International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 07 | July 2020 www.irjet.net p-ISSN: 2395-0072

CYBER SECURITY IN DIGITAL LIFE: A DETAILED STUDY

Chinchu S[1], Merin Mary Philip[2]

[1]Student Master of Computer Application, Dept. of CSE, Musaliar College of Engineering and Technology
[2]Asso. Professor, Dept of CSE, Musaliar College of Engineering and Technology

---

Abstract - Cyber Security is the activity of protecting information and information systems such as networks, computers, data base, data centres and applications with appropriate procedural and technological security measures. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the educational process. Security counter measure helps ensure the confidentiality, availability and integrity of information systems by preventing or serious asset losses from Cyber Security attacks.

Firewalls, antivirus software, and other technological solutions for safeguarding personal data and computer networks are essential but not sufficient to ensure security. Cyber-Ethics, Cyber-Safety, and Cyber-Security issues need to be integrated in the human life. The notion of "Cyber-Threats" is rather vague and implies the malicious use of information and communication technologies (ICT) either as a target or a tool by a wide range of malevolent actors.

1. INTRODUCTION

Cyber security is concerned with conception data bank safe from threats, namely cyber threats. The concept of "CyberHazard" is rather dim and implies the malicious use of information and communication technologies (ICT) either as a target or a tool by a wide range of malevolent actors. Although it should be emphasized that these figures are extrapolations. Internet is one of the fasted-thriving areas of technical framework development. In today's business environment, disruptive technologies such as cloud computing such as could computing, and next-generation mobile computing are fundamentally changing how organizations utilize information technology for sharing information and conducting commerce online. Today more than 80% of total commissary transactions are done online, so this field needs a high quality if security transparent and best transactions. Cyber security plays grave role in the development of information technology, as well as internet services.Boom cyber security and protecting critical information infrastructure are essential to each nation's security and economic well being. Cyber security is applied in the following domains.

- **Application Security**-Application security encompasses measures or counter-measures that are taken during the development life-cycle to protect applications from threats.
- **Information Security**-Information security protects information from unauthorized access to avoid identity theft and to protect privacy.
- **Network Security**-Network security includes activities to protect the usability, reliability, integrity and safety of the network. Active network security targets a soup of threats and rail them from entering or growing on the network.

2. WORKING PRINCIPLE OF CYBER SECURITY

To ensure a complete security posture assessment our process includes analysis and review of policies, information systems, network peripherals, information security devices remote access services, wireless access points, printers, back-up systems, log management systems, voice over IP systems, disaster recovery techniques and physical security.

2.1 Penetration Testing

Cyber security works penetration testing mimics an attacker with an adversarial intent to gain unauthorized access to client information, financial records, intellectual property, and sensitive portions of enterprise's network from the perspective of a trusted user and an adversary from inside, remote, and outside. Upon initial penetration, we exploit internal trust relationships between systems in an effort to perform possible secondary exploits. This is all done in a red teaming environment in an effort to provide an adversarial perspective to identify your information infrastructure's weakest links or "low hanging fruits" that might be visible to your employees, service providers, competitors, adversaries, and hackers.

Cyber security works **Dynamic Penetration Test (DPT)** provides an in-depth and comprehensive testing of information systems, network peripherals,information security devices,and web applications by intelligently launching interruption, interception, modification, and fabrication attacks with minimal disruption to the client's enterprise operations. DPT uses industry best practices for performing penetration testing in order to ensure cross validation, uniformity of processes, and consistency of results. DPT automates ***common hacker attack technique (CHAT)*** for performing penetration testing through a multistage process. Figure below illustrates key DPT steps.

DPT provides real-time testing capabilities against core information assurance building blocks (Network, Client, and

Application). DPT's attack modules consist of payloads that belong to one or more of the four major attack taxonomies (interruption, interception, modification, and fabrication). Testing is divided into three major categories internal, external and remote testing.DPT's major attack taxonomies are:

- **Availability Attacks or Denial of Service Attacks**- Information, information systems, and network becomes unavailable or unusable.
- **Interception or Confidentiality Attacks** Unauthorized access to information, information systems and network.
- **Interception or Confidentiality Attacks** Unauthorized tampering of information, information systems and network.
- **Fabrication or Accountability Attacks** Unauthorized creation, modification, and deletion of information, information systems and network elements.

