SECURITY ASPECTS OF OPERATING SYSTEM

HINA UROOJ MALIK

23L-7832

FAST NUCES

LAHORE

Abstract— An operating system is a type of software that facilitates hardware communication and allows the execution of other programs. It consists of the basic software applications required for a computer to start up and run. The operating system that provides a PC, tablet, or smartphone its fundamental functions is a part of all of these devices. Security is by far the most important aspect of OS. Operating system security is the process of ensuring the confidentiality, availability, and integrity of the operating system. Operating system security refers to the processes or measures implemented to shield the operating system from threats such as malware, viruses, worms, and remote hacker incursions. Operating system security refers to all preventive-control measures that guard against any system resources being lost, altered, or stolen in the case that OS security is breached. When discussing operating system reliability, security and privacy are two key topics that come up. They differ technically yet are the same. The kernel and processes of the operating system execute the given task as instructed. Program threats arise when malicious activities are carried out by these processes due to a user program. Software bugs, spoofing logins, and trojan horses are all part of OS security.

Keywords— **Operating system**, Security, Privacy, Authentication, Authorization, Cyber Security

1. **Introduction**

The most significant piece of software that runs on a computer is the operating system. It controls all the hardware and software on the computer, as well as its memory and processes. Additionally, it enables you to interact with the computer even if you are unfamiliar with its language. A computer is nothing without an operating system. So, what is operating system security? One way to shield their operating system (OS) from various attacks is to implement operating system security. All the preventive and control mechanisms that a person installs on their computer to protect it and other connected devices (like printers) that hold private data that hackers will probably steal, alter, or remove if the system is compromised are collectively referred to as operating system security. Both the operating system and application are responsible for maintaining data security. Up until recently, operating system developers have given security a great deal of attention. In general, operating system protection includes both file system and operating system defence against unauthorized users. If a computer system is unmanned and permits the simultaneous operation of many processes, then those processes need to be secured from one another. To put it more simply, protection refers to a system for limiting programmed access. For this reason, the security system forbids unauthorized users from accessing the system and verifies the malicious destruction of data. It also refers to the system users' authentication to preserve the accuracy of the data kept within. The method of securing **Confidentiality**, **Integrity**, and **Availability** is known as operating system security. It is made up of preventive control methods that guard system resources that could be lost, taken, or changed in the case that operating system security is compromised. When discussing computer system safety, the terms "security" and "privacy" are most frequently used. Though they differ from one another, they are nonetheless closely related to each other. Privacy explains the type of control that an individual or group has over their selective secrecy and their level of comfort with the sharing and storing of information. Security is the umbrella term for the controls and safeguards in place to guard against malicious attacks, unauthorized access, and data breaches, as well as protecting the system, its data, and its resources.

The issue of security has grown in importance in the current era of computer networking. For the OS to effectively defend computer resources from potential dangers such as virus infections, data theft, unintentional or deliberate data loss, and unauthorised access, it must have well-designed procedures. In addition to memory, CPU, discs, peripherals, and other hardware, computer resources can refer to the information that is stored within the system (both software and data). Within the computer system, the majority of the data is quite valuable. Protection policies are used to put the protection mechanisms into action. The system administrator may choose the protection policies or they may be included in the OS. A protection policy might, for instance, specify which processes are permitted to terminate one another. A policy like this is enforced by the protection mechanism.

Protection usually offers a way for only authorized users or individuals to access the programs and data (stored in a computer system). The information stored in the system is protected by this method. Unauthorized users are not allowed to utilize system resources, while authorized users are those whose identities are known and who are allowed to use the system resources.

Cybersecurity is the technology that prevents criminal actors from exploiting and misusing digital assets by preventing unauthorized access. These malicious entities might be anything from insiders to highly skilled and driven hacking organizations that target information systems online. Cybersecurity is an important part of protecting users from malicious code and hackers. A great deal of research has been completed on existing tools and processes used to improve security. Hamdani et al. [1] performed a literature review of various cybersecurity standards and proposed a set of minimum requirements to improve operating system hardening. The vast landscape of standards and frameworks available highlights the extensive amount of research conducted in developing ways to secure an operating system.

1. **Operating System Security Overview**

The main key concepts of operating system (OS) security revolve around ensuring the protection of information, resources, and system functionality. The five fundamental principles are Authentication, Authorization, Confidentiality, Integrity, and Availability, often referred to as the CIA triad.



