

- Virtual machines and sandboxes are based on the same principles.
So if we have a host and a guest, if the host is compromised
then it's possible that the guest could be compromised.

- A guest VM could compromise the host operating system or other VMs due to vulnerabilities and configuration settings.
- For vulnerable hypervisors, it allows an attacker to escape from the confines of a vulnerable virtual machine guest, which we call a virtual machine escape, and potentially obtain code execution access to the host.



VMs are used by security researchers to deliberately isolate malware, so that the malware can be forensically examined and reversed engineered in order to understand how the malware works. Because of this, advanced malware writers have designed counter measures that can detect when their malware is running on a virtual system, in an attempt to prevent that very same reverse engineering. The more sophisticated malware examines the memory, the file system, the registry, running processes for virtual machine environment artifacts, and looks for VM specific virtual hardware and processor instructions. It's relatively trivial to detect, if you're running in a virtual machine.



Các máy ảo được các nghiên cứu bảo mật sử dụng để cô lập phần mềm độc hại một cách có chủ ý, để phần mềm độc hại có thể được kiểm tra trước và đảo ngược thiết kế để hiểu cách thức hoạt động của phần mềm độc hại. Do đó, những người viết phần mềm độc hại tiên tiến đã thiết kế các biện pháp chống lại có thể phát hiện khi nào phần mềm độc hại của họ đang chạy trên một hệ thống ảo, nhằm ngăn chặn kỹ thuật đảo ngược giống hệt như vậy. Phần mềm độc hại phức tạp hơn kiểm tra bộ nhớ, hệ thống tệp, sổ đăng ký, các quy trình đang chạy cho các tạo tác môi trường máy ảo và tìm kiếm các hướng dẫn bộ xử lý và phần cứng ảo cụ thể của VM. Việc phát hiện tương đối nhỏ nếu bạn đang chạy trong một máy ảo.



• Shared Network

Shared networks are also an attack vector. If the guests and hosts share the same network, if any of those machines are compromised, the other machines could be targets for attack. Not technically escaping the virtual machine, but just simply by performing network attacks on the other machines that are part of the same network. In most instances, if you are using VirtualBox on your laptop, the host and guest will share the same network.



Mạng dùng chung cũng là một vector tấn công. Nếu khách và máy chủ chia sẻ cùng một mạng, nếu bất kỳ máy nào trong số đó bị xâm phạm, các máy khác có thể trở thành mục tiêu tấn công. Về mặt kỹ thuật, không phải thoát khỏi máy ảo, mà chỉ đơn giản bằng cách thực hiện các cuộc tấn công mạng trên các máy khác nằm trong cùng một mạng. Trong hầu hết các trường hợp, nếu bạn đang sử dụng VirtualBox trên máy tính xách tay của mình, máy chủ và khách sẽ chia sẻ cùng một mạng.



• Shared CPUs

VM hosts and guests obviously shares CPUs. This means it's theoretically possible to perform what is called covert timing channel attacks. This is the passing of information in which one process signals information to another process by modulating its own use of system resources. For example, central processing unit, time, in such a way that this manipulation affects the real response time observed by the second process. This means guest and host can communicate via timing variations based on prearranged methods. A timing channel is one example of a covert channel.

X

Máy chủ VM và khách rõ ràng dùng chung CPU. Điều này có nghĩa là về mặt lý thuyết, có thể thực hiện những gì được gọi là tấn công khen thời gian bí mật. Đây là quá trình truyền thông tin trong đó một quá trình báo hiệu thông tin cho một quá trình khác bằng cách điều chỉnh việc sử dụng tài nguyên hệ thống của chính nó. Ví dụ, đơn vị xử lý trung tâm, thời gian, theo cách mà thao tác này ảnh hưởng đến thời gian phản hồi thực được quan sát bởi quá trình thứ hai. Điều này có nghĩa là khách và chủ nhà có thể giao tiếp thông qua các biến thể về thời gian dựa trên các phương pháp được sắp xếp trước. Kênh thời gian là một ví dụ về kênh bí mật.

☆

- Features like shared folders, clipboard access and drag and drop functionality, all reduce the isolation and allow attack vectors.

Anything you allow the guest to access, for convenience, is a trade off with security.

The guest can then possibly view your files and copy and paste the contents of the clipboard.

Hardening (Improving Security)

Using a USB network dongle instead of the host network adapter, as discussed already in the area on physical isolation.

