VARNOST PODATKOV

UČNI NAČRT PREDMETA/COURSE SYLLABUS

Predmet:	Varnost podatkov
Course title:	Data Security
Članica nosilka/UL Member:	UL FRI

Študijski programi in stopnja	Študijska smer	Letnik	Semestri	Izbirnost
Računalništvo in informatika, prva stopnja, visokošolski strokovni (v postopku)	Ni členitve (študijski program)		1. semester	izbirni

Univerzitetna koda predmeta/University course code:	0643450
Koda učne enote na članici/UL Member course code:	63775

Predavanja /Lectures	Seminar /Seminar	Vaje /Tutorials	Klinične vaje /Clinical tutorials	Druge oblike študija /Other forms of study	Samostojno delo /Individual student work	ECTS
45		30			105	6

Nosilec predmeta/Lecturer:	Denis Trček
Vrsta predmeta/Course type:	izbirni-strokovni/elective-vocational

Jeziki/Languages:	Predavanja/Lectures:	Angleščina, Slovenščina
	Vaje/Tutorial:	Angleščina, Slovenščina

Pogoji za vključitev v delo oz. za opravljanje študijskih obveznosti:	Prerequisites:
Vpis v letnik.	Enrollment in the study year.

Vsebina:	Content (Syllabus outline):
Uvod in motivacija. Osnovne varnostne storitve. Pregled zgodovinskih šifer. Napadi in kriptoanaliza zgodovinskih šifer. Načela sodobne kriptografije. Sklepanje o varnosti in modeli groženj. Notacija. Serializacija podatkov. Tajnost in informacijsko-teoretska varnost. Definicija šifre. Šifra OTP. Informacijsko-teoretska varnost. Popolna tajnost, Shannonov izrek. Model grožnje in napad zgolj s tajnopisom. Omejitve šifre OTP. Simetrične šifre. Tokovne šifre in psevdonaključnost. Računske šifre in računska varnost. Enkratna semantična varnost. Napadi na tokovne šifre. Bločne šifre, psevdonaključne funkcije in permutacije. Podlaganje. Primeri bločnih šifer. Večkratna semantična varnost in napad z izbranim čistopisom. Vključevanje naključnosti, vrednosti NONCE in IV.	Motivation. Basic security services. Overview of historic ciphers. Attacks on and cryptoanalysis of historic ciphers. Principles of modern cryptography. Reasoning about security and threat models. Notation. Data serialization. Confidentiality and Information theoretic security. Ciphers. Vernam's One-Time pad. Information Theoretic Security. Perfect secrecy and Shannon's theorem. Ciphertext-only attack. Limitations of OTP. Symmetric ciphers. Stream ciphers and pseudorandomness. Computational ciphers and computational security. One-time semantic security. Attacks on stream ciphers. Block ciphers, pseudorandom functions and permutations. Padding. Block cipher examples. Semantic security for many-time key, chosen-plaintext attack. Randomized

