

עבודה סמינריונית

תכנות מערכות דפנסיבי

סמינר: תכנות מערכות דפנסיבי 20928

מגיש: עמית סידס

בהנחיית: פרופ' לאוניד ברנבוים

תעודת זהות: 206768780

תאריך:

# תוכן עניינים

[תוכן עניינים 1](#_Toc57503663)

[מבוא 3](#_Toc57503664)

[שפת C++ 4](#_Toc57503665)

[מבנה ותחביר השפה 4](#_Toc57503666)

[מחלקות, אובייקטים וירושה 4](#_Toc57503667)

[פולימורפיזם 4](#_Toc57503668)

[מודל הזיכרון 4](#_Toc57503669)

[איומי אבטחה 4](#_Toc57503670)

[חולשת Stack Buffer Overflow 4](#_Toc57503671)

[מתקפת Return-oriented Programming 4](#_Toc57503672)

[דריסת משתנים וטבלאות וירטואליות 4](#_Toc57503673)

[מנגנוני אבטחה 4](#_Toc57503674)

[שפת Python 5](#_Toc57503675)

[מבנה ותחביר השפה 5](#_Toc57503676)

[דינאמיות השפה 5](#_Toc57503677)

[מחלקות, אובייקטים וירושה 5](#_Toc57503678)

[איומי אבטחה 5](#_Toc57503679)

[חולשות ב-Deserialization 5](#_Toc57503680)

[טעינת קובץ זדוני 5](#_Toc57503681)

[חילוץ קבצים זדוניים 5](#_Toc57503682)

[שימוש בפונקציות מסוכנות 5](#_Toc57503683)

[מנגנוני אבטחה 5](#_Toc57503684)

[תקשורת 6](#_Toc57503685)

[אבטחה בתקשורת 6](#_Toc57503686)

[פרוטוקולי הצפנה ואימות 6](#_Toc57503687)

[אלגוריתם Diffie–Hellman 6](#_Toc57503688)

[הצפנת RSA 6](#_Toc57503689)

[פרוטוקול SSL 6](#_Toc57503690)

[פרוטוקול TLS 6](#_Toc57503691)

[מתקפות שונות על פרוטוקולי תקשורת 6](#_Toc57503692)

[מתקפת POODLE 6](#_Toc57503693)

[מתקפת BEAST 6](#_Toc57503694)

[מתקפת CRIME 6](#_Toc57503695)

[מתקפת Heartbleed 6](#_Toc57503696)

[מתקפה על מנגנון האימות של TLS 6](#_Toc57503697)

[אבטחת מערכת 7](#_Toc57503698)

[מתקפות MiTM 7](#_Toc57503699)

[מתקפת ARP Poisoning 7](#_Toc57503700)

[מתקפת DNS Poisoning 7](#_Toc57503701)

[מתקפות מניעת שירות 7](#_Toc57503702)

[מתקפת DOS 7](#_Toc57503703)

[מתקפת DDOS 7](#_Toc57503704)

[מתקפת DRDOS 7](#_Toc57503705)

[ביבליוגרפיה 8](#_Toc57503706)

# מבוא

# שפת C++

שפת C++ נוצרה לראשונה בשלהי שנות ה-70, ע"י מדען המחשבים ביארן סטרוסטרופ כשעבד על עבודת הדוקטורט שלו [1]. בעבודתו, הוא נהג להעזר בשפת התכנות Simula, שהייתה אחת מבין שפות התכנות הראשונות שתמכו במודל התכנות-מונחה עצמים. לטעמו, השפה הזו הייתה איטית מידי לשימושים מעשיים ועל כן החליט לעבוד על פיתוח שפה חדשה המובססת על שפת C אשר תאשר שימוש במחלקות. בזמנו, הוא כינה אותה בשם “C with Classes”, ועם השנים שמה שונה ל- C++. כפי שהשם מרמז, מדובר על שפת C עם עוד תוספות ושדרוגים, כפי שעושה האופרטור ++ אשר מגדיל את ערכו של משתנה ב-1.

במהלך השנים, שפת C++ התקדמה והשתדרגה באמצעות עוד תוספות ושדרוגים לשפה כמו: מחלקות, ירושה, מנגנון טיפול בחריגות (Exceptions), פונקציות וירטואליות, העמסת פונקציות, תבניות, ניהול זיכרון ועוד... [2]. במהלך השנים פורסמו מספר סטנדרטים המגדירים את מבנה, תחביר ומאפייני השפה, כשבכל אחד מהם הוספו, עודכנו ושונו הרבה מאוד תכונות בשפה שעזרו לה להתפתח והביאו אותה עד למצב היום. כל 3 שנים, מאז שנת 2011 שבה יצא הסטנדרט C++11, שכלל שינויים גדולים ומשמעותיים, פורסם סטנדרט חדש שהוספו אליו כל התוספות והשינויים שסיימו לפתח עד פרסום הסטנדרט [3]. הסטנדרט האחרון שפורסם ממש לאחרונה (בעת כתיבת המאמר) הוא C++20 [4].