You can place the VM on a separate network to the host or for virtual isolation via a VLAN. This is to help mitigate attacks that come from the network, from the virtual machines.

- To protecting the data within the virtual machine. You can enable encryption using the hypervisor for each of the individual virtual machines, but obviously again this only protects them when they are switched off.

Using the hypervisor's encryption is probably a less tried and tested solution than encrypting the operating system itself

using more well-known encryption technology such as **LUKS, FileVault 2, BitLocker, and VeraCrypt**



- You might want to disable the audio and the microphone, and not specific to virtual machines.
- You might want to cover your webcam with tape.
- Disable shared folders.
- Disable drag and drop and clipboard.
- Don't enable video acceleration, 3D acceleration.
- Do not enable serial ports.
- If you can, do not install VirtualBox Guest Addition or VMWare Tools or equivalent.

Disable the USB controller which is enabled by default.

Do not enable remote display server

Don't add virtual storage when setting up the virtual machine.

- **Snapshot feature**

You can use VMware snapshots to create non-persistence. You can use these snapshots for security for evidence elimination by establishing a securely updated virtual machine that has never performed any other activity than what you want it to have performed and then snapshot that VM. So for example, here would be the clean VM with no evidence and no history. This is your current state where you perform your activities, then after you've performed your activities you restore back to the original clean VM. This'll remove any malicious malware, it'll remove history, tracking, or any evidence of activity. This is not a perfect solution to remove evidence due to the previously discussed possibilities of data leakage remaining on the host, but it is a reasonably good solution for basic non-persistence.

Bạn có thể sử dụng ảnh chụp nhanh của VMware để tạo sự không bền bỉ. Bạn có thể sử dụng các ảnh chụp nhanh này để bảo mật nhằm loại bỏ bằng chứng bằng cách thiết lập một máy ảo được cập nhật an toàn chưa bao giờ thực hiện bất kỳ hoạt động nào khác với những gì bạn muốn nó đã thực hiện và sau đó chụp nhanh máy ảo đó. Vì vậy, ví dụ, đây sẽ là máy ảo sạch không có bằng chứng và không có lịch sử. Đây là trạng thái hiện tại của bạn, nơi bạn thực hiện các hoạt động của mình, sau đó sau khi thực hiện các hoạt động của mình, bạn sẽ khôi phục lại máy ảo sạch ban đầu. Thao tác này sẽ xóa mọi phần mềm độc hại nguy hiểm, xóa lịch sử, theo dõi hoặc bất kỳ bằng chứng nào về hoạt động. Đây không phải là một giải pháp hoàn hảo để xóa bằng chứng do khả năng rõ rỉ dữ liệu đã được thảo luận trước đó còn lại trên máy chủ, nhưng nó là một giải pháp hợp lý tốt cho các trường hợp không bền bỉ cơ bản.

• Encryption keys

- If you pause or suspend your device when you have an encrypted virtual machine, the encryption keys are stored on the hard disk. (**This is vulnerable**)
- If you put your laptop into sleep or standby, any whole disk encryption keys will be stored in memory.
- ⇒ **Solution:** If you're using encryption, either with a hypervisor or with a guest operating system, or with a host operating system, it is best for all of the operating systems, the guest and the host, to be logged out and shut down and switched off, fully switched off, not paused, not suspended, not hibernated. This way, the decryption keys are not stored on disk anywhere.

Whonix OS - Anonymous OS

- **Whonix** is a free open source operating system that's focused specifically on anonymity, privacy, and security.
 - It will help you hide your internet service provider assigned IP address,
 - It will prevent your ISP from spying on you.
 - It can prevent websites from identifying you.

- It can prevent malware from identifying you.
- It can help you circumvent censorship.

> **Gateway:** The gateway's role is to enforce the TOR connection, this is the network isolation.

The workstation cannot tell what its real IP address is, so neither can an adversary who may have happened to hack the workstation via say a browser hack or a phishing attack.

⇒ Which is why they say leaks are impossible in Whonix and malware with even root privileges cannot find out the user's real IP address

this is the isolation principle.

