Task 1: IoT Home Assistants

Task 1A) (216 Words)

Security Risks
Hacking Vulnerabilities: IoT devices like those with cameras are vulnerable to hacking. Ring devices, for instance, have been hacked on multiple occasions, allowing unauthorized access to home videos. This was highlighted in a situation where a family's Ring device was used to taunt their child. This type of vulnerability can lead to unauthorized surveillance and data theft.

Data Access: Products like Amazon's Astro, which can move around in the home, offer potential backdoors for intruders. This would allow them to observe users and tap into personal details.

Privacy Implications
Surveillance and Data Collection: IoT devices have the tendency to collect enormous amounts of personal data, which businesses use for various purposes. Amazon, for example, collects data from products like Echo and Ring in order to make customer service better and potentially targeted advertising.

Law Enforcement Access: Ring doorbells and Amazon Astro are able to provide law enforcement access to video within homes via a court order. This raises privacy issues, including when there have been warrants for video that is unrelated to the activity of the homeowner.

Facial Recognition: Facial recognition is used by some devices, such as Amazon Astro, to recognize people in the house. Facial recognition is a useful feature with privacy concerns in terms of storage and use of this data.

Sources Used:
- Politico: The privacy loophole in your doorbell
- SlashGear: The Amazon Astro Poses A Huge Privacy Threat
- The Verge: Amazon Alexa voice data targeted ads research report
- Wired: Ring hacks exemplify IoT security crisis

Task 1B) (262 Words)

Phone: iPhone 14 Plus with iOS 18.3.2
Computer: MacBook Air (2021, M1) with macOS Monterey
Manufacturer and Country of Origin: Apple Inc., United States

Apple devices, like the iPhone 14 Plus and MacBook Air, collect a variety of telemetry data, whether or not users have opted to share analytics. Below are the findings for each device:

iPhone 14 Plus (iOS)
Apple collects data such as device identifiers (UDID, Ad ID), location, app use, and browsing history in Apple apps like the App Store, even if the privacy option is selected to restrict tracking.

According to a study by Tommy Mysk, it was demonstrated that Apple apps deliver accurate usage data to Apple servers regardless of users' consent. The information includes what apps are handled, searches made, and ads viewed.

The data collected can be used for device fingerprinting and linked to user profiles through the use of distinct identifiers.

MacBook Air (macOS)
macOS collects crash reports, app usage metrics, and hardware/software information. This data is anonymized but nonetheless transmitted to Apple servers in the event users agree to sharing analytics.

However, macOS uses technologies like Gatekeeper, which sends one-time codes of applications executing on the operating system to verify whether they are safe. This has created concerns regarding data overcollection.

Did I Learn Anything New?
Yes, I found that even when you have privacy settings enabled, Apple devices continue to gather a great deal of telemetry data. For example, iPhone apps track user activity in significant detail in the Apple ecosystem, and macOS sends Apple app identifiers when an application is opened.

Sources Used
-The Register: Android and iOS telemetry study
-TechCrunch: Apple's data collection practices
-Apple Support: Analytics information from your Mac

Task 2: VPN comparison

Category	NordVPN	Surfshark	ProtonVPN
OpenVPN & WireGuard	Supports both OpenVPN and WireGuard (NordLynx protocol for faster speeds).	Supports both OpenVPN and WireGuard (high-speed performance).	Uses OpenVPN, WireGuard, and its own Stealth protocol for censorship bypass.
System/App Kill Switch	Comprehensive kill switch available on all platforms.	Kill switch available, but occasional bugs reported.	Reliable kill switch on all platforms.