2.2 Network Penetration Test

Clone actions of an attacker with an adversarial intent to gain unauthorized access to part of enterprise's network. Any device that has a network address or is accessible to any other device from the prospect of a trusted user and antagonist from inside, remote and outside.

2.3 Client Penetration Test

Clone actions of an attacker with an adversarial intent to gain illega laccess using persuasion and/or deception to gain access to, or information about, information systems.

2.4 Application Penetration Test

Replicates actions of an attacker to gain illegal access and/or gain greater level of access to web applications, e-commerce, ERP, and databases. Main goal of this test is to gain unauthorized access through privilege escalation using SQL injection, code injection, remote file inclusion, and cross site scripting.

Deception to gain access to, or information about, information systems.

3. CYBER SECURITY PRINCIPLES

These Principles recognize that the ISPs (and other service providers), internet users, and UK Government all have a role in minimizing and mitigating the cyber threats inherent in using the internet.

These Guiding Principles have been developed to react to this challenge by providing a persistent approach to help, inform, educate, and protect ISPs' (Internet Service Provider's) customers from online crimes. These Guiding Principles are aspirational, developed and delivered as a partnership between Government and ISPs. Some of the essential cyber security principles are described below.

3.1 Economy of mechanism

This principle states that Security mechanisms should be as simple and small as possible. The Economy of mechanism principle simplifies the design and implementation of security mechanisms. If the design and implementation are simple and small, fewer possibilities exist for errors. The checking and testing process is less complicated so that fewer components need to be tested.

Cinch between security modules are the pseudo area which should be as simple as possible. Because Interface modules often make implicit assumptions about input or output parameters or the current system state. If the any of these presumption are wrong, the module's actions may produce unexpected results.

3.2 Fail-safe defaults

The Fail-safe defaults principle states that the default contour of a system should have a moderate protection scheme. This principle also restricts how privileges are initialized when a subject or object is created. Whenever access, privileges/rights, or some security-related attribute is not explicitlygranted, it should not be grant access to that object.

Example: If we will add a new user to an operatingsystem, the defaultgroup of the user should have fewer access rights to files and services.

3.3 Least Privilege

This principle states that a user should only have those privileges that need to complete his task. Its primary function is to control the chore of rights granted to the user,not the identification of the user. This means that if the administrator demands root approach to a UNIX system that you administer, he/she should not be given that right unless he/she has a task that requires such level of access. If possible, the inflated rights of a user identification should be removed as soon as those rights are no longer needed.

3.4 Open Design

This principle states that the security of a structure should not depend on the mystery of its design or implementation. It suggests that complexity does not add security. This principle is the opposite of the approach known as "security through obscurity." This principle not only applies to information such as passwords or cryptographic systems but also to other computer security related operations.

Example: DVD player & Content Scrambling System (CSS) protection. The CSS is a cryptographic algorithm that protects the DVD movie disks from unauthorized copying.

3.5Complete mediation

The principle of complete mediation restricts the caching of information, which often leads to simpler implementations of mechanisms. The idea of this principle is that access to every object must be checked for compliance with a protection scheme to ensure that they are allowed.

Whenever someone tries to catch an object, the system should authenticate the access rights combine with that subject. The subject's access rights are verified once at the initial access, and for subsequent accesses, the system assumes that the same access rights should be accepted for that subject and object. The operating system should intercede all and every access to an object.

Example: An online banking website should need users to sign-in anew after a certain period like we can say, twenty minutes has elapsed.

3.6 Separation of Privilege

This principle states that a system should allocation access permission based on more than one status being satisfied. This principle may also be confining because it limits access to system individual. Thus before privilege is granted more than two verification should be performed.

Example: To change to root, two conditions must be follow- The user must know the root password. The user should be in the right group (wheel).

3.7 Least Common Mechanism

This principle states that in systems with multiple users, the mechanisms allowing resources shared by more than one user should be minimized as much as possible. This principle may also be confining because it limits the sharing of resources.

Example: If there is a need to be accesse a file or application by more than one user, then these users should use different channels to access these resources, which helps to prevent from unforeseen consequences that could cause security problems.