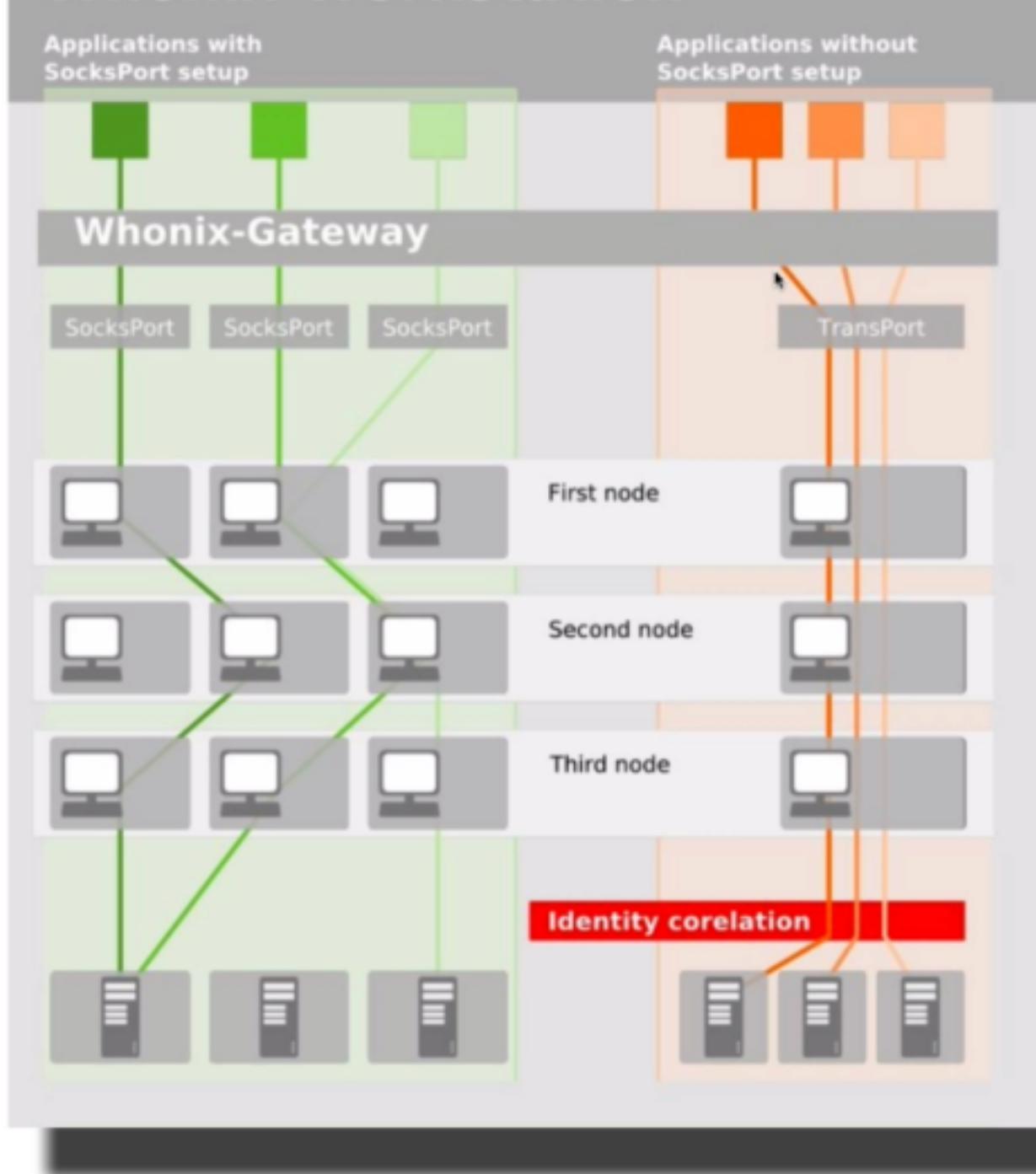
TOR requires an accurate time or it will fail to work. Establishing the correct time using standard methods such as an unauthenticated NTP is a potential deanonymizer, so Whonix has to use another method. Whonix uses something called SDW date and this is it now running in order to try and establish the time. When Whonix starts, if it doesn't believe it has the correct time, it will automatically start time sync and as it says here, don't use the internet until time sync has been successful.



TOR yêu cầu thời gian chính xác nếu không sẽ không hoạt động. Việc thiết lập thời gian chính xác bằng cách sử dụng các phương pháp tiêu chuẩn chẳng hạn như NTP chưa được xác thực là một phương pháp ẩn danh tiềm năng, vì vậy Whonix phải sử dụng một phương pháp khác. Whonix sử dụng một thứ gọi là ngày SDW và đây là ngày nó đang chạy để thử và thiết lập thời gian. Khi Whonix khởi động, nếu nó không tin rằng nó có thời gian chính xác, nó sẽ tự động bắt đầu đồng bộ thời gian và như nó nói ở đây, không sử dụng internet cho đến khi đồng bộ thời gian thành công.



