San Pablo Catholic University (UCSP)
Undergraduate Program in
Computer Science
SILABO

CS3I1. Computer Security (Mandatory)

2023-I

1. General information		
1.1 School	:	Ciencia de la Computación
1.2 Course	:	CS3I1. Computer Security
1.3 Semester	:	8^{vo} Semestre.
1.4 Prerrequisites	:	CS231. Networking and Communication. (7^{th} Sem)
1.5 Type of course	:	Mandatory
1.6 Learning modality	:	Face to face
1.7 Horas	:	1 HT; 4 HP;
1.8 Credits	:	3
1.9 Plan	:	Plan Curricular 2016

2. Professors

Lecturer

- Julio Omar Santisteban Pablo <jsantisteban@ucsp.edu.pe>
  - PhD in Ciencias de la Computación, Universidad Nacional de San Agustin, Perú, 2021.
  - MSc in Internetworking, University of Technology, Australia, 2008.

3. Course foundation

Nowadays, information is one of the most valuable assets in any organization. This course is oriented to be able to provide the student with the security elements oriented to protect the Information of the organization and mainly to be able to foresee the possible problems related to this heading. This subject involves the development of a preventive attitude on the part of the student in all areas related to software development.

4. Summary

1. Foundational Concepts in Security 2. Principles of Secure Design 3. Defensive Programming 4. Threats and Attacks 5. Network Security 6. Cryptography 7. Web Security 8. Platform Security 9. Digital Forensics 10. Secure Software Engineering

5. Generales Goals

- Discuss at an intermediate intermediate level the fundamentals of Computer Security.
- Provide different aspects of the malicious code.
- That the student knows the concepts of cryptography and security in computer networks.
- Discuss and analyze together with the student the aspects of Internet Security.

6. Contribution to Outcomes

This discipline contributes to the achievement of the following outcomes:

1) Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions. (**Assessment**)

2) Design, implement and evaluate a computing-based solution to meet a given set of computing requirements in the context of the program's discipline. (**Assessment**)

5) Function effectively as a member or leader of a team engaged in activities appropriate to the program's discipline. (**Usage**)

6) Apply computer science theory and software development fundamentals to produce computing-based solutions. (**Assessment**)

7) Develop computational technology for the well-being of all, contributing with human formation, scientific, technological and professional skills to solve social problems of our community. (**Assessment**)

7. Content

UNIT 1: Foundational Concepts in Security (25)

Competences:

Content	**Generales Goals**
• CIA (Confidentiality, Integrity, Availability) • Concepts of risk, threats, vulnerabilities, and attack vectors • Authentication and authorization, access control (mandatory vs. discretionary) • Concept of trust and trustworthiness • Ethics (responsible disclosure)	• Analyze the tradeoffs of balancing key security properties (Confidentiality, Integrity, Availability) [Familiarity] • Describe the concepts of risk, threats, vulnerabilities and attack vectors (including the fact that there is no such thing as perfect security) [Familiarity] • Explain the concepts of authentication, authorization, access control [Familiarity] • Explain the concept of trust and trustworthiness [Familiarity] • Recognize that there are important ethical issues to consider in computer security, including ethical issues associated with fixing or not fixing vulnerabilities and disclosing or not disclosing vulnerabilities [Familiarity]

Readings: W and L (2014)

UNIT 2: Principles of Secure Design (25)	
Competences:	
Content	**Generales Goals**
• Least privilege and isolation • Fail-safe defaults • Open design • End-to-end security • Defense in depth (e.g., defensive programming, layered defense) • Security by design • Tensions between security and other design goals • Complete mediation • Use of vetted security components • Economy of mechanism (reducing trusted computing base, minimize attack surface) • Usable security • Security composability • Prevention, detection, and deterrence	• Describe the principle of least privilege and isolation as applied to system design [Familiarity] • Summarize the principle of fail-safe and deny-by-default [Familiarity] • Discuss the implications of relying on open design or the secrecy of design for security. [Familiarity] • Explain the goals of end-to-end data security [Familiarity] • Discuss the benefits of having multiple layers of defenses [Familiarity] • For each stage in the lifecycle of a product, describe what security considerations should be evaluated. [Familiarity] • Describe the cost and tradeoffs associated with designing security into a product [Familiarity] • Describe the concept of mediation and the principle of complete mediation [Familiarity] • Be aware of standard components for security operations, instead of re-inventing fundamentals operations [Familiarity] • Explain the concept of trusted computing including trusted computing base and attack surface and the principle of minimizing trusted computing base [Familiarity] • Discuss the importance of usability in security mechanism design [Familiarity] • Describe security issues that arise at boundaries between multiple components. [Familiarity] • Identify the different roles of prevention mechanisms and detection/deterrence mechanisms [Familiarity]
Readings: W and L (2014)	

UNIT 3: Defensive Programming (25)

Competences:

Content	**Generales Goals**

• Input validation and data sanitization
• Choice of programming language and type-safe languages
• Examples of input validation and data sanitization errors
  – Buffer overflows
  – Integer errors
  – SQL injection
  – XSS vulnerability
• Race conditions
• Correct handling of exceptions and unexpected behaviors
• Correct usage of third-party components
• Effectively deploying security updates
• Information flow control
• Correctly generating randomness for security purposes
• Mechanisms for detecting and mitigating input and data sanitization errors
• Fuzzing
• Static analysis and dynamic analysis
• Program verification
• Operating system support (e.g., address space randomization, canaries)
• Hardware support (e.g, DEP, TPM)
	• Explain why input validation and data sanitization is necessary in the face of adversarial control of the input channel. [Usage]
	• Explain why you might choose to develop a program in a type-safe language like Java, in contrast to an unsafe programming language like C/C++ [Usage]
	• Classify common input validation errors, and write correct input validation code [Usage]
	• Demonstrate using a high-level programming language how to prevent a race condition from occurring and how to handle an exception [Usage]
	• Demonstrate the identification and graceful handling of error conditions [Familiarity]
	• Explain the risks with misusing interfaces with third-party code and how to correctly use third-party code [Familiarity]
	• Discuss the need to update software to fix security vulnerabilities and the lifecycle management of the fix [Familiarity]

Readings: W and L (2014)

UNIT 4: Threats and Attacks (25)	
Competences:	
Content	**Generales Goals**
• Attacker goals, capabilities, and motivations (such as underground economy, digital espionage, cyberwarfare, insider threats, hacktivism, advanced persistent threats) • Examples of malware (e.g., viruses, worms, spyware, botnets, Trojan horses or rootkits) • Denial of Service (DoS) and Distributed Denial of Service (DDoS) • Social engineering (e.g., phishing) • Attacks on privacy and anonymity • Malware/unwanted communication such as covert channels and steganography	• Describe likely attacker types against a particular system [Familiarity] • Discuss the limitations of malware countermeasures (eg, signature-based detection, behavioral detection) [Familiarity] • Identify instances of social engineering attacks and Denial of Service attacks [Familiarity] • Discuss how Denial of Service attacks can be identified and mitigated [Familiarity] • Describe risks to privacy and anonymity in commonly used applications [Familiarity] • Discuss the concepts of covert channels and other data leakage procedures [Familiarity]
Readings: W and L (2014)	

UNIT 5: Network Security (25)	
Competences:	
Content	**Generales Goals**
• Network specific threats and attack types (e.g., denial of service, spoofing, sniffing and traffic redirection, man-in-the-middle, message integrity attacks, routing attacks, and traffic analysis) • Use of cryptography for data and network security • Architectures for secure networks (e.g., secure channels, secure routing protocols, secure DNS, VPNs, anonymous communication protocols, isolation) • Defense mechanisms and countermeasures (e.g., network monitoring, intrusion detection, firewalls, spoofing and DoS protection, honeypots, tracebacks) • Security for wireless, cellular networks • Other non-wired networks (e.g., ad hoc, sensor, and vehicular networks) • Censorship resistance • Operational network security management (e.g., configure network access control)	• Describe the different categories of network threats and attacks [Familiarity] • Describe the architecture for public and private key cryptography and how PKI supports network security [Familiarity] • Describe virtues and limitations of security technologies at each layer of the network stack [Familiarity] • Identify the appropriate defense mechanism(s) and its limitations given a network threat [Usage]
Readings: W and L (2014)	

UNIT 6: Cryptography (25)

Competences:

Content	Generales Goals
• Basic Cryptography Terminology covering notions pertaining to the different (communication) partners, secure/unsecure channel, attackers and their capabilities, encryption, decryption, keys and their characteristics, signatures • Cipher types (e.g., Caesar cipher, affine cipher) together with typical attack methods such as frequency analysis • Public Key Infrastructure support for digital signature and encryption and its challenges • Symmetric key cryptography – Perfect secrecy and the one time pad – Modes of operation for semantic security and authenticated encryption (e.g., encrypt-then-MAC, OCB, GCM) – Message integrity (e.g., CMAC, HMAC) • Public key cryptography: – Trapdoor permutation, e.g., RSA – Public key encryption, e.g., RSA encryption, EI Gamal encryption – Digital signatures – Public-key infrastructure (PKI) and certificates – Hardness assumptions, e.g., Diffie-Hellman, integer factoring • Authenticated key exchange protocols, e.g., TLS • Cryptographic primitives: – pseudo-random generators and stream ciphers – block ciphers (pseudo-random permutations), e.g., AES – pseudo-random functions – hash functions, e.g., SHA2, collision resistance – message authentication codes – key derivations functions	• Describe the purpose of Cryptography and list ways it is used in data communications [Familiarity] • Define the following terms: Cipher, Cryptanalysis, Cryptographic Algorithm, and Cryptology and describe the two basic methods (ciphers) for transforming plain text in cipher text [Familiarity] • Discuss the importance of prime numbers in cryptography and explain their use in cryptographic algorithms [Familiarity] • Illustrate how to measure entropy and how to generate cryptographic randomness [Usage] • Use public-key primitives and their applications [Usage] • Explain how key exchange protocols work and how they fail [Familiarity] • Discuss cryptographic protocols and their properties [Familiarity]