## מבנה ותחביר השפה

## מחלקות, אובייקטים וירושה

## פולימורפיזם

## מודל הזיכרון

## איומי אבטחה

### חולשת Stack Buffer Overflow

[5]

### מתקפת Return-oriented Programming

### דריסת משתנים וטבלאות וירטואליות

[6]

[7]

## מנגנוני אבטחה

# שפת Python

## מבנה ותחביר השפה

## דינאמיות השפה

## מחלקות, אובייקטים וירושה

## איומי אבטחה

### חולשות ב-Deserialization

[8]

### טעינת קובץ זדוני

[9]

### חילוץ קבצים זדוניים

[10]

[11]

[12]

### שימוש בפונקציות מסוכנות

## מנגנוני אבטחה

# תקשורת

## אבטחה בתקשורת

## פרוטוקולי הצפנה ואימות

### אלגוריתם Diffie–Hellman

[13]

### הצפנת RSA

### פרוטוקול SSL

### פרוטוקול TLS

## מתקפות שונות על פרוטוקולי תקשורת

[14]

### מתקפת POODLE

### מתקפת BEAST

### מתקפת CRIME

### מתקפת Heartbleed

### מתקפה על מנגנון האימות של TLS

[15]

[16]

# אבטחת מערכת

## מתקפות MiTM

### מתקפת ARP Poisoning

[17]

[18]

### מתקפת DNS Poisoning

[19]

## מתקפות מניעת שירות

[20]

### מתקפת DOS

### מתקפת DDOS

### מתקפת DRDOS

# ביבליוגרפיה

z

|  |  |
| --- | --- |
| [1] | Albatross, "History of C++," [Online]. Available: http://www.cplusplus.com/info/history/. |
| [2] | Albatross, "C++ - Brief Description," [Online]. Available: http://www.cplusplus.com/info/description/. |
| [3] | "C++11," [Online]. Available: https://en.wikipedia.org/wiki/C++11. |
| [4] | "C++20," [Online]. Available: https://en.wikipedia.org/wiki/C++20. |
| [5] | P. LACROIX and J. DESHARNAIS, "Buffer Overflow Vulnerabilities in C and C++," 7 August 2008. [Online]. Available: http://www2.ift.ulaval.ca/~desharnais/Recherche/RR/DIUL-RR-0803.pdf. |
| [6] | "Exploiting C++ VTABLES: Instance Replacement," 11 May 2013. [Online]. Available: https://defuse.ca/exploiting-cpp-vtables.htm. |
| [7] | C. Zhang, C. Song, K. Z. Chen and Z. Chen, "VTint: Protecting Virtual Function Tables' Integrity," February 2015. [Online]. Available: https://www.researchgate.net/profile/Chengyu\_Song/publication/281784405\_VTint\_Protecting\_Virtual\_Function\_Tables'\_Integrity/links/55f8743d08ae07629dd5e648/VTint-Protecting-Virtual-Function-Tables-Integrity.pdf. |
| [8] | K. Tanaka and T. Saito, "Python Deserialization Denial of Services," in *Computational Science/Intelligence & Applied Informatics*, 2018, pp. 15-25. |
| [9] | A. Shaw, "10 common security gotchas in Python and how to avoid them," 16 June 2018. [Online]. Available: https://hackernoon.com/10-common-security-gotchas-in-python-and-how-to-avoid-them-e19fbe265e03. |
| [10] | A. Abraham, "Exploiting insecure file extraction in Python for code execution," 28 September 2017. [Online]. Available: https://ajinabraham.com/blog/exploiting-insecure-file-extraction-in-python-for-code-execution. |
| [11] | MITRE, "CVE-2019-9674 - denial of service via a ZIP bomb," 4 February 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-9674. |
| [12] | MITRE, "CVE-2019-20907 - TAR archive leading to an infinite loop," 13 July 2020. [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-20907. |
| [13] | Wikipedia, "Diffie–Hellman key exchange," [Online]. Available: https://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman\_key\_exchange. |
| [14] | A. Prodromou, "TLS Security 6: Examples of TLS Vulnerabilities and Attacks," 31 March 2019. [Online]. Available: https://www.acunetix.com/blog/articles/tls-vulnerabilities-attacks-final-part/. |
| [15] | D. Wagner and B. Schneier, "Analysis of the SSL 3.0 Protocol," November 1996. [Online]. Available: https://www.usenix.org/legacy/publications/library/proceedings/ec96/full\_papers/wagner/wagner.pdf. |
| [16] | N. Mavrogiannopoulos, F. Vercauteren, V. Velichkov and B. Preneel, "A cross-protocol attack on the TLS protocol," October 2012. [Online]. Available: https://www.researchgate.net/publication/262208728\_A\_cross-protocol\_attack\_on\_the\_TLS\_protocol. |
| [17] | B. Fleck and J. Dimov, "Wireless Access Points and ARP Poisoning," December 2013. [Online]. Available: https://digilander.libero.it/SNHYPER/files/arppoison.pdf. |
| [18] | C. Nachreiner, "Anatomy of an ARP Poisoning Attack," 18 November 2012. [Online]. Available: http://csci6433.org/Papers/Anatomy%20of%20an%20ARP%20Poisoning%20Attack%20\_%20WatchGuard.pdf. |
| [19] | S. Son and V. Shmatikov, "The Hitchhiker’s Guide to DNS Cache Poisoning," in *Security and Privacy in Communication Networks*, The University of Texas, Austin, 2010, pp. 466-483. |
| [20] | Prolexic, "An Analysis Of DrDoS DNS Reflection Attacks," [Online]. Available: http://vertassets.blob.core.windows.net/download/74db6f36/74db6f36-56e7-4f4f-a6b4-a1880089f28a/analysis\_of\_drdos\_dns\_reflection\_attacks\_white\_paper\_us\_031513.pdf. |