IC00AI83 Privacy and Social Engineering

Harsha Gunasekara

Study Right No. 2401908

Week 3: Operating system privacy

Task 1: Telemetry and other data collection

A) IoT Home Assistants

For each device separately describe two situations where the privacy and/or security of the user can be compromised

- Amazon's Ring

Privacy: Camera accessed by unauthorized individuals, potentially monitoring user activities or exploiting information

Security: Ring devices rely on secure Wi-Fi networks, but poorly secured network allow hackers to intercept communication, access personal data, remotely control the device.

- iRobot

Privacy: Mapping data crucial for navigation, but improper security expose valuable items or sensitive areas, potentially exposing unauthorized access.

Security: Hackers manipulate firmware/software, potentially gathering intelligence or conducting physical surveillance on location.

- Amazon's Alexa

Privacy: Recording private conversations accidentally expose information, such as financial details and passwords, to unauthorized access.

Security: Alexa and other smart home devices may be vulnerable to security vulnerabilities, allowing hackers to access user's home network, compromise sensitive data, conduct malicious activities.

- Amazon's Ring Smart Doorbell

Privacy: It’s like a standalone counterpart, can be hacked, allowing unauthorized individuals to access camera, potentially monitoring user's activities.

Security: Hackers access Ring account credentials, gaining access to live feed and historical footage, potentially revealing information about routines, visitors, package deliveries.

- Amazon's Astro

Privacy: Cameras and sensors may be hacked, allowing unauthorized individuals to access video/audio, potentially monitoring user activities.

Security: Software in a self-driving robot potentially manipulate movements or gather user information.

Find and list 5 CVEs for IOT devices such as those above. Give a short explanation of the CVEs.

- CVE-2019-3924 (Amazon Ring Video Doorbell Pro)

Vulnerability allowed attackers to intercept owner's Wi-Fi network credentials during device setup, potentially granting unauthorized access to home network and compromising other devices and data.

- CVE-2020-28914 (iRobot)

Mobile app vulnerable to hackers exploiting insecure Bluetooth communication, potentially eavesdropping user data.

- CVE-2020-13868 (Amazon Echo Dot)

Vulnerable to remote code execution attacks, potentially leading to unauthorized access, data theft and device control by attacker.

- CVE-2021-32674 (Amazon Ring Indoor Cam)

Device's access controls breached, allowing unauthorized access to camera, potentially allowing attackers spy on device owner's activities and commit other malicious acts.

- CVE-2021-29229 (iRobot Braava Jet)

Mobile app allowed attackers to remotely control the Braava Jet robot mop, potentially manipulating movements and causing property damage.

In the U.S., there is a so-called third-party doctorine, which essentially gives the government access to all of your data without warrants, if you have given consent for a service provider to collect your data. Does this apply in Finland? If not, is it prevented by the Finnish legislation or European Union regulation?

The General Data Protection Regulation (GDPR) is a stringent law governing data protection and privacy in Finland and the EU. The GDPR guarantees the legal and equitable handling of personal data, safeguards privacy and informed consent, and restricts government authorities' access to such data.

The EU and Finland do not follow the "third-party doctrine" in the U.S., which permits government access to data without warrants, as per GDPR. The GDPR requires valid, informed, and unambiguous consent for processing personal data, with the right to withdraw consent at any time. Finnish legislation and EU regulations, including GDPR, ensure privacy and personal data protection, with strict legal requirements for government access.

1B) Regular operating systems

Include at least two peer-reviewed research sources

Analyze your findings, write a summary and list your sources

- Data leakage from Android smartphones

https://ffi-publikasjoner.archive.knowledgearc.net/handle/20.500.12242/905?show=full

Communication devices connected to internet enable us to communicate with devices and computer services at any location. These devices also pose a risk and attackers can gain sensitive information. Many users trust their device's physical protection, but simple protections like pin- and password, pattern screen locks, device control are considered sufficient to maintain trust. Smart phone users expect secure storage of information and trust in security mechanisms. This trust often misplaced, as vendors of hardware/software are often untrustworthy. Research examines trust in operating system vendors and smart phone applications, focusing on information sharing startup and normal configuration. It examines location information release for smartphones from multiple vendors and Android versions.