**Authentication**:

**Definition:** Verifying the identity of a user, process, or system entity is the process of authentication.

**Purpose:** Ensuring that users or entities accessing the system are who they say they are is the purpose.

**Techniques:** Passwords, biometrics (fingerprints, retinal scans), security tokens, and multi-factor authentication are examples of common authentication techniques.

**Authorization:**

**Definition:** Authorization is the process of allowing or refusing authenticated people or entities access rights and permissions.

**Purpose:** Manages the resources and actions that a user or process is permitted to access in accordance with their verified identification.

**Implementation:** Common authorization mechanisms include mandatory access control (MAC), role-based access control (RBAC), and access control lists (ACLs).

**Confidentiality:**

**Definition:** Maintaining confidentiality helps to prevent unwanted access to or disclosure of private information.

**Purpose:** It is to stop unauthorized people or programs from viewing or using private information.

**Implementation:** To ensure the confidentiality of data, both in transit and at rest, encryption is a frequently employed approach.

**Integrity:**

**Definition:** Integrity guarantees that data and system resources are reliable and accurate.

**Purpose:** Prevents data or system files from being altered, deleted, or corrupted without authorization.

**Techniques:** To confirm the integrity of data and system components, hash functions, digital signatures, and integrity checks are employed.

**Availability:**

**Definition:** Availability guarantees the regular accessibility and functionality of a system or resource when required.

**Purpose:** Protect against disruption, failures, or denial-of-service attacks that can impair users' or system access ability.

**Techniques:** Availability is maintained by the use of redundancy, backup systems, disaster recovery plans, and attack mitigation techniques.

1. **Authentication Vs Authorization**

**Authentication:**

* The process of verifying that a person is who they say they are in order to establish their identification is known as authentication.
* Both the client and the server use it. When someone wants to access information and the server has to know who is accessing it, it utilizes authentication. When the client seeks confirmation that the server is who it says it is, he uses it.
* The username and password are mostly used by the server for authentication. Card authentication, retinal scans, voice recognition, and fingerprint authentication are further methods that the server can use for authentication.
* What a person can view, read, or change in a process, or the actions they can perform within it, are not guaranteed by authentication. It primarily reveals the true identity of the individual or system.
* It involves different techniques such as Password-based authentication, Password-less authentication (OTP), and Single Sign-on.



**Authentication Factors**

**Single-Factor Authentication**

* The most basic form of authentication is single-factor authentication. A user can access a system with simply their login and password.

**Two-Factor Authentication**

* Since the name implies that it is two-level security, user authentication requires two-step verification. In addition to a username and password, it also needs certain information that only the individual user is aware of, including their first school name and favourite place to travel. In addition, it can confirm the user by emailing an exclusive link or sending an OTP to the registered phone number or email address.

**Multi-factor Authentication**

* The highest level of authority is this one, which is also the safest. Two or more security tiers from distinct and independent categories are needed. Banks, law enforcement agencies, and financial institutions are the typical users of this kind of authentication. This guarantees that no third party or hacker will be able to access your data.

**AUTHORIZATION:**

* Giving someone permission to do something is the procedure of authorization. It refers to a method of determining whether or not the user is authorized to utilize a resource.
* What data and information a single user can access is defined by it. Another way to say it is AuthZ.
* In order for the system to determine who is accessing the information, authorization typically works in tandem with authentication.
* It's not always required to have authorization in order to access information found online. Certain information that is accessible online may be viewed without authorization.



**Authorization Techniques**

* **Role-based access control**  
  RBAC or Role-based access control technique is given to users as per their role or profile in the organization. It can be implemented for system-system or user-to-system.
* **JSON web token**  
  JSON web token or JWT is an open standard used to securely transmit the data between the parties in the form of the JSON object. The users are verified and authorized using the private/public key pair.
* **SAML**  
  SAML stands for **Security Assertion Markup** Language. It is an open standard that provides authorization credentials to service providers. These credentials are exchanged through digitally signed XML documents.
* **OpenID authorization**  
  It helps the clients to verify the identity of end-users on the basis of authentication.
* **OAuth**  
  OAuth is an authorization protocol, which enables the API to authenticate and access the requested resources.

