ÜSKÜDAR ÜNİVERSİTESİ

SİBER GÜVENLİK YÜKSEK LİSANS PROGRAMI DERS İÇERİKLERİ

MASTER OF SCIENCE PROGRAM IN CYBER SECURITY COURSE CONTENTS

SIB500 Araştırma Yöntemleri ve Bilimsel Etik

Bilimsel araştırma, bilimsel araştırma yöntemlerinin safhaları, bilim etiği konuları işlenecek olup, tez yazım kurallarına uygun akademik çalışma yeterliliğine yönelik içerik haftalık akışta detaylandırılmıştır.

CYS500 Research Methods and Scientific Ethics

Thesis necessities, scientific research, scientific reserach methods, ethics of science are some of the basic topics of the lectures; details are given at the weekly flow.

SIB501 Siber Sistemler ve Bilgi Güvenliği

Bu ders siber sistemlerin temellerini ve bilgi güvenliğini kapsayacaktır. Siber sistemler ve bilgi güvenliği konusunda güçlü bir temel oluşturur. Bu dersin amacı güvenlik ve risk yönetimi, varlık güvenliği, kimlik ve erişim yönetimi, güvenlik değerlendirmesi ve testi, kriptografi, penetrasyon testi, mobil güvenlik, sosyal mühendislik, yasal ve etik konulardır.

CYS501 Cyber Systems and Information Security

This course will cover fundamentals of cyber systems and information security. The course provides a strong foundation in cyber systems and information security. The focus of the course is security and risk management, asset security, identity and access management, security assessment and testing, cryptography, penetration testing, mobile security, social engineering, legal and ethical issues.

SIB502 Seminer

Seminer dersi siber güvenlik alanında bölüm içindeki öğretim üyelerinden veya dışarıdan gelen konuşmacıların yeni araştırma sonuçlarını sunmalarını hedeflemektedir.

CYS502 Seminar

A series of lectures in cyber security is given by faculty or outside speakers.

SIB503 Kriptografiye Giriş

Kriptografiye tarihsel giriş: genel ilkeler, monografik-poligrafik sistemler, monoalfabetik-polyalfabetik sistemler, ikame şifreleri, transpozisyon şifreleri, frekans analizi, kasiski analizi. Blok şifreler: difüzyon, karışıklık, feistel yapısı. Akış şifreleri: kaydırma kayıtları, senkron ve kendi senkron şifreleri, doğrusal karmaşıklık. Boolean fonksiyonları: doğrusal olmama, Walsh dönüşümü, kriptografik kriterler. Açık anahtarlı şifreleme: temel kavramlar, np- hard problemler, kesikli logaritma, faktörleşme, alt toplam, rsa, diffie hellman anahtar değişim

protokolü, dsa, şifreleme protokolleri. Kriptanaliz. Algoritmaların değerlendirilmesinde istatistiksel testler.

CYS503 Introduction to Cryptography

Historical Introduction to Cryptography: General Principles, Monographic-Polygraphic Systems, Monoalphabetic-Polyalphabetic Systems, Substitution Ciphers, Transposition Ciphers, Frequency Analysis, Kasiski Analysis. Block Ciphers: Diffusion, Confusion, Feistel Structure. Stream Ciphers: Shift Registers, Synchronous and Self-synchronous Ciphers, Linear Complexity. Boolean Functions: Nonlinearity, Walsh Transform, Cryptographic Criteria. Public Key Cryptography: Fundamental Concepts, NP-Hard Problems, Discrete Logarithm, Factorization, Subset Sum, RSA, Diffie Hellman Key Exchange Protocol, DSA, Cryptographic Protocols. Cryptanalysis. Statistical Tests for the Evaluation of the Algorithms.

SIB504 Uygulama Güvenliği

Bu derste öğrenciler, zararlı veya kötü amaçlı olarak nitelendirilebilecek bir bilgisayar kodunu anlayabileceklerdir. Hem teknik hem de teknik olmayan saldırılar tartışılacaktır. Öğrenciler bir kurumun kendisini bu saldırılara karşı nasıl koruyabileceğini öğreneceklerdir. Öğrenciler uç nokta cihaz güvenliği, bulut altyapısı güvenliği, büyük veri sistemlerini güvence altına almak ve sanal ortamları güvence altına almak için gerekli kavramları öğreneceklerdir.