3.8 Psychological acceptability

This principle states that a security structure should not make the property more complicated to access if the security mechanisms were not present. The psychological ac-8ceptability principle recognizes the human element in computer security. If security-related software or computer systems are complicated to design maintain, or operate, the user will not operate the necessary security mechanisms.

Example: When we enter a wrong password, the system should only tell us that the user id or password was incorrect. It should not tell us that only the password was wrong.System should only tell us that the user id or password was incorrect. It should not tell us that only the password was wrong as this gives the attacker information.

3.9 WorkFactor

This principle states that the cost of deceive a security mechanism should be compared with the resources of a probable attacker when designing a security scheme. In some cases, the cost of deceive ("known as workfactor") can be simply calculated. In other words, the workfactor is a betray cryptographic quantify which is used to determine the strength of a given cipher.

Example: Suppose the number of experiments essential to try all available four character passwords is 244 = 331776. If the potential attacker must try each experimental password at a terminal, one might consider a four-character password to be satisfactory. On the other hand, if the possible attacker could apply an astronomical computer apt of trying a million passwords per second, a four-letter password would be a minor barrier for a possible intruder.

3.10 Compromise Recording

The concession Recording principle states that sometimes it is more enticing to record the details of interference that to adopt a more sophisticated measure to prevent it. Example: The servers in an office network may keep logs for all accesses to files, all emails sent and received, and all browsing sessions on the web.

4. CYBER SECURITY TECHNOLOGIES

With the rapid growth in the Internet, cyber security has become a major concern to organizations throughout the world. The fact that the information and tools & technologies needed to penetrate the security of corporate organization networks.

Some of the important security technologies used in the cyber security are described below-

4.1 Firewal

Firewall is a computer network security system designed to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both. Firewalls are used to block unauthorized Internet users from accessing private networks linked to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall check each message and blocks those that do not clash the specified security criteria.

Categories of Firewalls

4.1.1. Processing mode: The

five processing modes that firewalls can be categorised are-

4.2.1. Packet filtering

Packet filtering firewalls examine header information of a data packets that come into a network. This firewall installed on TCP/IP network and determine whether to forward it to the next network connection or drop a packet based on the rules programmed in the firewall. It scans network data packets looking for a violation of the rules of the firewalls database. Most firewall often based on a combination of Internet Protocol (IP) source and destination address. .Direction (inbound or outbound). .Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) source and destination port requests.

4.2.2. Application gateways

It is a firewall proxy which usually installed on a dedicated computer to grant network security. This proxy firewall acts as an intermediary between the requester and the protected device. This firewall proxy filters entering node traffic to certain specifications that mean only transmitted network application data is filtered. Such network applications include FTP, Telnet, Real Time Streaming Protocol (RTSP), BitTorrent, etc.

4.2.3. Circuit gateways

A circuit-level gateway is a firewall that operates at the

transport layer. It provides UDP and TCP connection security which means it can reassemble, examine or block all the packets in a TCP or UDP connection. It works between a transport layer and an application layers such as the session layer. Unlike application gateways, it monitors TCP data packet handshaking and session fulfilment of firewall rules and policies. It can also act as a Virtual Private Network(VPN) over the Internet by doing encryption from firewall to firewall.

4.2.4. MAC layer firewalls

This firewall is designed to operate at the media access control layer of the OSI network model. It is able to consider a specific host computer's identity in its filtering decisions. MAC addresses of specific host computers are linked to the access control list (ACL) entries.

This entry identifies specific -types of packets that can be sent to each host and all other traffic is blocked. It will also check the MAC address of a requester to determine whether the device being used are able to make the connection is authorized to access the data or not.

4.2.5. Hybrid firewalls

It is a type of firewalls which combine features of other four types of firewalls. These are elements of packet filtering and proxy services, or of packet filtering and circuit gateways. The kernel of Windows NT Executive. This firewall proxy operates at the application layer.

In this, when a packet arrives, a new virtual stack table is created which contains only the protocol proxies needed to examine the specific packet. These packets investigated at each layer of the stack, which involves evaluating the data link header along with the network header, transport header, session layer information, and application layer data. This firewall works faster than all the application-level firewalls because all evaluation takes place at the kernel layer and not at the higher layers of the operating system.

