UČNI NAČRT PREDMETA / COURSE SYLLABUS	
Predmet:	Varnost komponent
Course title:	Component Security

Študijski program in stopnja **Study programme and level**	**Študijska smer** **Study field**	**Letnik** **Academic year**	**Semester** **Semester**
Kibernetska varnost, magistrski študijski program druge stopnje	-	Prvi	Drugi
The second cycle masters study programme Cyber Security	-	First	Second

Vrsta predmeta / Course type	Obvezni / Obligatory
Univerzitetna koda predmeta / University course code:	5-KV-MAG-VK-2021-12-14

Predavanja **Lectures**	**Seminar** **Seminar**	**Vaje** **Tutorial**	**Klinične vaje** **work**	**Druge oblike študija**	**Samost. delo** **Individ. work**	**ECTS**
30	/	30	/	/	90	5

Nosilec predmeta / Lecturer:	doc. dr. Rok Bojanc

Jeziki / **Languages:**	**Predavanja / Lectures:**	Slovenski / Angleški
	Vaje / Tutorial:	Slovenski / Angleški

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	**Prerequisites:**

Za vključitev v delo je potrebo usvojit zanje predmeta Varnost sistemov. Študent/študentka mora pred pristopom k izpitu pripraviti in zagovarjati seminarsko nalogo.	In order to be included in the work, it is necessary to master the content of the course System security. Prior to the exam, the student has to prepare and present seminar work

Vsebina:	**Content (Syllabus outline):**
• Ranljivosti komponent sistema - identifikacija groženj varnosti artefaktov oblikovanja komponent. • Varen življenjski cikel komponente (od ideje, načrtovanja, izdelave, delovanja, vzdrževanja, do odstranitve). • Načela načrtovanja varnih komponent - načela, kot so vzpostavitev trdne varnostne politike, obravnavanje varnosti kot sestavnega dela zasnove sistema. • Varnost upravljanja dobavne verige komponent (strategije, kot je fizična varnost, porazdeljena proizvodnja, sledljivost, pregledovanje tovora in validacija ter pregledi za odkrivanje in preprečevanje ogrožanja varnosti komponent med postopkom naročanja). • Varnostno testiranje komponent s poudarkom na tehnikah in orodjih za testiranje varnostnih lastnosti komponente. • Obratno inženirstvo s poudarkom na orodjih in tehnikah raziskovanja dizajna komponent.	• Vulnerabilities of system components - identification of security threats to component design artifacts. • Secure component life cycle (from idea, design, fabrication, operation, maintenance, to disposal). • Principles of safe component design - principles such as establishing a sound security policy, treating security as an integral part of system design. • Security of component supply chain management strategies such as physical security, split manufacturing, traceability, cargo screening and validation, and inspections to detect and prevent compromises of component security during the procurement process). • Component safety testing with emphasis on techniques and tools for testing component safety properties. • Reverse engineering with an emphasis on component design research tools and techniques.

Temeljni literatura in viri / Readings:

- Szefer, J. Principles of Secure Processor Architecture Design, Morgan & Claypool Publisher, 2018 (izbrana poglavja)
- Adkins,H,. Beyer, B., Blankinship, P., Lewandowski, P., Oprea, A., Stubblefield,A. Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems, 1.st edition, O'Reilly, 2020 (izbrana poglavja)
- Johnson, L. Security Controls Evaluation, Testing and Assessment Handbook, 2nd edition, Academic Press, 2019 (izbrana poglavja)
- Ng, K. The Art of PCB Reverse Engineering: Unravelling the Beauty of the Original Design, Createspace Independent Publishing Platform, 2015 (izbrana poglavja)
- Prosojnice iz predavanj in vaj pri predmetu Varnost komponent, Moodle, FIŠ.

Cilji in kompetence:

Učna enota prispeva k razvoju naslednjih splošnih in predmetno specifičnih kompetenc:

Splošne kompetence:
- Poglobljeno razumevanje delovanja organizacijskih informacijskih sistemov, komponent in omrežij.
- Sposobnost uporabe različnih programskih rešitev za zagotavljanje, upravljanje, nadzorovanje in evalvacijo kibernetske varnosti
- Sposobnost fleksibilne uporabe pridobljenega znanja o kibernetski varnosti v praksi

Predmetno-specifične kompetence:
- Sposobnost razložiti, kako lahko varnost komponent sistema vpliva na varnost sistema.
- Sposobnost razložiti faze življenjskega cikla komponente.
- Sposobnost uporabe več tehnik za preizkušanje varnostnih lastnosti
- Zmožnosti navajanja artefaktov načrtovanja komponent, ki bi lahko zahtevale zaščito
- Zmožnost uporabe skupnih točk ranljivosti v dobavni verigi komponente.
- Sposobnost navajanja varnostnih tveganj v komponenti dobavne verige.
- Sposobnost uporabe različnih tehnik za testiranje varnostnih lastnosti komponente.

Objectives and competences:

The instructional unit contributes to the development of the following general and subject-specific competences:

General competences:
- In-depth understanding of the functioning of organizational information systems, components and networks.
- The ability to use various software solutions to provide, manage, monitor and evaluate cyber security
- The ability of flexible usage of the acquired knowledge on cyber security in practice

Subject-specific competences:
- The ability to explain how the security of a system's components might impact the security of the system.
- The ability to explain the phases of a component's lifecycle.
- The ability to use several techniques for testing security properties
- The ability to list component design artifacts which may require protection
- The ability to explain common points of vulnerability in a component's supply chain.
- The ability to list security risks in a component supply chain component.
- The ability to use different techniques for testing security properties of a component.