1. **Security And Privacy in Operating System**

In order to protect data, resources, and user information, operating systems must prioritize security and privacy. To keep consumers' trust and defend against a variety of cyberthreats, it is essential to ensure both security and privacy. In order to establish a safe and private environment, operating systems are essential to the implementation and enforcement of these safeguards.

**Security in Operating Systems:**

Operating system security refers to the policies and procedures put in place to protect the system, its parts, and the data it handles.

* **Access Control:** Controlling and limiting access to resources according to user permissions and rights.
* **Authentication:** Using passwords, fingerprints, or other techniques to confirm a user's identity and make sure they are who they say they are.
* **Authorization:** Permissions are granted or denied to users depending on their verified identities.
* **Encryption:** Sensitive information is protected using encryption, which transforms it into a code that only authorized parties can decode.
* **Firewall:** Installing barriers to regulate and keep an eye on incoming and outgoing network traffic in order to stop unwanted access.
* **Intrusion Detection Systems (IDS):** keeping an eye on and spotting unusual behavior or activity that might point to a security violation.
* **Patch management:** is the process of routinely installing and upgrading patches to fix security holes and vulnerabilities.
* **Audit Trails:** Monitoring and reviewing events for security analysis by keeping records of system activity.

**Privacy in Operating System**

Protecting users' private information and making sure their data is handled in a way that respects confidentiality are the two main goals of privacy in operating systems.

* **Data minimization:** is the process of gathering and preserving the least amount of personal information required for system operation.
* **User Consent:** Before collecting or processing a user's personal information, get their express consent.
* **Anonymization:** is the process of deleting or encrypting personally identifying data to avoid being linked to a specific person.
* **Secure Communication:** Making sure that operating system channels for communication are safe to avoid interception or eavesdropping.
* **Privacy Settings:** Giving people the ability to adjust privacy settings and preferences to manage how their data is utilized.
* **Transparency:** Giving information regarding data collection and processing procedures in an understandable and accessible manner.
* **Legal Compliance:** Keeping appropriate privacy laws and rules that control how personal data is handled.

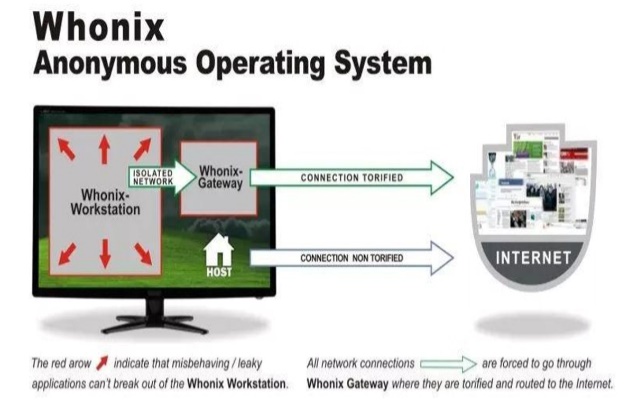
1. **Advancements in Security And Privacy**

**Privacy Hardened Linux Distros (Distributions)**

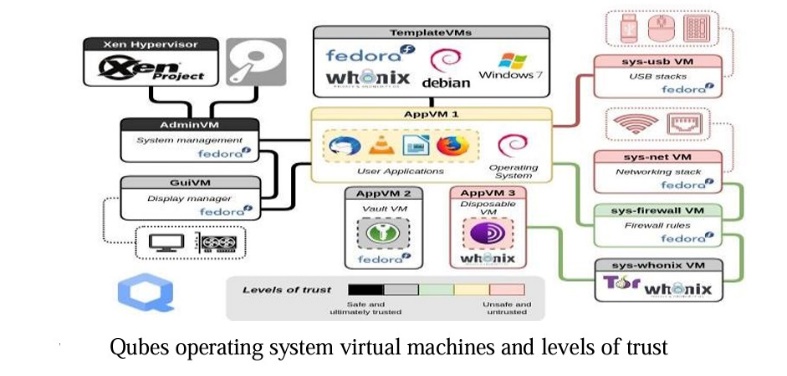
The present piece analyses Linux operating systems that put increased privacy and security first, concentrating on three variants in particular: Tails, Whonix, and Qubes OS. In order to strengthen the privacy of users and overall system security, these operating systems set themselves apart by integrating cutting-edge features like virtualization, division and interaction with the Tor network (short for The Onion Routing project—is an open-source privacy network that enables anonymous web browsing. The worldwide Tor computer network uses secure, encrypted protocols to ensure that users' online privacy is protected - The Tor Browser hides your IP address )