Protection from Inter all evaluation takes place at the kernel layer and not at the higher layers of the operating system. protection from Internet security threats. A firewall for a SOHO (Small Office Home Office) is the first line of defence and plays an essential role in an overall security strategy. SOHO firewall has limited resources so that the firewall product they implement must be relatively easy to use and maintain, and be cost-effective.

4.2. Intrusion Detection System (IDS)

An IDS is a security system which monitors the computer systems and network traffic. It analyses that traffic for possible hostile attacks originating from the outsider and also for system misuse or attacks originating from the insider. A firewall does a job of filtering the incoming traffic from the internet, the IDS in a similar way compliments the firewall security. Like, the firewall protects an organization sensitive data from malicious attacks over the Internet, the Intrusion detection system alerts the system administrator in the case when someone tries to break in the firewall security and tries to have access on any network in the trusted side.

4.3. Access Control

Access control is a process of selecting restrictive access to a system. It is a concept in security to minimize the risk of unauthorized access to the business or organization. In this, users are granted access permission and certain privileges to a system and resources. Here, users must provide the credential to be granted access to a system.

These credentials come in many forms such as password, keycard, the biometric reading, etc. Access control ensures security technology and access control policies to protect confidential information like customer data.

The access control can be categories into two types-

➢ **Physical Access Control-** This type of access control limits access to buildings, rooms, campuses, and physical IT assets.

➢ **Logical access control-** This type of access control limits connection to computer networks, system files, and data. The more secure method for access control involves two - factor authentication.

5. CYBER SECURITY TOOLS

There are numbers of hacking attacks which affecting businesses of all sizes. Hackers, malware, viruses are some of the real security threats in the virtual world. It is essential that every company is aware of the dangerous security attacks and it is necessary to keep themselves secure.

Here are six essential tools and services that every organization needs to consider to ensure their cybersecurity is as strong as possible.

5.1 Firewalls

The firewall is the core of security tools, and it becomes one of the most important security tools. Its job is to prevent unauthorized access to or from a private network. It can be implemented as hardware, software, or a combination of both.

The firewalls are used to prevent unauthorized internet users from accessing private networks connected to the Internet. All messages are entering or leaving the intranet pass through the firewall. The firewall examines each message and blocks those messages that do not meet the specified security criteria. We can pass the program through the firewall without any problems.

5.2 Antivirus Software

Antivirus software is a program which is designed to prevent, detect, and remove viruses and other malware attacks on the individual computer, networks, and IT systems. It also protects our computers and networks from the variety of threats and viruses such as Trojan horses, worms, key loggers, browser hijackers, root kits, spyware, botnets, adware, and ransomware.

Most antivirus program comes with an auto-update feature and enabling the system to check for new viruses and threats regularly. It provides some additional services such as scanning emails to ensure that they are free from malicious attachments and web links.

5.3 PKI Services

PKI stands for Public Key Infrastructure. This tool supports the distribution and identification of public encryption keys. It enables users and computer systems to securely exchange data over the internet and verify the identity of the other party. We can also exchange sensitive information without PKI, but in that case, there would be no assurance of the authentication of the other party.

People associate PKI with SSL or TLS. It is the technology which encrypts the server communication and is responsible for HTTPS and padlock that we can see in our browser address bar.

5.4 Managed Detection and Response Service (MDR)

MDR is an advanced security service that provides threat hunting, threat intelligence, security monitoring, incident analysis, and incident response. It is a service that arises from the need 18for organizations (who has a lack of resources) to be more aware of risks and improve their ability to detect and respond to threats.

MDR also uses Artificial Intelligence and machine learning to investigate, auto detect threats, and orchestrate response for faster result. The managed detection and response has the following characteristics:

➢ Managed detection and response is focused on threat detection, rather than compliance.

➢ MDR relies heavily on security event management and advanced analytics.

➢ While some automation is used, MDR also involves humans to monitor our network.

➢ MDR service providers also perform incident validation and remote response.