CYS504 Application Security

In the Application Security Course, students will gain an understanding of computer code that can be described as harmful or malicious. Both technical and non-technical attacks will be discussed. Students will learn how an organization can protect itself from these attacks. Students will learn concepts in endpoint device security, cloud infrastructure security, securing big data systems, and securing virtual environments.

SIB505 Ağ Güvenliği

Bu ders ağ güvenliğinin temellerini kapsayacaktır. Ders, ağ güvenliği konusunda güçlü bir temel sağlar. Aşağıdaki konular ele alınmaktadır: şifreleme teknikleri, anahtar yönetimi ve kimlik doğrulama, karma, genel anahtar şifrelemesi, web güvenliği, TCP / IP, DDoS saldırıları, DNS güvenliği.

CYS505 Network Security

This course will cover fundamentals of network security. The course provides a strong foundation in network security. The following topics are covered: encryption techniques, key management and authentication, hashing, public key cryptography, web security, TCP/IP, DDoS attacks, DNS security.

SIB506 Kodlama Teorisi

Ders, lineer blok kodları, döngüsel kodlar ve konvolüsyon kodları ile temel matematiğe yönelik cebirsel kodlama teorisine giriş yapar. İşlenen konular şunlardır: Kodlama

parametreleri için sınırlar; Hamming kodlarının özellikleri, kodlanması ve kodlarının çözülmesi; Reed-Muller kodları; BCH kodları ve Reed-Solomon kodları; Berlekamp-Massey algoritması ve kod çözme için Viterbi algoritması. Sonlu alanlar. Sonlu alanlar üzerinde doğrusal cebir. Kuvvet serilerinin halkaları.

CYS506 Coding Theory

The course gives an introduction to algebraic coding theory for linear block codes, cyclic codes and convolution codes, as well as to the underlying mathematics. Topics covered include: Bounds for coding parameters; properties, coding and decoding of Hamming codes; Reed-Muller codes; BCH codes and Reed-Solomon codes; Berlekamp-Massey algorithm and Viterbi algorithm for decoding. Finite fields. Linear algebra over finite fields. Rings of power series.

SIB507 Adli Bilişim

Adli bilişim ve dolandırıcılık soruşturmaları, sayısal adli muayene araçları ile çalışma, adli bilişim muayene süreci, adli bilişim ilkeleri, sayısal belgeler, yazışma ve iletişim, kanıt toplama ve güvenlik ilkeleri, veri analizi, ağdan adli kanıt toplama, karşı-adli kanıt toplama, mobil cihazlar.

CYS507 Computer Forensics

Computer forensics and fraud ınvestigations, working with the digital forensic examiner tools, computer forensic examination process, principles of computer forensics, digital documents, correspondence and communication, evidence seizure and security, analyzing data, network forensics, anti-forensics, mobile devices.

SIB508 Siber Saldırı Teknikleri

Siber saldırı tekniklerine giriş: Kavramlar ve tanımlar, Siber saldırı türleri, izinsiz giriş aşamaları, Hedef ve kırılganlık analizleri hakkında bilgi edinmek: Zekâ teknikleri. Açık kaynaklar, Ağ ve port taraması, Tanımlama ve güvenlik açığı analizi, Keşif: Yazılım ve doğrulama sistemlerini kullanma, Kaynak tüketimi / tükenme ve Hizmet Reddi, Sosyal Mühendislik, kötü amaçlı yazılım ve kaçırma teknikleri, Kalıcılık: Delil gizleme, Ayrıcalıklı ölçeklendirme, Alternatif erişim kanalları hazırlama, Varlık gizleme.

CYS508 Cyber Attack Techniques

Introduction to cyber attacks techniques: Concepts and definitions, Types of cyber attacks, Phases of a intrusion, Acquiring information on the target and vulnerability analysis: Techniques of intelligence. Open sources, Network and port scanning, Identification and vulnerability analysis, Explotation: Exploiting software and authentication systems, Resource consumption/exhaustion and Denial of Service, Social Engineering, malware and evasion techniques, Persistence: Evidence hiding, Privilege scaling, Preparing alternative access channels, Presence hiding.