Whonix-Workstation



Section 8: Security Bugs and Vulnerabilities

The importance of patching

Updates & Patching

1. Directly interface with the Internet – Browsers (e.g Opera, Edge, Firefox, Chrome etc.) browser extensions & plugins (e.g. Java, Flash, Silverlight etc), email applications (e.g. Outlook, Thunderbird etc)

2. Applications that use, play, view any sort of downloaded file – e.g. Windows Media player, Adobe Reader, Image viewer, Excel, Word etc.

3. Operating System - e.g. OS X, Windows 7, 8.x, 10, Android

The screenshot shows a Microsoft Security Bulletin page with a table titled "Microsoft Windows – Table 1 of 2". The table lists vulnerabilities for Windows Vista across different editions and service packs. The columns include: Operating System, OpenType Font Parsing Vulnerability – CVE-2015-2506, Font Driver Elevation of Privilege Vulnerability – CVE-2015-2507, Font Driver Elevation of Privilege Vulnerability – CVE-2015-2508, Graphics Component Buffer Overflow Vulnerability – CVE-2015-2510, Win32k Memory Corruption Elevation of Privilege Vulnerability – CVE-2015-2511, and Updates Replaced*. The table shows various severity levels (Important, Not applicable, Critical) and replacement patches (e.g., 3079904 in MS15-078, 2957503 in MS14-036). A large callout box highlights the term "KB = Patch number" pointing to the first row. Another callout box highlights the term "CVE = Vulnerability number" pointing to the second column.

Operating System	OpenType Font Parsing Vulnerability – CVE-2015-2506	Font Driver Elevation of Privilege Vulnerability – CVE-2015-2507	Font Driver Elevation of Privilege Vulnerability – CVE-2015-2508	Graphics Component Buffer Overflow Vulnerability – CVE-2015-2510	Win32k Memory Corruption Elevation of Privilege Vulnerability – CVE-2015-2511	Updates Replaced*
Windows Vista						
Windows Vista Service Pack 2 (3087039)	Important Elevation of Privilege	Important Elevation of Privilege	Not applicable	Not applicable	Important Elevation of Privilege	3079904 in MS15-078
Windows Vista Service Pack 2 (3087135)	Not applicable	Not applicable	Not applicable	Critical Remote Code Execution	Not applicable	2957503 in MS14-036
Windows Vista x64 Edition Service Pack 2 (3087039)	Important Elevation of Privilege	Important Elevation of Privilege	Not applicable	Not applicable	Important Elevation of Privilege	3079904 in MS15-078
Windows Vista x64 Edition Service Pack 2 (3087135)	Not applicable	Not applicable	Not applicable	Critical Remote Code Execution	Not applicable	2957503 in MS14-036

Automate updating tool

Social Engineering and Social Media Offence and Defence

- The less information out there about you, the better protected against identity theft

Ex: phishing attacks, spam, comment, social engineering, hackers, nation state surveillance, local law enforcement, basically everything.

This is the list of what information you should consider sharing online.

<https://www.stationx.net/list-of-personally-identifiable-information-pii/>

Identify Verification and Registration

Disposable email accounts

<https://mailinator.com/>
<https://www.guerrillamail.com/>
<http://www.mytrashmail.com/>
<http://www.mailexpire.com/>
<http://www.tempinbox.com>
<https://www.trash-mail.com/en/>
<http://www.dispostable.com/>
<http://crapmail.dk/en/>

Temporary email accounts

<https://anonbox.net/>
<http://freemail.ms/>
<http://10minutemail.com/>
10MinuteMail/index.html
<http://getairmail.com/>
<http://dontmail.net/>
<http://www.migmail.net/>