5.5 Penetration Testing

Penetration testing, or pen-test, is an important way to evaluate our business's security systems and security of an IT infrastructure by safely trying to exploit vulnerabilities. These vulnerabilities exist in operating systems, services and application, improper configurations or risky end-user behavior. A pen test attempts the kind of attack a business might face from criminal hackers such as password cracking, code injection, and phishing. It involves a simulated real-world attack on a network or application.

This tests can be performed by using manual or automated technologies to systematically evaluate servers, web applications, network devices, endpoints, wireless networks, mobile devices and other potential points of vulnerabilities. Once the pen test has successfully taken place, the testers will present us with their findings threats and can help by recommending potential changes to our system.

5.6 Staff Training

Staff training is not a 'cyber security tool' but ultimately, having knowledgeable employees who understand the cyber

security which is one of the strongest forms of defence against cyber-attacks. We know that cyber criminals continue to expand their techniques and level of sophistication to breach businesses security, it has made it essential for organizations to invest in these training tools and services. Failing to do this, they can leave the organization in a position where hackers would be easily targeted their security system.

6. TYPES OF CYBER ATTACKS

A cyber-attack is an assaul of computer systems and networks. It uses malevolent code to alter computer code, logic or data and lead to cyber attacks, such as information and identity theft. Due to the dependency on digital things, the illegal computer activity is growing and developing like any type of crime. Cyber-attacks can be classified into the following categories:

6.1 Webbased attacks

These are the attacks which occur on a Web page or web applications. Some of the important web-based attacks are as follows-

6.1.1 Injection attacks

It is the attack in which some data will be infuse into a web application to wield the application and fetch the required information.

6.1.2 DNS Spoofing

DNS Spoofing is a type of computer security hacking. By which a data is offer into a DNS resolver's cache cause the name server to twist an incorrect IP address, diverting traffic to the attacker's computer or any other computer. The DNS spoofing attacks can go on for a long period of time without being detected and can cause serious security issues.

6.1.3 Session Hijacking

It is a security attack on a user session up a protected network. Web applications create cookies to store the state and user sessions. An attacker can have access to all of the user data.

6.1.4 Phishing

Phishing is a type of attack which attempts to steal conscious information like user login credentials and credit card number. It occurs when an attacker is dissemble as a accurate entity in electronic communication

6.1 .5 Brute force

It is a type of attack which uses a exploratory and error method. This attack generates a large number of inference and validates them to obtain actual data like user password and personal identification number. This attack may be worn by criminals to ace encrypted data, or by security, analysts to test an organization's network security.

6.1.6 Denial of Service

It is an attack which meant to cause a server or network reserve unavailable to the users. It accomplishes this by flooding the target with traffic or sending it information that triggers a crash. It help the single system and single internet connection to strike a server.

It can be classified into the following-

- Volume-based attacks- Its goal is to saturate the bandwidth of the attacked site, and is measured in bit per second.
- Protocol attacks- It consumes actual server resources, and is measured in a packet.
- Application layer attacks- Its goal is to crash the web server and is measured in request per second.

6.1 7. Dictionary attacks

This type of attacks are found in the list of a commonly used password and validated them to get original password.

6.1 8. URL Interpretation

It is a type of attack were we can change the certain parts of a URL, and one can generate a web server to deliver web pages for which he is not authorized to browse.

6.1 9.File Inclusion attacks

It is a type of attack that allows an attacker to access unauthorized or necessary files which is available on the web server or to execute malicious files.

6.1 10. Man in the middle attacks

It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.

6.2 System-based attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

6.2.1. Virus

It is a malicious software program that transmit throughout the computer files without the knowledge of a user. It is a self-replicating malicious computer code that replicates by

enter copies of itself into other computer programs when executed. It can also execute codes that cause harm to the system.

6.2.2. Worm

It is a type of malware whose primary function is to replicate itself to distribute to uninfected computers. It works same as the computer virus. Worms originate from email attachments that appear to be from trusted senders.

6.2 3. Trojan horse

It is a malicious program that causes unexpected changes to computer setting and unusual activity, even when the computer should be idle. It misleads the user of its true intent. It appears in a normal application but when executed some malicious code will run in the background.

6.2.4. Backdoors

It is a method that circumvent the normal authentication process. A developer may create a backdoor so that an operating system can be penetrate for troubleshooting or other purposes.

