



סילבוס קורס

שם הקורס: אבטחת מידע

שם קורס באנגלית: Information Security

מס' קורס: 202-1-5421

סוג קורס: הרצאה : 2 ש"ש

נק"ז: 2.0

מרצה הקורס: ד"ר מיכאל אורלוב

דרישות קדם: 202-1-2091 ארכיטקטורה במחשבים ומעבדה בתכנות מערכות

סילבוס בעברית

הקורס עוסק בתחום הרחב של אבטחת מידע, ומכסה את הנושאים של קריפטוגרפיה בסיסית, בטיחות תוכנה, אבטחת רשתות ו-web, נזקה, אבטחת מערכות הפעלה, בטיחות בסיסי נתונים וקריית מידע, ואנונימיות ופרטיות ברשת. עם השלמת הקורס, הסטודנט יצבור ידע תאורטי ומעשי בתחום הכללי של אבטחת מידע, יבין את נושאי האבטחה הסובבים ארכיטקטורה של מערכות ופיתוח תוכנה, ויוכל להתמחות בנושאים ספציפיים של אבטחת מידע במקרה הצורך. הקורס כולל תרגילים מעשיים המכסים את החומר הנלמד.

סילבוס באנגלית

The course deals with the broad subject of information security, covering the topics of elementary cryptography, program security, network and web security, malware, operating systems security, database and data mining security, and online anonymity and privacy. Upon completing the course, the student will gain theoretical and practical knowledge in the general area of information security, will understand security issues surrounding systems architecture and software development, and will be able to further specialize in information security subjects if necessary. The course includes practical assignments that cover the material studied.

מטרת ונושא הקורס

לימוד נושאים בתחום של אבטחת מידע, כולל נושאים בסיסיים בהצפנה, אבטחת תוכנה ותהליכים, אבטחת רשתות ואתרי רשת, נזקה ווירוסים, אבטחת מערכות הפעלה, אבטחת בסיסי נתונים וקריית נתונים, ואנונימיות ברשת.

נושאי ההרצאות

Lecture	Subject	References
1	Security problem in computing: what is security, type of attacks, attack classification, security services and tools. The attackers.	[1] Ch. 1
2–3	Elementary cryptography: classic encryption methods, cryptanalysis, rotor machines (Enigma). Symmetric encryption: stream ciphers, Feistel block ciphers, DES, modes of operation. Asymmetric encryption: RSA, Diffie-Hellman, digital signatures. Long messages: secure hashes, MACs.	[1] Ch. 2 [3]
4–5	Program security: memory structure, buffer overflow vulnerabilities and exploitation, stack guards, ASLR.	[1] Ch. 3 [4] 0x300
6–7	Network security: spoofing attacks in different network layers, denial of service, port scanning, DNS infrastructure attacks.	[1] Ch. 6 [4] 0x400
8–9	Web security: web servers, maintaining common state, HTTPS, phishing, XSS/CSRF, SQL injection.	[1] Ch. 4
10	Malware: virus types and principles of propagation, worms and Trojans, methods of malware detection.	[1] Ch. 3
11	Operating systems security: memory and address protection, access control, RBAC, virtual machines.	[1] Ch. 5
12	Databases and data mining security: access control, privacy, statistical inference attacks, multi-level security.	[1] Ch. 7
13	Online anonymity and privacy: anonymity vs. pseudonymity, onion routing, correlation attacks, fingerprinting.	

דרישות הקורס

יהיו במהלך הסמסטר מספר עבודות מעבדה. הגשת העבודות היא ביחידים או בזוגות. סטודנט שיגיש ויקבל ציון עובר בכל עבודות המעבדה יזכה לבונוס של 2 נקודות בציון הסופי (הציון הסופי המקסימלי הוא 100).

הנוכחות בהרצאות היא חובה. מצגות הינן רק חלק מהחומר המועבר בהרצאות. תתכן פגיעה בציון עקב חוסר נוכחות לפי שיקול דעתו של המרצה (עד 15% מהציון). רישום נוכחות יתבצע בתחילת ההרצאות. כל תאום של חוסר נוכחות עקב סיבה מוצדקת יש לעשות לפני ההרצאה הרלוונטית.

מרכיבי ציון הקורס

70% – מבחן סוף סמסטר
30% – תרגילי מעבדה

ציון הסמסטר יחושב לפי הכלל הנ"ל רק בתנאי שציון המבחן יהיה לפחות 56. אחרת ציון המבחן הוא הציון הסופי בקורס.

ספרות הקורס

1. C. P. Pfleeger, S. L. Pfleeger, J Margulies, "[Security in Computing](#)", 5th Edition, Prentice Hall, 2015.

2. R. J. Anderson, "[Security Engineering](#): A Guide to Building Dependable Distributed Systems", 2nd Edition, Prentice Hall, 2008.
3. C. Paar, J. Pelzl, "[Understanding Cryptography](#): A Textbook for Students and Practitioners" ([Springer Link](#)), Springer, 2010.
4. J. Erickson, "[Hacking: The Art of Exploitation](#)", 2nd Edition, No Starch Press, 2008.
5. W. Du et al., [Hands-on Labs for Security Education](#), Syracuse University, online resource, 2017.