Example

Real Identity - billy.bob@gmail.com
Registering - register123@gmail.com

<https://www.guerrillamail.com/compose> FAKE mail tools

Behavioural Security Controls

1. If you didn't request it - don't click on it!

2. Never download and run any file you don't 100% trust.

3. Never enter sensitive information after following a link or popup.

4. Validate the link.

Subdomains & Misspelt

<http://www.google.com.stationx.net>

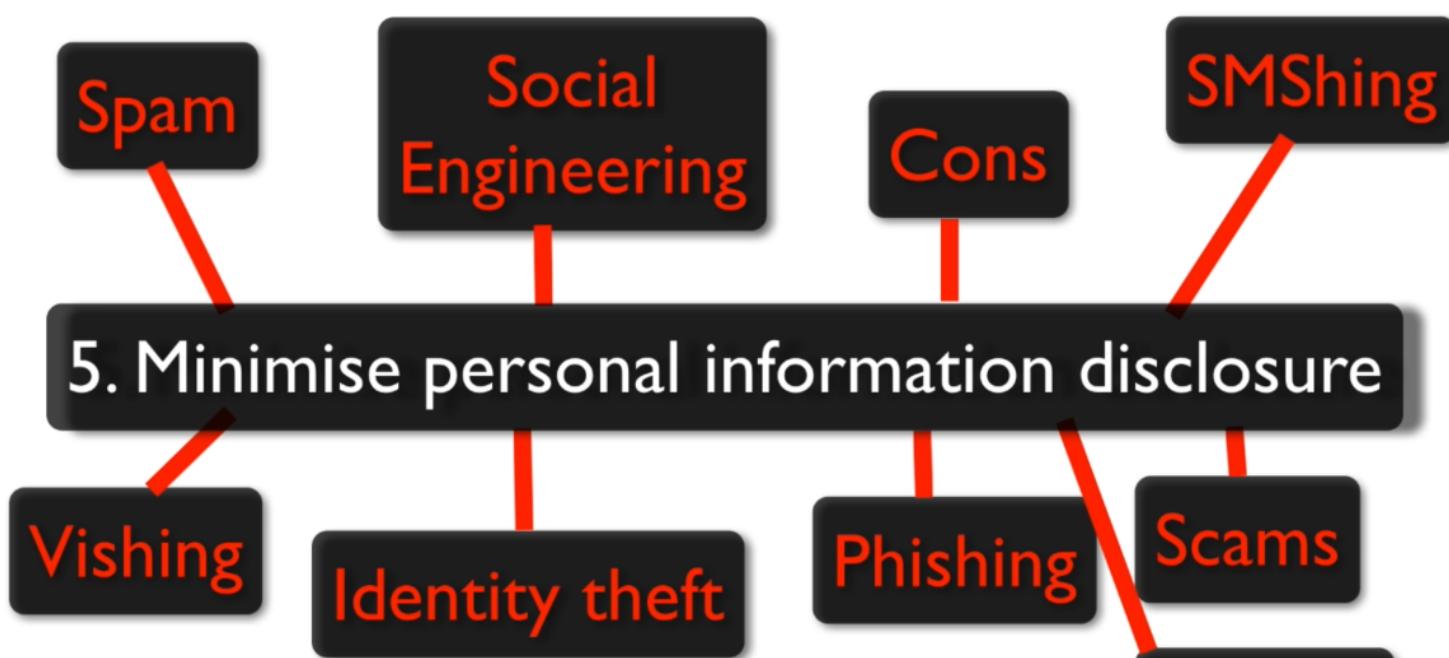
<http://stationx.net/sa/google.com/support/>

<http://www.rnicrosoft.com>

IDN homograph attack

<http://www.g00gle.com>

<http://www.goog1e.com>



Subject: Phish Test

From: Marg <margarettareifenberg@yahoo.com> on Thu Mar 10 2016 5:52:58 PM

To: nathan@ghostmail.com

+

Subdomains & Misspelt

<http://www.google.com.stationx.net>

<http://stationx.net/sa/google.com/support/>

<http://www.microsoft.com>

IDN homograph attack

<http://www.g00gle.com>

<http://www.goog1e.com>

Hidden URLs

7. Validate the sender.

- You can validate the sender by contacting them to verify if it is legitimate

Find out where the mail is coming from

1. This website help you to find the source IP of where is sent: <https://www.parsemail.org/msg/-JmHBOn>
2. Check for the email source.