Načini delovanja: Elektronska kodirna knjiga, veriženje tajnopisnih blokov, števčni način. Integriteta in zgoščevanje. Primeri uporabe in pomen overjenega sporočila. Shema overitvene kode sporočila. Model grožnje: napad z izbranim sporočilom in stvarno ponarejanje. Shema MAC iz psevdonaključne funkcije. CBC-MAC. Napad s podaljšanjem sporočila. Zgoščevalne funkcije, kolizijska odpornost. Konstrukcija in standard Hash-MAC. Splošni napad na kolizijo. Napadi na preverjanje vrednoti MAC: napad po stranskem kanalu in napadi z merjenjem časa. Overjeno šifriranje. Celovitost tajnopisa in overjeno šifriranje. Napad z izbranim tajnopisom. Konstrukcije: šifriraj zatem OKS, OKS in šifriraj, OKS zatem šifriraj. Standardi GCM, CCM, EAX. Overjeno šifriranje s pridruženimi podatki. Asimetrično šifriranje. Primeri uporabe. Definicija asimetrične šifre. Semantična varnost asimetrične šifre. Asimetrično šifriranje in varnost zoper napad z izbranim tajnopisom. Funkcije (FSV) in permutacije (PSV) s skrivnimi vrati. Asimetrična šifra na osnovi FSV in hibridna šifra. RSA, varnostna domneva in primeri. Protokoli za dogovor o ključu. Problem upravljanja s ključi. Stalno razpoložljive zaupanja vredne entitete: idejni protokol, varnostna analiza in omejitve. Protokol Diffie-Hellman: varnostna analiza in odprta vprašanja. Izmenjava ključev z asimetričnim šifriranjem: varnostna analiza in odprta vprašanja. Tehnike razširitve ključa. Digitalni podpis. Shema digitalnega podpisa in primerjava s shemo overitvene kode sporočila. Javna preverljivost ter neovrgljivost. Model grožnje: napad z izbranim sporočilom in stvarno ponarejanje. Paradigma zgosti-in-podpiši. Tehnika FDH, RSA FDH. RSA PKCS#1 v1.5. Verjetnostna podpisna shema. Standarda DSA, ECDSA. Overitev. Overitev uporabnika, podatkov in sporočil. Faktorji overitve (nekaj, kar vem, kar imam, kar sem) in koncept močne overitve. Gesla in vnaprej razdeljeni ključi: Enkratna gesla, gesla na osnovi protokola izziv-odgovor, napadi na gesla, tehnike shranjevanja gesel. Overitev z asimetrično kriptografijo. Overitev na podlagi javnih ključev. Ročni pristop v SSH. Centraliziran pristop z infrastrukturo javnih ključev (PKI). Digitalna potrdila. Porazdeljeni pristop z mrežo zaupanja (WOT). Hibridni pristopi. Primeri komunikacijskih protokolov. SSL/TLS: pregled, uporabljeni gradniki in protokoli, certifikati TLS, varnost in znani napadi. Šifriranje elektronske pošte: Protokola S/MIME, in PGP ter njune omejitve. Primeri protokolov za ohranjanje zasebnosti. Kompromis med varnostjo in zasebnostjo. Težava z zasebnostjo pri protokolu TLS idr. Varnost od	encryption: nonces, initialization vectors. Modes of operation: electronic code book, cipher block chaining, counter mode. Integrity and hashing. Use cases and the meaning of message authenticity. Message Authentication Code. Chosen-message attack and existential forgery. Secure MACs from secure PRFs. CBC-MAC.Length-extension attacks. Hash functions, collision resistance. Hash-MAC and HMAC standard. Generic attacks on collision resistance. Attacks on MAC verification: side-channel and timing-attacks. Authenticated encryption. Ciphertext integrity and authenticated encryption. Chosen-ciphertext attack. Constructions: Encrypt then MAC, MAC and encrypt, MAC then encrypt. Standards GCM, CCM, EAX. Authenticated enc. with associated data. Public Key Encryption. Use cases. Public Key (PK) cipher. Semantic security for PK encryption. Chosen-ciphertext security for PK encryption. Secure trapdoor functions (TDF) and trapdoor permutations (TDP). Public-key cipher from secure TDF, hybrid encryption. RSA, security assumption and examples. Key-exchange protocols. The key management problem. On-line Trusted Third Parties (TTP): Example protocol, security analysis, and limitations. The Diffie-Hellman protocol: security analysis and open issues. Key exchange with public key encryption: security analysis, and open issues. Key derivation techniques. Digital signatures. Digital signature scheme. Comparison to MACs. Public verifiability and non-repudiation. Chosen message attack and existential forgery. Hash-and-sign paradigm. Full Domain Hash. RSA Full Domain Hash. RSA PKCS#1 v1.5 signatures. Probabilistic Signature Schemes. Standards DSA, ECDSA. Authentication. Authenticating users, data and messages. Authentication factors (knowledge, ownership, inherence) and strong authentication. Passwords and pre-shared keys: one-time passwords, challenge-response passwords, attacks against passwords. Storing passwords. Authentication with public key cryptography. Authentication with public keys. The manual approach in SSH. Centralized approach with Public-Key Infrastructure (PKI). Digital certificates. Distributed approach with Web of Trust (WOT). Hybrid approaches. Example communication protocols. SSL/TLS: overview, primitives and protocols, TLS certificates, security and attacks. Encrypted email: S/MIME and PGP, and corresponding issues. Example privacy preserving protocols. Privacy vs. security trade-off. Privacy issues in TLS and similar protocols. End-to-end security. Deniability. Perfect forward secrecy. Off-the-Record messaging protocol.