Infrastructure Audit	Regular audits conducted; NordVPN has passed multiple independent audits.	No public infrastructure audits yet.	Fully audited infrastructure and open-source client.
Logging Policy	Strict no-logs policy, independently verified multiple times.	No-logs policy, but lacks transparency reports.	Strict no-logs policy backed by audits and transparency reports.
Jurisdiction	Panama (privacy-friendly).	Netherlands (14 Eyes jurisdiction).	Switzerland (strong privacy laws).
14 Eyes	Outside 14 Eyes surveillance alliance.	Located within 14 Eyes jurisdiction.	Outside 14 Eyes jurisdiction (Switzerland).
Warrant Canary/Transparency Report	Publishes transparency reports regularly but no warrant canary.	No transparency reports or warrant canary available.	Offers both transparency reports and warrant canary.
Anonymous Payment/Signup	Accepts cryptocurrency payments for anonymity.	Accepts cryptocurrency payments for anonymous signup.	Accepts Monero for maximum anonymity in payments.
Misleading Security Marketing	Transparent marketing; avoids exaggerated claims.	Some exaggerated claims about privacy features (e.g., "No Borders").	Transparent marketing with a focus on privacy-first design.
Open-Source Client	Proprietary client, not open-source.	Proprietary client, not open-source.	Fully open-source client available for review.
Multihop	Supports Double VPN for enhanced security.	Offers Multihop servers for added privacy layers.	Secure Core servers provide multihop functionality through privacy-friendly locations like Iceland and Switzerland.
Port Forwarding	No port forwarding available due to security concerns.	No port forwarding support available.	No port forwarding support available either.

WireGuard is superior to OpenVPN for several reasons:

Performance: WireGuard is lighter and quicker since it uses a more streamlined codebase (~4,000 lines vs. ~600,000 lines for OpenVPN). This results in reduced latency and higher speeds in transferring data.

Security: WireGuard utilizes modern cryptography primitives like ChaCha20 and Poly1305, which are more secure against attacks compared to the aging protocols utilized by OpenVPN.

Ease of Use: Its less complicated framework is easier to audit and keep up with.

WireGuard is a privacy risk, however, because it holds IP addresses on the server for a short time when sessions are ongoing, which could be utilized if logs were held in the wrong way. OpenVPN fails to do this by not holding session details.

VPNs to Avoid
TunnelBear: Canadian company with US parent (McAfee), TunnelBear is located in non-privacy-friendly jurisdictions (Five Eyes alliance) and has limited features like no Tor-over-VPN or unblocking Netflix.

Hola VPN: Hola has a poor reputation for bad security practices, and it uses a peer-to-peer approach that could share users' IP addresses and bandwidth with others.