orprk1+39jx5err5g41o@guerrillamail.com

to me ▾

hahahahahaha

Jun 24, 2021, 2:32 PM (1 da

Reply

Forward

Filter messages like this

Print

Delete this message

Block "orprk1+39jx5err5g41o@g

Report spam

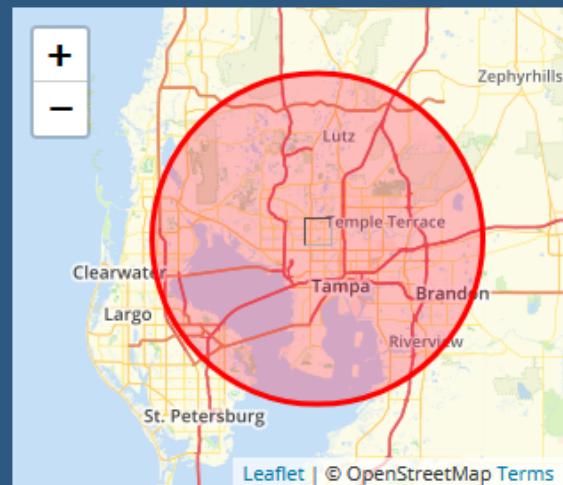
Report phishing

Show original

3. Look up IP address

IP Details For: 72.185.229.238

Decimal: 1220142574
Hostname: 072-185-229-238.res.spectrum.com
ASN: 33363
ISP: Spectrum
Organization: Spectrum
Services: None detected
Type: Broadband
Assignment: Likely Static IP
Continent: North America
Country: United States
State/Region: Florida
City: Tampa



[CLICK TO CHECK BLACKLIST STATUS](#)

Attachment

- **Never run these extension files** if you don't know where it is coming from

Executable file extensions

Very dangerous - Likely contains malware

- .EXE (machine language)
- .COM (machine language)
- .VB (Visual Basic script)
- .VBS (Visual Basic script)
- .VBE (Visual Basic script-encoded)
- .CMD (batch file - Windows)
- .BAT (batch file - DOS/Windows)
- .WS (Windows script)
- .WSF (Windows script)
- .SCR (screen saver)
- .SHS (OLE object package)
- .PIF (shortcut to DOS file plus code)
- .HTA (hypertext application)
- .JS (JavaScript script)
- .JSE (JScript script)
- .LNK (shortcut to an executable)
- .DEB (Debian software package)
- .RPM (Redhat software package)

8. Validate the attachment.



Document file extensions

Dangerous - Can contain macro viruses

- .XLS (Excel)
- .DOC (Word)
- .PDF (Adobe)

Compression and file archives

Dangerous - Can contain executable malware files

.ZIP (Compression)

.RAR (Compression)

.z (Compression)

.Z (Compression)

.7z (Compression)

.DMG (Apple disk image) – These can autorun on mac

- **Maybe Safe**

Other

Probably safe

- .TXT (text)
- .GIF (image)
- .JPG & .JPEG (image)
- .BMP (image)
- .PNG (image)
- .AI (image)
- .WMF (image)
- .TIF (image)
- .EPS (image)
- .PCX (image)
- .DXF (image)
- .MP3 (Audio)
- .WAV (Audio)
- .FLAC (Audio)
- .WMA (Audio)
- .MPG (Audio)
- .MPEG (Video)
- .AVI (Video)
- .MOV (Video)
- .MP4 (Video)
- .MKV (Video)
- .WMV (Video)



Too good to be true offer

Print Close

Subject: Final reminder: Notice of Tax Return

▼ Sent By "IRS Online" <reminde@irs.com> On: April 10, 2013 1:56 PM
To: undisclosed-recipients:
Reply To: noreply@irs.com



Department of the Treasury
Internal Revenue Service

04/10/2013
Reference: I3H583326/13

Claim Your Tax Refund Online

Dear Taxpayer,

We identified an error in the calculation of your tax from the last payment, amounting to \$ 319.95.

In order for us to return the excess payment, you need to create a e-Refund account after which the funds will be credited to your specified bank account.

Please click "Get Started" below to claim your refund:

Get Started Hover the mouse over the link, but DO NOT click the link!

Wow! Looks official, right? It says IRS, it has the logo... etc.

If it sounds too good to be true, then it probably is too good to be

careybaptist.org.uk/inc/s/

Now observe the actual link you would be taken to!

Technical Security Control

Technical Security Controls to Protect Against Social attacks

- View as text
- Use Google Safe Browsing (For Security - Turn off for privacy)
- Use Ublock origin filter lists (+ other browser extensions)
- Isolation and compartmentalisation
- Use a virtual machine
- Application white listing
- Application and execution controls
- Sandboxes
- Opening attachments online (Google Docs and Etherpad)
- Use Live operating system
- Using OpenPGP signatures to validate sender
- Host files and provide links instead of attaching to email
- Use Anti-virus and endpoint protection

(More on these later...)