začetka do konca. Zanikanje. Tajnost za naprej. Protokol OTR. Nadzor dostopa. Fizična in logična varnost podatkov. Vrste in modeli nadzora dostopa. Seznami za nadzor dostopa (ACL). Povezava z overitvijo in avtorizacijo. Načelo najmanjšega privilegija. Varnost podatkovnih nosilcev. Šifriranje diskov in datotek z uporabo ustreznih šifer in obstoječih orodij za šifriranje. Izbris podatkov: ničenje, naključno prepisovanje, zaščita pred napadi za obnovitev podatkov. Maskiranje podatkov: zamenjava, tokenizacija, šifriranje. Primeri: vdori in slabe prakse šifriranja, brisanja in maskiranja.	Access control. Physical data security and logical data security. Access control types and models. Access control Lists (ACLs). Relation to authentication and authorization. Least privilege principle. Information Storage security. Disk and file encryption, using appropriate ciphers, and existing encryption tools. Data erasure: zeroing, random overwriting, protection from data recovery attacks. Data masking: substitution, tokenization, encryption. Real-world examples of data breaches, and poor usages of encryption, erasure and masking.

Temeljna literatura in viri/Readings:

1. Katz, Jonathan, and Yehuda Lindell. Introduction to modern cryptography. CRC press, 2020.
2. Stallings, William, et al. Computer security: principles and practice. Vol. 3. Upper Saddle River: Pearson, 2012.
3. Wong, David. Real-world cryptography. Simon and Schuster, 2021.
4. Trček, Denis. Managing information systems security and privacy. Springer Science & Business Media, 2006.
5. Boneh, Dan, and Victor Shoup. A graduate course in applied cryptography. Draft 0.6: http://toc.cryptobook.us, 2020.

Cilji in kompetence:	**Objectives and competences:**
• Študentom podati osnovo za razumevanje konceptov sodobne kriptografije, tako da spoznajo osnovne primitive in metode, njihovo delovanje, njihova varnostna zagotovila in model groženj, v katerem so dana, pri čemer je poudarjen praktični in aplikacijsko usmerjen vidik; • Študente naučiti, kako izbrati in pravilno uporabiti primitive v praksi ter razviti občutek, kdaj se posvetovati s strokovnjakom (da se zavedajo meja lastnega znanja); • Študentom pokazati nevarnosti izumljanja lastnih primitivov in metod ter pasti implementacije, ter vzpodbuditi zavedanje, da vedno uporabijo preverjene in odprte kriptografske knjižnice; • Študente seznaniti z varnostnimi storitvami na višjih ravneh (npr. overitev, avtorizacija, nadzor dostopa, primeri varnih komunikacijskih protokolov in varnost shranjevanja informacij) in načini njihove uporabe v praksi.	• To provide students the basis for understanding modern cryptography concepts, so they know which primitives and methods exist, how they work, what makes them secure and under what threat model, while putting emphasis on the practical and application-oriented aspects; • To teach students how to choose and correctly apply primitives in practice as well as develop a sense of when to consult a specialist (to be aware of the limits of their own knowledge); • To show students the dangers of trying to invent and implement cryptographic methods and demonstrate why one should always use vetted and open libraries; • To familiarize students with higher-level security services (e. g. authentication, authorization, access control, example communication protocols, and information storage security) and means to apply them in practice.