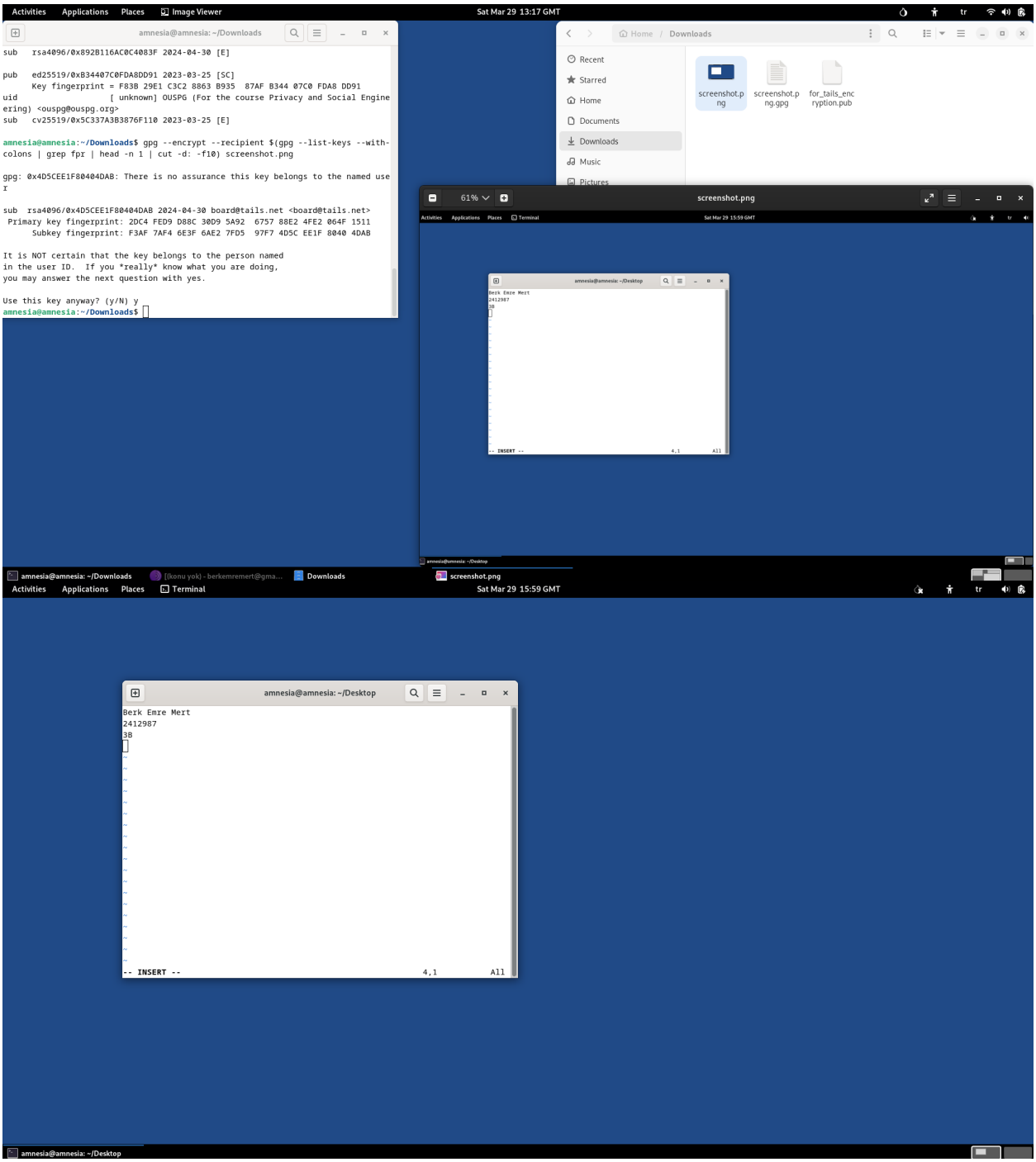
PureVPN: While it has professed to be no-logs, PureVPN has been linked with instances of user information being handed over to the authorities, putting its integrity in question.

These VPNs have poor privacy protection or are based in jurisdictions that can potentially betray user information.