**Tails**, for example, is intended to operate as a live CD and provides users with the full set of applications needed for private internet surfing. It is difficult for users to install extra packages due to its strict security procedures, and it is strongly advised that they only install packages with low Common Weakness Enumerations (CWEs). Creating a secure install code, following security rules, and inspecting the source code for vulnerabilities are all part of the installation process

When it comes to routing all network traffic through the Tor network, **Whonix** takes a different method, requiring users to set up and configure separate virtual computers (Workstation and Gateway). To maintain maximum anonymity(unknown) and confidentiality, any changes to the Whonix operating system or Gateway virtual machine are discouraged. This setup requires a significant amount of technical knowledge for proper deployment.

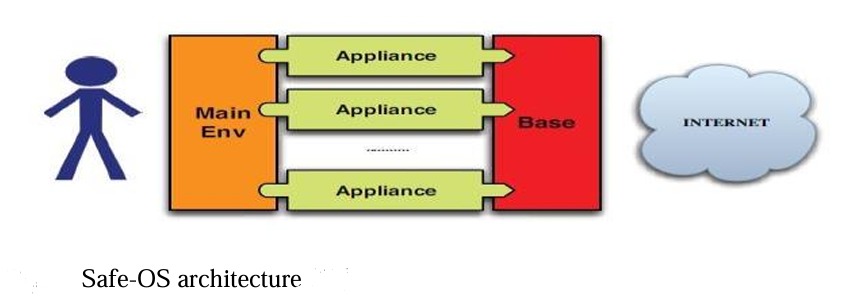


**Qubes** OS sets itself apart with its security-through-isolation approach, using virtualization to build many virtual machines for different purposes. These domains are managed by the Xen hypervisor, which is built upon a customized Fedora domain (Dom0). Each domain has a separate configuration and function, as well as varying security settings. Although this architecture offers better security, it is more difficult and requires more steps for users to set up and personalize each virtual machine.

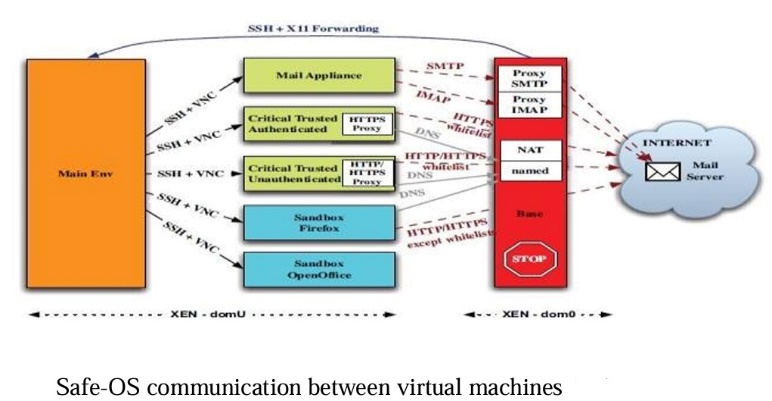


**Safe OS**

Like the Qubes operating system, Safe-OS uses virtualization to improve operating system security by offering strong isolation. If one virtual machine is compromised, it just affects that particular machine and is not able to interact with other virtual machines when numerous virtual machines are used on a single physical machine. In comparison to Qubes, Safe-OS offers additional task control with the addition of a more detailed task management system. According to the authors, Safe-OS is easier to use and more successfully reduces security vulnerabilities associated with file sharing amongst virtual computers.



Two virtual machine interfaces are part of Safe-OS's architecture: the Base virtual machine interface is responsible for maintaining communication policies, while the Main Env virtual machine interface acts as the user interface by displaying all apps that are executed by users. Virtual Network Computing (VNC) and Secure Shell (SSH) allow virtual computers to communicate with one another by creating a tunnel during login. The Main Env and application virtual machines communicate with each other via VNC, while SSH makes use of the user's private key that is kept on the base virtual machine.



Safe-OS is not without its problems, though; its strategy of executing each application in its own virtual machine and operating system presents obstacles. File transfers between virtual machines demand additional steps and technical expertise, adding complexity to everyday tasks—for example, moving a file from an email program to Microsoft Word requires transferring the file into the Office sandbox. Although application isolation improves security, it complicates file transfers between virtual machines, requiring human intervention and user judgment.