Readings: W and L (2014)

UNIT 7: Web Security (25)

Competences:

Content	**Generales Goals**
• Web security model – Browser security model including same-origin policy – Client-server trust boundaries, e.g., cannot rely on secure execution in the client • Session management, authentication – Single sign-on – HTTPS and certificates • Application vulnerabilities and defenses – SQL injection – XSS – CSRF • Client-side security – Cookies security policy – HTTP security extensions, e.g. HSTS – Plugins, extensions, and web apps – Web user tracking • Server-side security tools, e.g. Web Application Firewalls (WAFs) and fuzzers	• Describe the browser security model including same-origin policy and threat models in web security [Familiarity] • Discuss the concept of web sessions, secure communication channels such as TLS and importance of secure certificates, authentication including single sign-on such as OAuth and SAML [Familiarity] • Investigate common types of vulnerabilities and attacks in web applications, and defenses against them [Familiarity] • Use client-side security capabilities [Usage]

Readings: W and L (2014)

UNIT 8: Platform Security (25)	
Competences:	
Content	**Generales Goals**
• Code integrity and code signing • Secure boot, measured boot, and root of trust • Attestation • TPM and secure co-processors • Security threats from peripherals, e.g., DMA, IOMMU • Physical attacks: hardware Trojans, memory probes, cold boot attacks • Security of embedded devices, e.g., medical devices, cars • Trusted path	• Explain the concept of code integrity and code signing and the scope it applies to [Familiarity] • Discuss the concept of root of trust and the process of secure boot and secure loading [Familiarity] • Describe the mechanism of remote attestation of system integrity [Familiarity] • Summarize the goals and key primitives of TPM [Familiarity] • Identify the threats of plugging peripherals into a device [Familiarity] • Identify physical attacks and countermeasures [Familiarity] • Identify attacks on non-PC hardware platforms [Familiarity] • Discuss the concept and importance of trusted path [Familiarity]
Readings: W and L (2014)	

UNIT 9: Digital Forensics (25)	
Competences:	
Content	**Generales Goals**
• Basic Principles and methodologies for digital forensics • Design systems with forensic needs in mind • Rules of Evidence - general concepts and differences between jurisdictions and Chain of Custody • Search and Seizure of evidence: legal and procedural requirements • Digital Evidence methods and standards • Techniques and standards for Preservation of Data • Legal and Reporting Issues including working as an expert witness • OS/File System Forensics • Application Forensics • Web Forensics • Network Forensics • Mobile Device Forensics • Computer/network/system attacks • Attack detection and investigation • Anti-forensics	• Describe what is a Digital Investigation is, the sources of digital evidence, and the limitations of forensics [Familiarity] • Explain how to design software to support forensics [Familiarity] • Describe the legal requirements for use of seized data [Familiarity] • Describe the process of evidence seizure from the time when the requirement was identified to the disposition of the data [Familiarity] • Describe how data collection is accomplished and the proper storage of the original and forensics copy [Familiarity] • Conduct data collection on a hard drive [Usage] • Describe a person's responsibility and liability while testifying as a forensics examiner [Familiarity] • Recover data based on a given search term from an imaged system [Usage] • Reconstruct application history from application artifacts [Familiarity] • Reconstruct web browsing history from web artifacts [Familiarity] • Capture and interpret network traffic [Familiarity] • Discuss the challenges associated with mobile device forensics [Familiarity]
Readings: W and L (2014)	

UNIT 10: Secure Software Engineering (25)	
Competences:	
Content	**Generales Goals**
• Building security into the software development lifecycle • Secure design principles and patterns • Secure software specifications and requirements • Secure software development practices • Secure testing- the process of testing that security requirements are met (including static and dynamic analysis).	• Describe the requirements for integrating security into the SDL [Familiarity] • Apply the concepts of the Design Principles for Protection Mechanisms, the Principles for Software Security (Viega and McGraw), and the Principles for Secure Design (Morrie Gasser) on a software development project [Familiarity] • Develop specifications for a software development effort that fully specify functional requirements and identifies the expected execution paths [Familiarity]
Readings: W and L (2014)	

8. Methodology

1. El profesor del curso presentará clases teóricas de los temas señalados en el programa propiciando la intervención de los alumnos.
2. El profesor del curso presentará demostraciones para fundamentar clases teóricas.
3. El profesor y los alumnos realizarán prácticas
4. Los alumnos deberán asistir a clase habiendo leído lo que el profesor va a presentar. De esta manera se facilitará la comprensión y los estudiantes estarán en mejores condiciones de hacer consultas en clase.

9. Assessment

Continuous Assessment 1 : 20 %

Partial Exam : 30 %

Continuous Assessment 2 : 20 %

Final exam : 30 %

References

W, Stallings. and Brown. L (2014). *Computer Security: Principles and Practice*. Pearson Education, Limited. ISBN: 9780133773927.