Phone - Galaxy Tab 7 & OS version - Android 2.3 Gingerbread.
Manufacturer - Samsung Electronics & Country of Origin - South Korea

- Mobile Security: Threats and Best Practices

  https://doi.org/10.1155/2020/8828078

This research aims to identify and analyze mobile security threats and best practices through a literature review and survey of 167 mobile application users. Results show high awareness of threats and countermeasures, with most utilizing built-in methods to mitigate malicious software and social-engineering scams. Study contributes to mobile security theory and practical value at both individual and enterprise levels. Understanding user intentions and motivations is crucial for leveraging mobile application security. Security always an arms race between attackers and defenders. Since the mobile application market is growing, security is often matter of balancing risk and reward, defense versus convenience.

Overall I learned demands for better user awareness and regulatory actions and brings out importance of accountability, transparency, user consent in data-sharing practices, particularly in mobile apps.

Task 2: VPN comparison

Explain the listings and compare three VPNs

	ProtonVPN	Surfshark	StrongVPN
OpenVPN	√	√	√
Wireguard	√	√	√
System/app killswitch	√	√	√
Infrastructure & client audit	√	√	x
Logging policy	No Logs	No Logs	No Logs
Jurisdiction	SwitzerlandCH	NetherlandsNL	USAUS
14 Eyes	√	x	x
Warrant canary	x	√	x
Anonymous Payment & Signup	Cash/Crypto	XMR/Crypto	x
Transparency report	√	√	x
Misleading security marketing	√	x	x
Open-source client	√	x	x
Multihop	Plus/Unlimited	√	x
Port Forwarding	Plus/Unlimited	x	x

Reason on a technical level, why privacy might, or might not be an issue, with Wireguard

WireGuard is often considered superior to OpenVPN from a performance and security standpoint due to several factors:

Performance:

Efficiency - WireGuard, a lightweight and efficient VPN, offers faster connection speeds and lower latency compared to OpenVPN due to its streamlined codebase and modern cryptographic techniques.

Connection Establishment - WireGuard utilizes advanced protocols and cryptographic primitives for key exchange and connection establishment, enhancing connection times, particularly in scenarios involving frequent network changes or handoffs.

Security:

Simplicity - WireGuard's minimalistic codebase enhances security by reducing the likelihood of implementation flaws and reducing the potential attack surface.

Modern Cryptography - WireGuard employs advanced cryptographic primitives like the Noise protocol framework, secure elliptic curve cryptography, and authenticated encryption to enhance security.

However, while WireGuard excels in performance & security, there are considerations regarding privacy,

Privacy Concerns:

Lack of Anonymity - Focuses on encryption and secure communication, lacking features like multi-hop routing or traffic obfuscation that can enhance privacy by masking network traffic origin & destination.

Logging Policies - VPN users' privacy is influenced by VPN service provider's logging policies, as some providers may still collect and retain user metadata or identifying information.

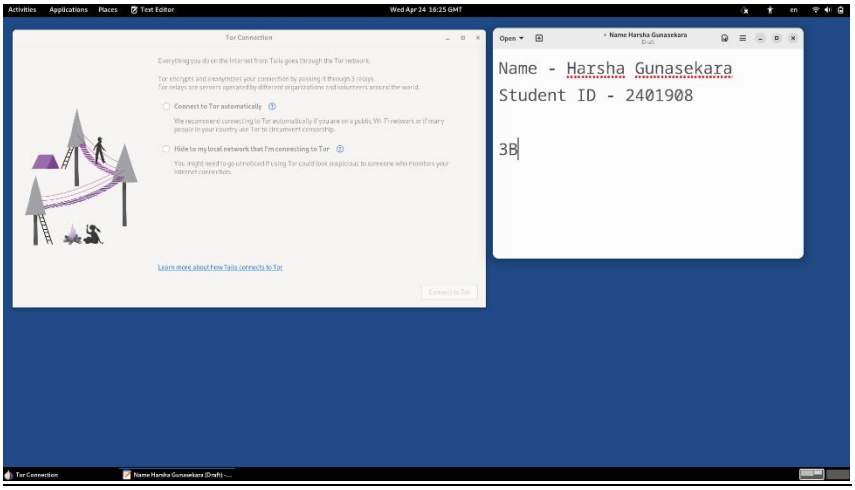
Which three VPN service providers do you think are the most important to avoid and why?