SIB509 Gelişmiş Şifreleme ve Veri Güvenliği

Homomorfik şifreleme, kimlik tabanlı şifreleme, yüklem tabanlı şifreleme, şifreli veri üzerinde anahtar kelime arama, şifreli veri üzerinden aralık sorgulama, rasyonel gizli paylaşma, diferansiyel gizlilik ve şifreleme.

CYS509 Advanced Cryptography and Data Security

Homomorphic encryption, identity-based encryption, predicate based encryption, keyword search over encrypted data, range queries over encrypted data, rational secret sharing, differential privacy and cryptography.

SIB510 Kablosuz ve Mobil Güvenlik

Mobil kullanıcılar için kablosuz erişim ağlarında kimlik doğrulama, anahtar dağıtım, bütünlük, gizlilik ve anonimlik için fonksiyonlar, protokoller ve yapılandırmalar. Ders, WPAN, WLAN, UMTS, IMS gibi mevcut sistemlerde kullanılan güvenlik tekniklerini sunar. Çeşitli ad-hoc ağları gibi yeni ağ teknolojisi için önerilen çözümler. Kablosuz sistemlerde sayısal adli kanıt toplama.

CYS510 Wireless and Mobile Security

Functions, protocols and configurations for realizing authentication, key distribution, integrity, confidentiality and anonymity in wireless access networks for mobile users. The course presents security techniques employed in existing systems, such as WPAN, WLAN, UMTS, IMS. Proposed solutions for new network technology, such as various types of ad-hoc networks. Digital forensics in wireless systems.

SIB511 Siber Güvenliğin Yasal Boyutları

Siber güvenlik kavramı, ulusal güvenlik açısından kritik öneme sahiptir ve bu nedenle hem iç hem de dış hukukta etkileri vardır. Siber suç siber güvenlik için bir tehdit oluşturuyor ve hem iç hem de karşılaştırmalı yasalarla cezalandırılıyor. Buna göre, dersin başlangıç noktası, 5237 sayılı Türk Ceza Kanunu kapsamında siber suçların ne olduğunu kapsamaktır. İkincisi, 5846 Sayılı Fikri Mülkiyet Yasası ve 5070 sayılı Elektronik İmza Yasası gibi çeşitli yasalar uyarınca tanımlanan suç faaliyetlerine bakacağız. Türkiye iç hukuku çerçevesinde ele alacak ve yasal internet erişim kısıtlamasına yol açan başvuru sürecine odaklanacağız. İlgili mevzuat ışığında soruşturma ve kovuşturma prosedürlerini gözden geçireceğiz. Son olarak, 5271 sayılı Türk Ceza Muhakemesi Kanunu'nun hükümleri uyarınca, mahkeme hukukunda ceza unsurlarının varlığını kanıtlamak için kullanılmasına yol açan olay yerinden dijital delillerin elde edilmesi ile başlayan yasal sürece bakacağız. Bu ders, siber güvenlik alanında çalışması beklenen öğrencilere adli kararları ve çeşitli vaka çalışmalarını kapsayan gerekli yasal altyapıyı kazandırmayı amaçlamaktadır.

CYS511 The Legal Dimensions of Cyber Security

The concept of cybersecurity is critical in terms of national security, and as such has implications in both domestic and international law. Cybercrime poses a threat to cybersecurity, and has been made punishable by domestic and comparative law alike.

Accordingly, the starting point of the course shall be to cover what constitutes cybercrime under the Turkish Criminal Code No. 5237. Secondly, we shall look at criminal activities defined under various laws, such as the Intellectual Property Act No.5846 and the Electronic Signature Act No. 5070. We shall elaborate on the legal aspect of cybercrime mitigation within the context of Turkish domestic law, and shall focus on the application process leading to legal internet access restriction. We shall go over the procedures of investigation and prosecution in light of related legislation. Finally, we will look at the legal process starting with the acquisition of digital evidence from the crime scene leading up to it being used to prove the existence of criminal elements at a court law, under the provisions of the Turkish Criminal Procedure Act No. 5271. The course aims to provide students who are expected to work in the field of cybersecurity with the necessary legal background by covering judicial decisions and various case studies.