Like Qubes, Safe-OS has additional disadvantages caused by its dependence on virtualization. Virtualization is less user-friendly for new users without the right introduction and training because it requires specialised hardware and more resources.

**Privacy – Cookie Law**

The Cookie Law is a privacy law that was first enacted in the United Kingdom and then followed by many other countries. Its purpose is to safeguard users' privacy online by ensuring that websites gain user consent before keeping or receiving any information. The law places a strong emphasis on the user's freedom to provide clear, explicit, and informed consent for the processing of their personal data. Consent for cookies should not be combined with other goals or terms and conditions, and users should be able to withdraw their consent as simply as they gave it. The law protects users' private information by encouraging openness and giving them discretion over how their data is collected and used.

**Privacy – Usable Privacy**

The importance of usability in successful security and privacy measures is emphasised in this section. It makes the case that if users—including administrators—find well-configured systems to be overly complicated, they lose their relevance. The section uses enterprise settings as an example to show how apparent complexity often leads to security settings being configured incorrectly, which affects overall security.

Regarding privacy, the conversation focuses on end users who are in charge of their privacy settings. Decisions regarding cookie settings, application access, and conditions of use are always there for users. It emphasizes the necessity of user caution by highlighting the persistent threat posed by phishing attempts.

The complexity of security and privacy systems, in addition to legal restrictions, is a major difficulty that has been highlighted. Agreements are frequently difficult for users to understand, and it might be difficult to access the choices for restricting or withdrawing consent. In order to overcome these obstacles, the section ends by promoting more usability and simplicity in privacy and security solutions.

**Security – Mobile Operating System**

This section focuses on how mobile operating systems, because of their extensive use and the volume of personal data they keep, are more open to privacy and security threats. Particularly at risk are mobile operating systems that have not been updated. The main issue raised is the resource limitations present in mobile systems, such as those related to memory, storage, processing speed, and total device power. These limitations make typical computer operating system security follows inappropriate for mobile operating systems, prompting new research and approaches aimed at improving security and privacy in the mobile environment.

**Security – Usable Mandatory Integrity Protection for Operating Systems (UMIP)**

The crucial problem of host computer system compromises is addressed by the Usable Mandatory Integrity Protection for Operating Systems (UMIP). These compromises can have serious consequences, including unauthorised access, data modification, and the development of botnets for malicious reasons. Vulnerable software, a lack of timely security patching, and insufficient Discretionary Access Controls (DAC) to prevent network-based attacks are the main weaknesses that lead to compromised hosts.

Conventional security techniques that have demonstrated effectiveness in enhancing system security include Mandatory Access Control, Linux Intrusion Detection System, LOMAC, and Security Enhanced Linux. But their imposing appearance and intricate setup may prevent them from being widely used and adopted.

To address these issues, the security model was made simpler with the development of UMIP. By making use of the Linux Security Modules Framework, it provides benefits including little overhead and strong defense against a range of network threats. Each process is given a security designation (high or poor integrity) as part of the basic architecture of UMIP. A process takes on its parent's integrity level when it is created. A process's integrity level decreases when it submits a possibly tainted request.

With most attacks, UMIP seeks to guarantee that an attacker may only gain restricted access and cannot jeopardize(risk) the integrity of the system as a whole. An attacker cannot write to files belonging to account B, for instance, if they gain access through a running program owned by account A.

A policy file that includes important data including program associations, types, exceptions, and executing relationships is used in the implementation of UMIP. This more thoughtful approach to security improves usability and offers a more workable way to secure host computer systems.

**Usable Privacy versus Usable Security**

It is imperative to acknowledge the distinction in meaning between "usability" with privacy when developing the model, as opposed to security.

Usability in terms of privacy is related to one's capacity to utilize the operating system in any way. As was covered in the Tails section, one of the biggest obstacles to creating operating systems that prioritize privacy is ensuring that users can carry out everyday tasks like visiting well-known websites. On the other hand, security usability mostly relates to how easy it is for users to utilize privacy options.