- HideMyAss
- IPVanish
- PureVPN

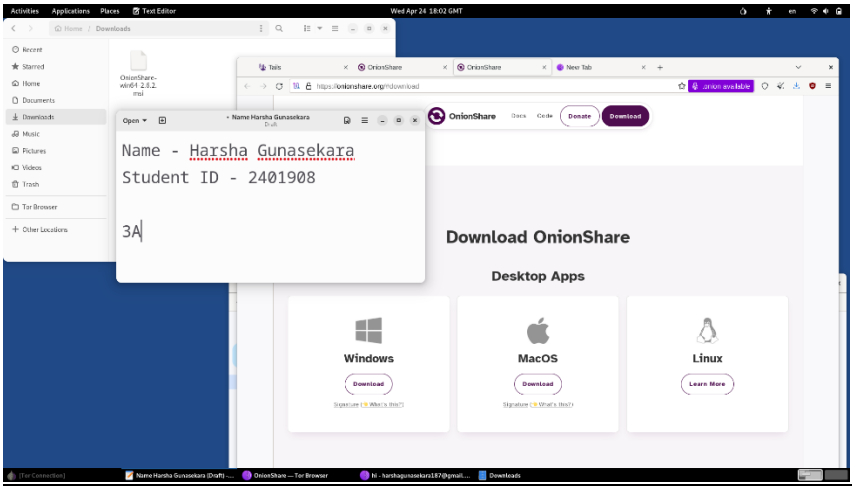
When considering VPN service providers to avoid, it's important to assess factors such as privacy policies, logging practices, jurisdiction, security vulnerabilities, and past incidents. Based on these criteria and the reputation of the VPN providers listed. While these VPN providers may offer certain features or attractive pricing, users should carefully consider the potential privacy and security risks associated with using them. It's essential to conduct thorough research and choose a VPN provider with a strong commitment to user privacy, transparent policies, and a track record of protecting user data.

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

3 A) What to return on the GitHub



3 B) Onionshare website



3 C) Then answer the questions below

What happens when you pull out your Tails USB stick, did you try this?

There was an error command with files running on the screen. Shut down the laptop

Why do these kinds of operations and services exist? Answer at around between 100 and 200 words.

The tools and services mentioned serve specific purposes within the broader context of privacy, security, and anonymity on the internet. That's protect users' privacy, security, and anonymity in digital world, enabling safe communication, sharing, and browsing without unwanted interference.

Tails - Live operating system designed for privacy and anonymity, booted from external media and providing built-in encryption tools and online anonymity networks like Tor, ensuring secure computing environments for web browsing, secure communication, sensitive information access.

GPG / GPA - Open-source encryption and signing tool, enabling users to encrypt and decrypt data, verify digital signatures, manage cryptographic keys. GPA is a graphical frontend for GPG, ensuring data security and authenticity.

Tor - Tor is a free, open-source software that protects users' privacy and anonymity by routing their internet traffic through worldwide network volunteer-operated servers, preventing network surveillance and traffic analysis.

OnionShare - Tor-based tool for securely and anonymously sharing files, allowing users to create temporary onion services to share files directly from their computer, preserving privacy and data security.

Task 4: Reproducible Onionshare site

Take a screenshot of your website from the Onion address. Identifier and address should be visible