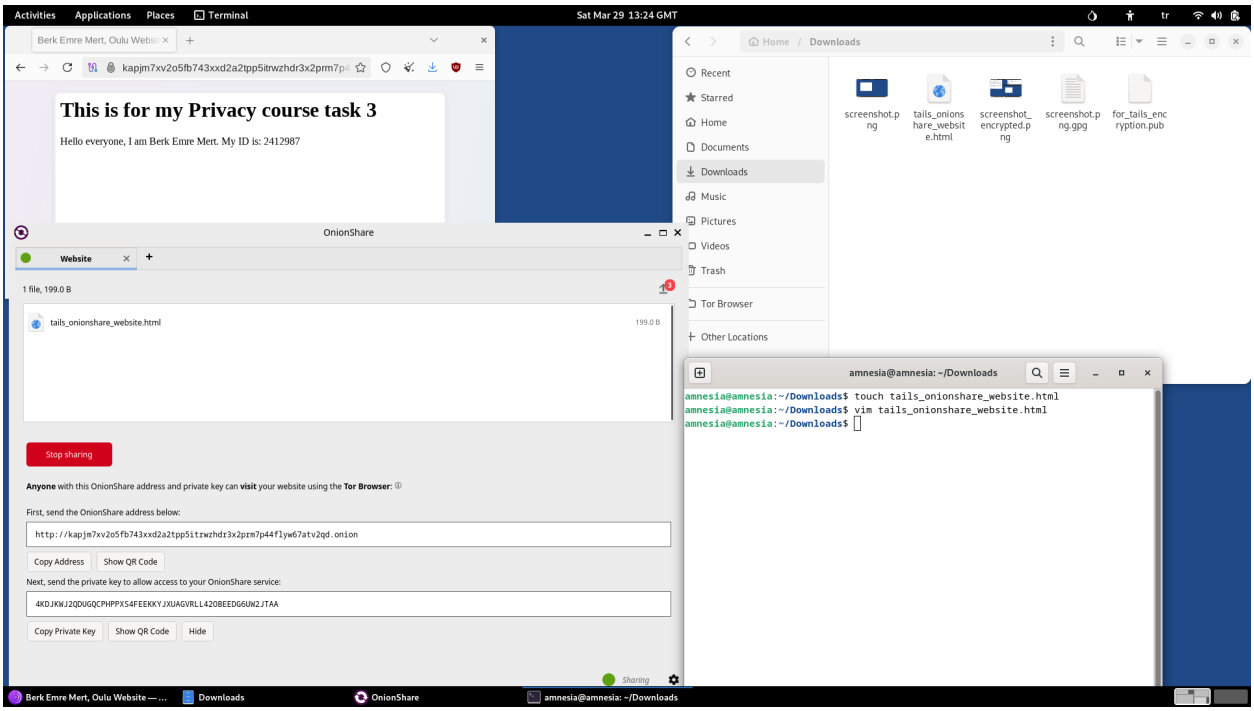
Task 3: Leaving no traces with, Tails, GPG, Tor and OnionShare

Task 3A)

I installed Tails and ran it on my brother’s computer. I am adding the screenshot both here and Github.


Activities
Applications
Places
Image Viewer
Sat Mar 29 13:17 GMT
amnesia@amnesia: ~/Downloads
sub rsa4096/0x892B116AC0C4083F 2024-04-30 [E]
pub ed25519/0xB34407C0FDA8DD91 2023-03-25 [SC]
Key fingerprint = F83B 29E1 C3C2 8863 B935 87AF B344 07C0 FDA8 DD91
uid [unknown] OUSPG (For the course Privacy and Social Engineering) <ouspg@ouspg.org>
sub cv25519/0x5C337A3B3876F110 2023-03-25 [E]
amnesia@amnesia:~/Downloads$ gpg --encrypt --recipient $(gpg --list-keys --with-colons | grep fpr | head -n 1 | cut -d: -f10) screenshot.png
gpg: 0x4D5CEE1F80404DAB: There is no assurance this key belongs to the named user
sub rsa4096/0x4D5CEE1F80404DAB 2024-04-30 board@tails.net <board@tails.net>
Primary key fingerprint: 2DC4 FED9 D88C 30D9 5A92 6757 88E2 4FE2 064F 1511
Subkey fingerprint: F3AF 7AF4 6E3F 6AE2 7FD5 97F7 4D5C EE1F 8040 4DAB
It is NOT certain that the key belongs to the person named
in the user ID. If you *really* know what you are doing,
you may answer the next question with yes.
Use this key anyway? (y/N) y
Home / Downloads
Recent
Starred
Home
Documents
Downloads
Music
Pictures
screenshot.png
screenshot.png.gpg
for_tails_encryption.pub
61%
screenshot.png
Berk Emre Mert
2412987
3B
-- INSERT --
4,1
All
amnesia@amnesia: ~/Downloads
[konu yok] - berkemremert@gma...
Downloads
screenshot.png
Activities
Applications
Places
Terminal
Sat Mar 29 15:59 GMT
amnesia@amnesia: ~/Desktop
Berk Emre Mert
2412987
3B
-- INSERT --
4,1
All
amnesia@amnesia: ~/Desktop