SIB512 Biyometrik Sistemler ve Kimlik Doğrulama

Kişinin tanınması ve biyometriye giriş tarihi, Biyometrik sistemler, Biyometrik işlevler, Biyometrik performans ölçüleri, Parmak izi tanımaya giriş, Parmak izi için özellik çıkarımı, Parmak izi eşleştirme, Yüz tanımaya giriş, Yüz imgesinin eldesi ve ön işleme, Yüz algılama, Yüze ait öznitelik çıkarımı, Yüz Eşleştirme, Yüzdeki varyasyonlarla başetme, Yüz modelleme.

CYS512 Biometric Systems and Authentication

History of person recognition and introduction of biometrics, Biometric systems, Biometric functionalities, Biometric performance measures, Introduction to fingerprint recognition, Feature extraction for fingerprint, Fingerprint matching, Introduction to face recognition, Facial image acquisition and preprocessing, Face detection, Facial feature extraction, Face matching, Handling facial variations, Face modeling.

SIB513 Kripto Para Teknolojileri

Kriptografiye giriş: dijital imzalar, kriptografik karma fonksiyonlar, kriptografik veri yapıları: karma işaretçiler, blok zincirler, merkle ağaçları, bitcoin protokolü: kimlik olarak anahtarlar, basit kripto-para birimleri, dağıtılmış mutabakatla dağıtma, teşvikler, mühendislik detayları: bitcoin blokları, sıcak ve soğuk depolama, anahtarları bölme ve paylaşma, rezerv kanıtı, yükümlülük ispat belgesi, anonimlik, sahte kimlik, bağlantısızlık, istatistiksel saldırılar (işlem grafiği analizi), ağ katmanı anonimleştirme, Chaum kör imzaları, tek karışım ve karışım zincirler, merkezi olmayan karışım, sıfır bilgi korumalı kripto para birimleri, kripto para birimi teknolojileri: akıllı mülkiyet, verimli mikro ödemeler, eşleştirme işlemleri ve ödeme, genel rastgele kaynak, tahmini piyasalar, emanet işlemleri, yeşil adresler, açık artırma ve piyasalar, çok partili piyangolar.

CYS513 Cryptocurrency Technologies

Introduction to cryptography: digital signatures, cryptographic hash functions, cryptographic data structures: hash pointers, append-only ledgers (block chains), Merkle trees, bitcoin’s protocol: keys as ıdentities, simple cryptocurrencies, decentralization through distributed

consensus, incentives, engineering details: bitcoin blocks, hot and cold storage, splitting and sharing keys, proof of reserve, proof of liabilities, anonymity, pseudonymity, unlinkability, statistical attacks (transaction graph analysis), network-layer de-anonymization, Chaum's blind signatures, single mix and mix chains, decentralized mixing, zero-knowledge proof cryptocurrencies, cryptocurrency technologies: smart property, efficient micro-payments, coupling transactions and payment, public randomness source, prediction markets, escrow transactions, green addresses, auctions and markets, multi-party lotteries.

SIB514 Büyük Veri Güvenliği ve Gizliliği

Dağıtılmış programlama çerçevelerinde güvenli hesaplamalar, ilişkisel olmayan veri depoları için en iyi güvenlik uygulamaları, güvenli veri depolama ve işlem kayıtları, son nokta giriş onayı / filtreleme, gerçek zamanlı güvenlik / uyumluluk izleme, ölçeklendirilebilir ve bileşilebilir gizlilik, analitik koruma, büyük veri için şifreleme teknolojileri, granüler erişim kontrolü, granül denetimler, veri kaynağı.

CYS514 Big Data Security and Privacy

Secure Computations in Distributed Programming Frameworks, Security Best Practices for NonRelational Data Stores, Secure Data Storage and Transactions Logs, Endpoint Input Validation/Filtering, Real-Time Security/Compliance Monitoring, Scalable and Composable Privacy Preserving Analytics, Cryptographic Technologies for Big Data, Granular Access Control, Granular Audits, Data Provenance

SIB515 Saldırı Tespit ve Koruma

IDS / IPS tanımı ve sınıflandırması. Saldırı temel unsurları ve bunların tespiti. Suistimaltespit sistemleri (IDS'de arama algoritmaları ve uygulamaları). Anomali tespit sistemleri (makine öğrenmesi temelleri: ilkeler, önlemler, performans değerlendirmesi, yöntem kombinasyonları, yapay sinir ağlarının temelleri), IDS'de kümeleme (hiyerarşik ve bölümlendirme) ve denetimli öğrenme). IDS test etme ve performanslarının ölçülmesi. Hesaplamalı karmaşıklık-kuramsal ve bilgi-kuramsal IDS modelleri ve kalite ölçütleri. Sanal ağlarda izinsiz giriş tespiti.