1. **Program Threats**

Mostly the attackers use computer programs to break the security system of a computer and to access the computer resources. The computer programs that are used to access the computer resources illegally or to damage them are known as malicious programs or malware. These programs spread themselves to other computers via e-mail, applications or through websites. There are different types of malicious attacks that can damage the operating system of computers.

**Major Attacks in Operating System**

**Trojan Horses**

**Definition**: A Trojan horse, often known as a Trojan, is a kind of malware that poses as trustworthy software in order to trick users into downloading and running it. Trojan horses cannot replicate like worms and viruses do.

**Characteristics:**

* Deceptive Nature: Trojans frequently pose as attractive or legitimate software to trick users into installing them.
* Payloads: Once activated, Trojan horses have the ability to carry out a number of malicious deeds, including data theft, granting unauthorized access, and file damage.

**Example:** The Zeus Trojan, designed to steal banking information by logging keystrokes and capturing screen images.

**Prevention:**

* Use Antivirus Software: To identify and get rid of Trojans, utilise reliable antivirus software that you update on a regular basis.
* Exercise Caution: Use caution while downloading software and opening links, especially from sources you don't know or trust.

**Login Spoofing**

**Definition:** Creating a false login interface with the intention of tricking users into disclosing sensitive information, like passwords and usernames, is known as login spoofing.

**Characteristics:**

* Imitation: Users may find it challenging to discern between fake and authentic websites when they encounter spoof login pages that imitate authentic login interfaces.
* Social Engineering: It's a common tactic used to trick consumers into disclosing their login information.

**Example:** Phishing emails containing links to fake login pages that resemble popular online services like banking or email platforms.

**Prevention:**

* Education and Awareness: Inform users about the dangers of phishing attempts and the significance of double-checking URLs before entering login information.
* 2FA, or two-factor authentication: Put in place 2FA to boost security beyond passwords.

**Buggy Software**

**Definition:** Programmes or applications that have bugs, glitches, or programming mistakes that can cause unexpected behaviour are referred to as buggy software.

**Characteristics:**

* Errors & Flaws: Programming faults can cause software to display unexpected crashes, crashes, or unexpected consequences.
* Security Vulnerabilities: Attackers may be able to undermine system security by taking advantage of certain faults.

**Example:** Heartbleed, a security vulnerability in the OpenSSL cryptographic software library, allowed attackers to access sensitive data.

**Prevention:**

* Regular Updates: Apply the most recent security updates to operating systems and software.
* Code Reviews: Before deploying software, do comprehensive code reviews to find and correct programming mistakes.
* Conduct security audits: on a regular basis in order to find and fix any potential vulnerabilities.

1. **CYBER SECURITY**

The importance of cybersecurity in shielding digital assets from online threats and illegal access. It highlights the wide variety of computing devices—from massive workstations to tiny Internet of things devices (IoT) —that require cybersecurity safeguards. Several cybersecurity standards have been developed as a result of the text's statement of the need for cybersecurity standardisation. Cybersecurity, which emphasises the availability, confidentiality, and integrity of digital assets, is presented as an essential protective mechanism for people, organisations, and governments.

The introduction of the Parkerian Hexad model broadens the scope to encompass Possession or Control, Authenticity, and Utility. Cybersecurity is applied to unintended compromises brought on by natural disasters as well as planned attacks. The article emphasises the significance of monitoring cybersecurity in various data operations elements by highlighting that weaknesses may result in unauthorised access.

The difficulty of users—including network administrators—prioritizing usability over security, which may lead to configuration errors, is acknowledged in the text. The chapter addresses this by highlighting the contribution of academics and security specialists in creating guidelines and rules that have spread over the world. These standards address specifics like password protection, firewalls, anti-malware, encryption, and user training and encompass data at rest, data in motion, and data in use.

How difficult it is for common people and organisations to find security flaws, incorrect setups, and weak points in their systems. Laws governing data access, treatment, and processing are mentioned as the source of some standardisation. Even for seasoned cybersecurity firms, detecting security flaws is seen to be almost impossible for average users, and meeting standards is thought to be a difficult undertaking. Microsoft presents Security Compliance Manager, an interface-friendly solution for managing system setups. The fact that cybersecurity guidelines are broad and do not target operating systems (OS) in particular. As a result, even with tools like Microsoft Security Compliance Manager, system hardening becomes laborious for end users, requiring the manual extraction of requirements relating to the operating system from many standards.