Task 3B)

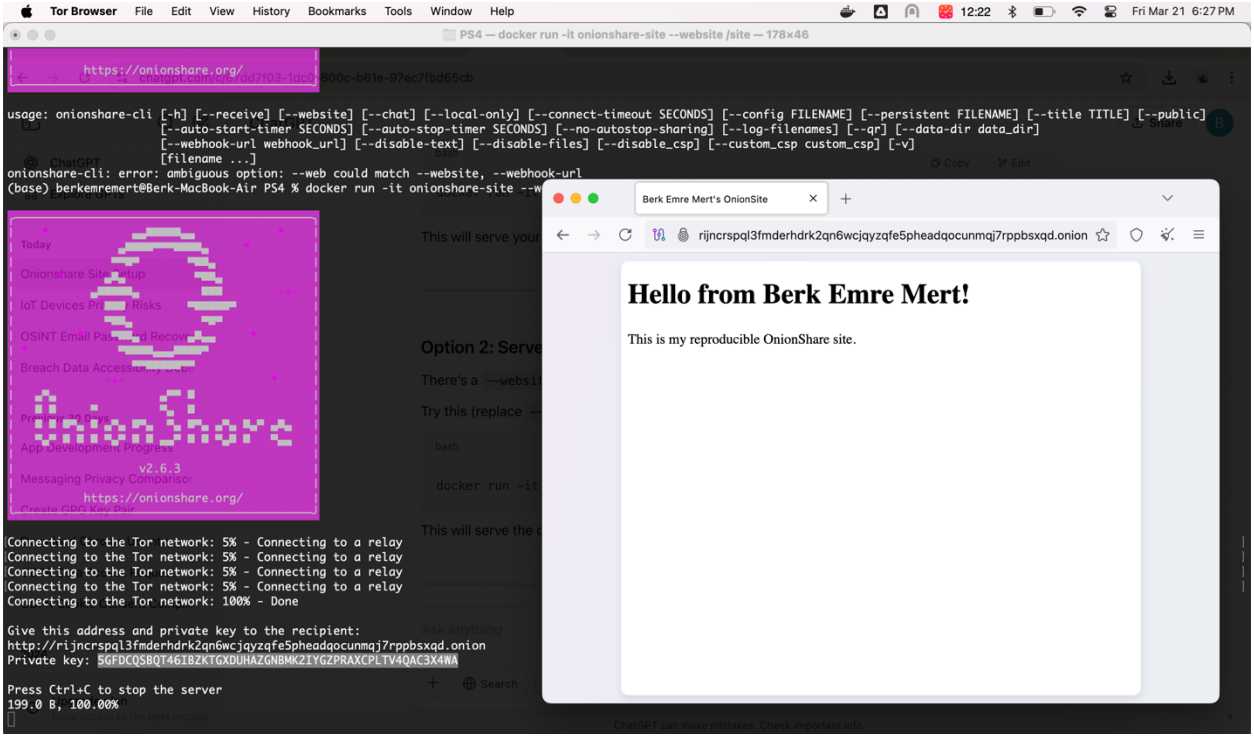


Task 3C)

1. The files are still in the RAM unit will remain however otherwise, rest will be deleted. System will be closed safely in that case.
   I didn't wanna try it because both the USB device and computer weren't mine.
2. These tools are essential for individuals and organizations that need to keep their privacy, secure their communications, and avoid surveillance. For example, journalists use them to keep sources anonymous, activists use them to bypass censorship, and companies use them to store sensitive information securely.

   Tor and Tails allow for anonymity online by preventing tracking and leaving no data trail behind. GPG provides strong encryption to protect messages and documents from being read. OnionShare can securely share files while the sender and receiver remain anonymous.

Task 4: Reproducible Onionshare site



All the files are in my repository.