UNDERSTANDING CYBERSECURITY THROUGH MORPHOLOGICAL ANALYSIS

Sadoqat Alimbayevna Abdirazzakova

TUIT, English teacher of Foreign Languages Department

sadush1982@gmail.com

Annotation: This article explores the importance of understanding cybersecurity terminology in today's digital age. It explains how morphological analysis, breaking down words into their component parts, helps us grasp the meaning and function of cybersecurity terms.

Keywords: cybersecurity, terminology, morphological analysis, cyber threats, digital safety

Annotatsiya: Bu maqola bugungi raqamli asrda kiberxavfsizlik terminologiyasini tushunishning muhim ahamiyat kasb etishini ochib beradi Kibertahdidlar rivojlanib, murakkatlashib borayotganligi sabab, kiberxavfsizlik sohasida ishlatiladigan terminologiyani tushunish juda zarurdir. Morfologik tahlil yordamida so'zlarni tarkibiy qismlarga (prefikslar, ildizlar va qo'shimchalar) ajratish orqali biz kiberxavfsizlik terminlarining ma'nosi va funktsiyalarini yaxshi anglaymiz.

Kalit so‘zlar: kiberxavfsizlik, terminologiya, morfologik tahlil, kiberxavf, raqamli xavfsizlik

In today's digital world, where we rely heavily on technology for communication, financial transactions, and storing sensitive information, cybersecurity has become an essential concern. As cyber threats evolve and become more sophisticated, understanding the terminology used in cybersecurity is crucial. By breaking down these terms into their constituent parts (prefixes, roots, and suffixes) through morphological analysis, we gain a deeper understanding of their meanings and the concepts they represent. This knowledge empowers us to make informed decisions about our online safety, identify potential threats, and navigate the complex landscape of cybersecurity. Some terms have well-established meanings, the field of cybersecurity is constantly evolving, leading to the emergence of new terms and the reinterpretation of existing ones. Bruce Schneier, a renowned security expert, highlights the challenge of defining terms like "cybersecurity" itself. He argues that the term encompasses a broad range of practices and technologies, making it difficult to provide a single, universally accepted definition.

Here, we analyze some common cybersecurity terms to illustrate their morphological structures:

1. Antivirus

Prefix: "anti-" (against)

Root: "virus" (a type of malicious software)

Analysis: The term "antivirus" combines the prefix "anti-" with the root "virus" to describe software designed to detect and eliminate viruses.

Example: "The antivirus software detected and removed the malware from my computer."

2. Firewall

Compound Word: "fire" + "wall"

Roots: "fire" (protection) and "wall" (barrier)

Analysis: "Firewall" is a compound word where "fire" and "wall" together symbolize a protective barrier against cyber threats.

Example: "A firewall helps prevent unauthorized access to your network."

3. Malware

Prefix: "mal-" (bad)

Root: "ware" (software)

Analysis: The prefix "mal-" modifies "ware" to describe software designed to harm or exploit systems.

Example: "Malware can cause significant damage to computer systems."

4. Phishing

Root: "fish" (to lure)

Suffix: "-ing" (indicating an action)

Analysis: "Phishing" uses the root "fish" metaphorically to describe the act of luring individuals into providing sensitive information.

Example: "The email was a phishing attempt to steal my login credentials."

5. Ransomware

Root: "ransom" (payment demanded)

Suffix: "-ware" (software)

Analysis: "Ransomware" combines "ransom" and "ware" to denote malicious software that demands payment to restore access to data.

Example: "Ransomware encrypted my files and demanded payment for the decryption key."

6. Botnet

Compound Word: "bot" + "net"

Roots: "bot" (robot, automated program) and "net" (network)

Analysis: "Botnet" combines "bot" and "net" to refer to a network of infected devices controlled remotely by an attacker.

Example: "The botnet was used to launch a DDoS attack on the website."

7. Spyware

Root: "spy" (to observe secretly)

Suffix: "-ware" (software)

Analysis: The term "spyware" combines "spy" with "ware" to describe software that covertly monitors and collects information.

Example: "Spyware was found on my computer, tracking my online activities."

8. DDoS (Distributed Denial of Service)

Prefix: "Distributed" (spread out)

Root: "Denial of Service" (interrupting services)

Analysis: "DDoS" describes an attack where multiple systems are used to overwhelm and disrupt the normal traffic of a targeted server or network.

Example: "The website went down due to a massive DDoS attack."

9. Keylogger

Compound Word: "key" + "logger"

Roots: "key" (keystrokes) and "logger" (recording program)

Analysis: "Keylogger" combines "key" and "logger" to describe software that records every keystroke made on a computer.

Example: "The keylogger captured my password as I typed it."

The Rise of Acronyms and Initialisms:

Another trend in cybersecurity vocabulary is the proliferation of acronyms and initialisms. While convenient for those familiar with the field, these can be confusing for newcomers. Kevin Mitnick, a former hacker turned security consultant, emphasizes the importance of clear communication in cybersecurity. He suggests using plain language whenever possible to avoid alienating non-technical audiences.

1. **DDoS (Distributed Denial of Service)** (as analyzed previously)
2. **API (Application Programming Interface):** APIs are sets of protocols and tools that allow applications to communicate with each other. Understanding APIs is crucial for securing data transmitted between applications.
3. **IoT (Internet of Things):** The IoT refers to the network of physical devices embedded with software, sensors, and other technologies that connect and exchange data. As the IoT continues to expand, securing these devices becomes a growing concern.

The morphological analysis of cybersecurity terms reveals the intricate ways words are constructed to convey specific meanings related to cyber threats and defenses. Understanding these structures helps in comprehending the technical vocabulary of cybersecurity, aiding both communication and education in the field. However, it is important to acknowledge the evolving nature of cybersecurity terminology and the need for clear communication to bridge the gap between technical experts and the general public.

REFERENCES:

1. Polyanichko, M. A. (2019). Application of a maturity model to action against internalthreats to information security. International research journal, 4 (82), 57–60. (In Russ.)
2. Christopher, J. (2018). The Cybersecurity Maturity Model: A Means To Measure And Improve Your Cybersecurity Program // Forbes. 01.11.2018. https://www.forbes.com/sites/forbestechcouncil/2018/11/01/thecybersecuritymaturity modelameanstomeasureandimproveyourcybersecurityprogram.
3. Grevatt, J. (2021). Seoul looks to enhance protection of military technologies against cyber attacks // Jane’s Defence. https://www.janes.com/defencenews/ newsdetail/seoullookstoenhanceprotectionofmilitarytechnologiesagainstcyberattacks_14765
4. https://www.mitnicksecurity.com/.
5.https://www.schneier.com/blog/archives/2017/02/security_and_th.html.

5. www.reddit.com/r/IOT/comments/ui6c7i/why_are_iot_devices_so_insecure/.