CYS515 Intrusion Detection and Protection

IDS/IPS definition and classification. Basic elements of attacks and their detection. Misuse detection systems (search algorithms and applications in IDS). Anomaly detection systems (machine learning basics: principles, measures, performance evaluation, method combinations, basics of artificial neural networks, clustering (hierarchical and partitional) and supervised learning in IDS). Testing IDS and measuring their performances. Computational complexity-theoretic and information-theoretic IDS models and quality criteria. Intrusion detection in virtual networks.

SIB516 Kötü Amaçlı Yazılım Analizi ve Tespiti

Öğrenciler, disassembler, ikili hata ayıklayıcı analizi, hata ayıklayıcıları, statik ve dinamik analiz ve diğer araçları kullanarak bilgisayar virüsleri, Truva atları ve rootkitler de dahil olmak üzere kötü amaçlı yazılımları analiz etmeyi öğrenirler.

CYS516 Malware Analysis and Detection

Learn how to analyze malware, including computer viruses, trojans and rootkits using disassemblers, debuggers, static and dynamic analysis, using disassemblers, binary analysis debuggers and other tools.

SIB517 Penetrasyon Testi ve Güvenlik Açığı Analizi

Penetrasyon testine giriş. Penetrasyon testi planlaması; Sözleşme belgelerinin kapsamı ve kurallarının belirlenmesi. Penetrasyon testi araçları: sanal kurulum ve araç takımı kurma. Keşif evresi: açık kaynak istihbarat, bilgi toplama, korelasyon, doğrulama ve önceliklendirme. Tarama aşaması: numaralandırma, bağlantı noktası taraması ve güvenlik açığı analizi. İstismar aşaması: manuel istismar, şifre kırma ve Metasploit çerçevesi. İstismar sonrası aşama: Veri toplama, ağ analizi, erişimi sağlama, dönme. Raporlama aşaması: penetrasyon testi rapor yapısı ve bileşenleri. Güvenlik kontrollerini atlama ve algılanmaktan kaçınma.

CYS517 Penetration Testing and Vulnerability Analysis

Introduction to penetration testing. Penetration testing planning; determining scope and rules of engagement documentation. Penetration testing tools: setting up virtual up and toolset. Reconnaissance phase: open source intelligence, information gathering, correlation, verification, and priorization. Scanning phase: enumeration, port scanning, and vulnerability analysis. Exploitation phase: manual exploitation, password cracking and Metasploit framework. Post-exploitation phase: Data gathering, network analysis, maintaining access, pivoting. Reporting phase: penetration test report structure and components. Bypassing security controls and avoiding detection.

SIB518 Bulut Bilişimde Siber Güvenlik

Bulut bilişime giriş, Sanallaştırma, Çoklu- kullanım, Ölçeklenebilirlik, İsteğe bağlı erişim, Esneklik, Bulut yığını, Hizmet modelleri, Dağıtım modelleri, Hizmet Olarak Yazılım, Hizmet Olarak Platform, Hizmet olarak Altyapı, Hizmet Olarak Güvenlik, Bulut güvenlik sorunları, Şifreleme, Veri güvenliği, Kimlik ve erişim yönetimi.

CYS518 Cybersecurity in Cloud Computing

Introduction to cloud computing, Virtualization, Multi-tenancy, Scalability, On-demand access, Elasticity, Cloud stack, Service models, Deployment models, Software-as-a-Service, Platform-as-a-service, Infrastructure-as-a-service, Security-as-a-Service, Cloud security challenges, Encryption, Data security, Identity and Access Management.