Predvideni študijski rezultati:	**Intended learning outcomes:**
Po uspešno zaključenem predmetu bodo študenti: • razumeli, kako sodobna kriptografija pristopa k varnosti; • znali opisati kriptografske primitive, ki se uporabljajo za zagotavljanje zaupnosti, celovitosti, digitalnega podpisovanja, dogovarjanja o ključu in jih v omejenem obsegu	After successful completion of the course, students will be able to: • gain an understanding of how modern cryptography approaches security; • describe cryptographic primitives used for providing confidentiality, integrity, digital signing, keys negotiation, and, in a limited scope, apply

uporabiti v praksi za reševanje problemov informacijske varnosti; • znali opisati in primerjati različne načine overjanja uporabnikov s poudarkom na uporabi gesel; • znali opisati in primerjati različne mehanizme, kako uporabnikovo identiteto povežemo z njegovim javnim ključem; • znali opisati delovanje nekaterih sodobnih varnih komunikacijskih protokolov; • znali pojasniti razliko med varnostjo in zasebnostjo v kriptografiji ter opisati komunikacijski protokol, ki ohranja zasebnost; • znali opisati proces nadzora dostopa in njegove različne vrste; • znali opisati različne tehnike za zaščito informacij na podatkovnih nosilcih.	them in practice to solve information security problems; • describe and compare various user authentication methods with emphasis on using passwords; • describe and compare different methods of connecting user identity to their public keys; • describe how certain modern secure communication protocols work; • describe the difference between security and privacy and describe a privacy-preserving communication protocol; • describe the process of access control and its various types; • describe various techniques used for protecting information stored on disks and files.

Metode poučevanja in učenja:	**Learning and teaching methods:**
Predavanja, praktične vaje in demonstracije, projektni način dela pri seminarjih in vajah.	Lectures, lab work, home assignments, project work.

Načini ocenjevanja:	**Delež/Weight**	**Assessment:**
Način (pisni izpit, ustno izpraševanje, naloge, projekt)		Type (examination, oral, coursework,project)
Sprotno preverjanje (domače naloge, projektno delo)	50,00 %	Continuous (home assignments, project work)
Končno preverjanje (pisni izpit)	25,00 %	Final (written exam)
Končno preverjanje (ustni izpit)	25,00 %	Final (oral exam)
Ocene: 6-10 pozitivno, 5 negativno (v skladu s Statutom UL)		Scale: 6-10 pass, 5 and below fail (According to the rules and ordnances of the University of Ljubljana)

Reference nosilca/Lecturer's references:

- TRČEK, Denis. Lightweight protocols and privacy for all-in-silicon objects. Ad hoc networks, ISSN 1570-8705, July 2013, vol. 11, no. 5, str. 1619-1628, ilustr. http://www.sciencedirect.com/science/journal/15708705, doi: 10.1016/j.adhoc.2013.02.005, Elsevier.
- JELENC, David, HERMOSO, Ramón, SABATER-MIR, Jordi, TRČEK, Denis. Decision making matters: a better way to evaluate trust models. Knowledge-based systems, ISSN 0950-7051, Elsevier, 2013, vol. 52, str. 147-164.
- TRČEK, Denis, BRODNIK, Andrej. Hard and soft security provisioning for computationally weak pervasive computing systems in e-health. IEEE Wireless Communications, ISSN 1536-1284. [Print ed.], Aug. 2013, vol. 20, no. 4, 8, IEEE.
- JELENC, David, TRČEK, Denis. Qualitative trust model with a configurable method to aggregate ordinal data. Autonomous agents and multi-agent systems. Sep. 2014, vol. 28, iss. 5, str. 805-835, ilustr. ISSN 1387-2532. https://link.springer.com/article/10.1007/s10458-013-9239-8, DOI: 10.1007/s10458-013-9239-8.
- HUČ, Aleks, TRČEK, Denis. Anomaly detection in IoT networks : from architectures to machine learning transparency. IEEE Access, IEEE, ISSN 2169-3536, Apr. 2021, vol. 9, str. 60607-60616, https://ieeexplore.ieee.org/document/9406023, doi: 10.1109/ACCESS.2021.3073785.
- TRČEK, Denis. Mollitia: Toward standardization of resilience provisioning in IoT/CPS structures. IEEE Internet of Things magazine, IEEE, ISSN 2576-3180, Sep. 2021, vol. 4, no. 3, str. 109-113, ilustr. https://ieeexplore.ieee.org/document/9530712, doi: 10.1109/IOTM.0101.2100037.