1. **APPLICATIONS OF CYBERSECURITY**

**HealthCare:**

the rise in cybersecurity attacks directed at the healthcare industry, even while the financial services sector bears the greatest overall risk. Since 2015, the healthcare sector has been a top target for cyberattacks. The Internet of Things (IoT) is widely used in healthcare, especially for gathering data from Electronic Health Records (EHRs), as the text points out. The benchmark for cybersecurity compliance in the healthcare sector is the Health Insurance Portability and Accountability Act (HIPAA). The difficulties in protecting such sensitive data against various threats that could lead to compromise and security breaches because healthcare data is vital and extremely secret.

**Finance:** State and federal regulators have put strict cybersecurity norms and obligations on the financial sector. The Federal Financial Institution Examination Council (FFIEC) is referenced in its manual as a major body that establishes universal standards. This manual lists several pamphlets that include specifications for financial institutions. Furthermore, the Financial Industry Regulatory Authority (FINRA) establishes standards for the financial services sector, stressing the importance of having written policies and processes in place to protect consumer-sensitive data. According to the passage, cloud-based solutions and web-based content delivery technologies have an impact on information systems and create issues for industry standardization in cybersecurity. Recognized as well is the rise of the cybersecurity insurance market, which offers security and support to businesses affected by data breaches.

**Retail:**

The cybersecurity challenges faced by the retail sector, particularly the frequent targeting of end-user credit card data. The Payment Card Industry Data Security Standard (PCI DSS) is highlighted as the primary guideline for retailers to follow in order to address these issues. Unlike other industries, the retail sector is not federally regulated but adheres to PCI DSS guidelines to mitigate fraudulent attempts and data breach risks associated with payment-related information. Retailers must implement various security controls to meet regulatory requirements, generating compliance reports for verification. PCI DSS specifically focuses on securing cardholder data from major credit card issuers, emphasizing the importance of compliance to safeguard sensitive information. The passage outlines the three stages of PCI compliance—assessment, remediation, and final reporting—and emphasizes the significance of adopting best practices in information security. The overall effectiveness of PCI compliance is contingent on the frameworks adopted and their alignment with the protection of information assets. The passage suggests that while organizations often prioritize improving processes and technology, they may overlook the human element in information technology.

**Energy:**

the impact of digitization on the energy sector, bringing economic benefits through increased efficiency but also raising the risk of cyberattacks. Recent incidents in Ukraine underscore the growing threat, prompting the U.S. and the EU to implement rules and policies for defending against cyber threats in the energy sector. While the U.S. follows a detailed and strict "in-depth security" approach, the EU adopts a more comprehensive and flexible system. The U.S. is considered more advanced in terms of detailed cybersecurity rules, but there's potential for collaboration, particularly in areas like protecting personal data, privacy, and securing electrical networks. Harmonizing regulations between the U.S. and the EU is a goal to establish common cybersecurity standards, although existing differences may pose challenges. The passage highlights the opportunity for transatlantic collaboration in enhancing cybersecurity in the energy sector.

**References**

* A SECURITY-PRIVACY BASED MODEL FOR OPERATING SYSTEMS by Mohammed Mahmoud - 29 May 2022
* Take It or Leave It: A Survey Study on Operating System Upgrade Practices by Sadegh Farhang, Jake Weidman – Dec 2018
* Building a Security OS With Software Defined Infrastructure by Guofei Gu, Hongxin Hu – Sep 2017
* Private Browsing Forensic Analysis: A Case Study of Privacy Preservation in the Brave Browser by Ahmed Redha Mahlous1\* Houssam Mahlous2 – 25 Aug 2020
* A Survey of Security Research for Operating Systems by Masaki HASHIMOTO
* Synthesis Lectures on Information Security, Privacy and Trust by Ravi Sandhu
* European Union Institute for Security Studies (EUISS) – 2021
* Cybersecurity Standards in the Context of Operating System: Practical Aspects, Analysis, and Comparisons by SYED WASIF ABBAS HAMDANI, HAIDER ABBAS – May 2021
* OPERATING SYSTEM CONCEPTS by ABRAHAM SILBERSCHATZ
* Security Engineering A Guide to Building Dependable Distributed Systems Second Edition by Ross J. Anderson
* Issues of Operating Systems Security by CONSTANTINESCU Radu, ZOTA Razvan Daniel

Top of Form