Predvideni študijski rezultati:

Znanje in razumevanje:

- razlage načinov, pri katerih je lahko ogrožena zaupnost zasnove komponente;
- opisa načinov pridobivanja informacij o funkcionalnosti komponente z omejenimi informacijami o njeni zasnovi in izvedbi;
- razlage tehnik za zaščito konstrukcijskih elementov integriranega vezja;
- opisa varnostnih tveganj v dobavni verigi komponent;
- obrazložitve opisa med statično in dinamično analizo v programski opremi za obratni inženiring.

Intended learning outcomes:

Knowledge and understanding:

- to describe ways in which the confidentiality of a component's design may be compromised;
- to list ways to learn information about component's functionality with limited information about its design and implementation;
- to describe techniques for protecting the design elements of an integrated circuit;
- to list security risks in a component supply chain;
- to explain between static and dynamic analysis in reverse engineering software.

Metode poučevanja in učenja:

- *Predavanja z aktivno udeležbo študentov* (razlaga, diskusija, vprašanja, primeri, reševanje problemov);
- *Vaje*, kjer študentje na primerih ponovijo temeljne koncepte, predstavljene na predavanjih;
- *Seminarska naloga,* kjer študenti predstavijo pridobljeno znanje

Learning and teaching methods:

- *Lectures with active participations by the students* (explanation, discussion, questions, cases, problems solving);
- *Tutorials*, where students will recall, reinforce, and shed light on the concepts and methods introduced at lectures;
- *Seminar work*, where students present the acquired knowledge

Načini ocenjevanja: Delež (v %) / Weight (in %) **Assessment:**

Način (pisni izpit, ustno izpraševanje, naloge, projekt):		Type (examination, oral, coursework, project):
Pisni izpit	60 %	Written Exam
Seminarska naloga	40 %	Seminar work

Reference nosilca / Lecturer's references:

- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. A quantitative model for information-security risk management. Engineering management journal. 2013, vol. 25, no. 3, str. 25-37. ISSN 1042-9247. [COBISS.SI-ID 26755879]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka, TEKAVČIČ, Metka. Managing the investment in information security technology by use of a quantitative modeling. Information

processing & management. [Print ed.]. 2012, vol. 48, no. 6, str. 1031-1052. ISSN 0306-4573. DOI: 10.1016/j.ipm.2012.01.001. [COBISS.SI-ID 25578535]

- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. Towards a standard approach for quantifying an ICT security investment. Computer standards & interfaces. [Print ed.]. 2008, vol. 30, no. 4, str. 216-222. ISSN 0920-5489. [COBISS.SI-ID 21277735]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. An economic modelling approach to information security risk management. International journal of information management. [Print ed.]. 2008, vol. 28, no. 5, str. 413-422. ISSN 0268-4012. [COBISS.SI-ID 21486887]
- JERMAN-BLAŽIČ, Borka, MATSKANIS, Nikolaos, BOJANC, Rok. Semantic ontology design for a multi-cooperative first responder interoperable platform. Computing and informatics. 2016, vol. 35, no. 6, str. 1249-1276. ISSN 1335-9150. [COBISS.SI-ID 30268711]
- BOJANC, Rok, MÖREC, Barbara, TEKAVČIČ, Metka, JERMAN-BLAŽIČ, Borka. Model določitve optimalnega obsega vlaganj v informacijsko varnost. IB revija : za strokovna in metodološka vprašanja gospodarskega, prostorskega in socialnega razvoja Slovenije. [Slovenska tiskana izd.]. 2012, letn. 46, št. 3/4, str. 53-61, tabele, graf. prikazi. ISSN 1318-2803. [COBISS.SI-ID 21276134]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka. Quantitative model for economic analyses of information security investment in an enterprise information system. Organizacija : revija za management, informatiko in kadre. [Tiskana izd.]. nov.-dec. 2012, letn. 45, št. 6, str. 276-288, ilustr. ISSN 1318-5454. [COBISS.SI-ID 26317095]
- BOJANC, Rok. Kvantitativni model za upravljanje informacijskovarnostnih tveganj. Uporabna informatika. [Tiskana izd.]. apr./maj/jun. 2012, letn. 20, št. 2, str. 82-98, ilustr. ISSN 1318-1882. [COBISS.SI-ID 36236805]
- BOJANC, Rok, JERMAN-BLAŽIČ, Borka, TEKAVČIČ, Metka. Informacijska varnost v podjetniškem okolju : potrebe, ukrepi in ekonomika vlaganj. Ljubljana: Ekonomska fakulteta, 2014. Znanstvene monografije Ekonomske fakultete. ISBN 978-961-240-284-6. http://maksi2.ef.uni-lj.si/zaloznistvoslike/440/E-verzija_Monografija_Bojanc%20in%20soav_Informacijska%20varnost%20v%20podjetniskem%20okolju_feb2015.pdf. [COBISS.SI-ID 276133632]
- BOJANC, Rok. Analysis of research on e-invoicing in Slovenia = Analiza raziskav o izdajanju e-računov v Sloveniji. V: AŠKERC ZADRAVEC, Katarina (ur.). EECME conference 2021 : sustainable development in modern knowledge s : conference abstracts. Ljubljana: Ljubljana School of Business, 2021. [COBISS.SI-ID 67225603]
- BOJANC, Rok. Prototype of common IT-platform and test results. V: ITS Adriatic Multiport Gateway : technical workshop. Bruxelles: [s. n.]. 2013, str. 1-15. [COBISS.SI-ID 37142277]
- BOJANC, Rok. Analysis of e-invoicing as a driver for digital transformation. V: BELE, Darko (ur.), WEIS, Lidija (ur.). Sustainable development in a modern knowledge society : collective monograph. Ljubljana: Ljubljana School of Business, 2021. Str. 65-76, ilustr. ISBN 978-961-7110-02-9. [COBISS.SI-ID 70041603]