6.2.5. Bots A bot is an automated process that Search merge with other network services. Some bots program run automatically, while others only execute commands when they receive specific input. Common examples of bots program are the crawler, chat room bots, and malicious bots.

7. NECESSITY OF CYBER SECURITY

Information is the most valuable asset with respect to an individual, cooperate sector, state and country with respect to an individual the concerned areas are:

- Protecting unauthorized access, disclosure, modification of the resources of the system.
- Security during on-line transactions regarding shopping, banking, railway reservations and share markets.
- Security of accounts while using social-networking sites against hijacking.
- One key to improved cyber security is a better understanding of the threat and of the vectors used by the attacker to circumvent cyber defences.
- Need of separate unit handling security of the organization.
- Different organizations or missions attract different types of adversaries, with different goals, and thus need different levels of preparedness.
- In identifying the nature of the cyber threat an organization or mission faces, the interplay of an adversary's capabilities, intentions and targeting activities must be considered. With respect to state and country

  • Securing the data basis maintaining the details of all the rights of the organizations at state level.

8. TRENDS CHANGING CYBER SECURITY

These are some of the trends that are having large impact on cyber security in digital life.

8.1 Web servers

The hazard of attacks on web applications to extract data or to share malicious code pursue. Cyber criminals distribute their malicious code by legitimate web servers they've negotiate. But data-stealing attacks,large number of which get the attention of media, are also a big threat. Now, we need a greater significance on protecting web servers and web applications.Web servers are the best platform for these cyber criminals to steal the data. Hence we must always use a safer browser especially during important transactions in order not to fall as a prey for these crimes.

8.2 Cloud computing and its services

All small, medium and large companies are slowly adopting cloud services. In other words the world is slowly moving towards the clouds. This current trend shows a considerable challenge for cyber security, as traffic can go around traditional points of inspection. More over, as the number of applications available in the cloud . Policy controls for web applications and cloud services will also need to evolve in order to break the wastage of valuable information. So cloud services are developing their own models still a lot of problems are being brought up about their security.

8.5 IPv6: New internet protocol

IPv6 is the new Internet protocol which is replacingIPv4 which has been a backbone of our networks in generic and he Internet at large. There are some very fundamental differences to the protocol which need to be considered in security policy. Hence it is always better to switch to IPv6 in order to reduce the risks regarding. cyber-crime.

8.6 Encryption of the code

Encryption is the process of encoding information in such a way that hearer or hackers cannot read it..In an encryption scheme, the message or information is encrypted using an encryption algorithm, turn it into an unreadable cipher text. This is done with the encryption key, which describes how the message is to be encoded. Encryption at a very opening level protects data privacy and its integrity. But the use of encryption brings more claim in cyber security.

9. CONCLUSION

Cyber security examined the significance of privacy for individuals as a fundamental human right. Abuse of human rights arise from their imprudent collection and storage of personal data. The problems associated with inaccurate personal data, or the abuse, or unauthorized disclosure of such data. We also include the current threats, issues, challenges and measures of IT sector in our society. With the increasing coincidence of cyber attacks, building an adequate intrusion detection model with good accuracy and real-time performance are essential. Indian citizens must identify the best techniques in order to protect the information and system, as well as the network in which they work. Thus there is a need of cyber –security schedule in the near future which will in-build the cyber-security awareness in the current youth and finally the IT sector will get more profound, securely skilled professionals not only i n the security sector but also in every sector, thus enhancing the transmission, the brain rapport skills of the employees and the employers.

REFERENCES

[1]. Ravi Sharma, Study of Latest Emerging Trends on "Cyber Security and its challenges to Society" .International Journal of Scientific &Engineering Research, Volume 3, Page no (67-86)

[2]. IEEE Security and Privacy Magazine –IEEECS "Safety Critical Systems – Next Generation "July/ Aug 2013

[3]. International Journal of Scientific & Engineering Research, Volume 4, Issue 9, September-2013 Page no(.68 – 71) "Study of Cloud Computing in Health Care Industry" by G. Nikhita Reddy, G.J. Ugander Reddy

[4].Myriam Dunn Cavelty, 2008," cyber security", edition no-3, Page no (367-386)