SIB519 Güvenli Gömülü Sistemler

Bu ders gömülü güvenliğin temellerini gerçek hayat uygulamaları ile birlikte öğretir. Dersin ilk yarısında, öğrenciler gömülü cihazlara, öğrencilerin geçmişine bağlı olarak bir mikrodenetleyici veya bir FPGA kullanarak kriptografiyi nasıl etkili bir şekilde uygulayacaklarını öğrenirler. Dersin ilk yarısı laboratuvarda güvenlik modülü uygulamalarını içerir. Dersin ikinci yarısında, gömülü sistemlere tehdit ve saldırma (örneğin, yan kanal analizi) teknikleri sunulmaktadır. İlk yarıdaki uygulamalar tanıtılan yöntemlerle pratik olarak saldırıya uğratılır. Dersin sonunda, ikinci yarıda başlatılan saldırı türlerine karşı alınacak önlemler kısaca tartışılacak ve gösterilecektir. Ders süresince öğrenciler osiloskopları ve güvenlik analizleri için kullanılan diğer araçları kullanmayı öğreneceklerdir.

CYS519 Secure Embedded Systems

This course teaches the fundamentals of embedded security with real-life implementations. In the first half of the course, students learn how to efficiently implement cryptography on embedded devices, using a microcontroller or an FPGA depending on the students' background. This first half includes security module implementations, which is solved during the lab time. In the second half of the course, threats against and techniques to attack embedded systems (e.g., side-channel analysis) are presented. The implementations from the first half part one are practically attacked with the introduced methods. At the end of the course, countermeasures against the types of attacks introduced in the second half will be briefly discussed and demonstrated. During the course, students will learn to use oscilloscopes and other tools used for security analyses.

SIB520 Siber Güvenlikte Özel Konular

Siber Güvenlik Standartları ve Uyumluluğu, Uygulamalı Ağ Güvenliği, Uygulama Güvenliği İlkeleri / Uygulamaları, Siber Operasyonel Planlama, Yazılım Güvenliği, Siber Güvenlik Risk Yönetimi ve Uyumluluğu, Mobil Cihaz Yönetimi, Güvenli Unix Yönetimi, Tersine Mühendisliğe Giriş, İçeriden Gelen Tehditler, Sayısal Adli Kanıt Toplamaya Giriş, Çin'in Siber Gücü: Perspektifler ve Uygulamaları, SCADA ve Endüstriyel Kontrol Sistemleri için Siber Güvenlik.

CYS520 Special Topics in Cyber Security

Cybersecurity Standards & Compliance, Applied Network Security, Application Security Principles/Practices, Cyberspace Operational Planning, Software Security, Cybersecurity Risk Management & Compliance, Mobile Device Management, Secure Unix Administration, Intro to Reverse Engineering, Insider Threats, Introduction to Digital Forensics, Chinese Cyber Power: Perspectives and Implications, Cybersecurity for SCADA and Industrial Control Systems

SIB521 Endüstri 4.0 İçin Siber Güvenlik: Tasarım ve İmalat Analizi

Bu ders siber güvenliği ve Endüstri 4.0 vizyonunun gerçekleştirilmesindeki etkisini tanıtmaktadır. Endüstri 4.0 kapsamı dahilindeki siber güvenliğin teknolojik temellerini kapsar ve Endüstri 4.0'ın karşılaştığı siber güvenlik tehditlerinin yanı sıra, hem akademik araştırma hem de pratik uygulamalar ile ilgili en son teknolojiye sahip çözümleri detaylandırır. Endüstri

4.0 ve Endüstriyel Nesnelerin İnterneti ve bulut tabanlı tasarım ve üretim sistemleri gibi ilgili teknolojiler yıkıcı yenilikleriyle birlikte incelenir.

CYS521 Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing

This course introduces cybersecurity and its impact on the realization of the Industry 4.0 vision. It covers the technological foundations of cybersecurity within the scope of the Industry 4.0 landscape and details the existing cybersecurity threats faced by Industry 4.0, as well as state-of-the-art solutions with regard to both academic research and practical implementations. Industry 4.0 and its associated technologies, such as the Industrial Internet of Things and cloud-based design and manufacturing systems are examined, along with their disruptive innovations.

SIB522 Nesnelerin İnternetinde Adli Bilişim ve Güvenlik

Nesnelerin İnterneti (IoT), her türlü hizmeti sunarken yaygın, bağlantılı ve akıllı düğümlerin özerk biçimde etkileşime girmesini öngörmektedir. Geniş dağıtım, açıklık ve IoT nesnelerinin nispeten yüksek işlem gücü, onları siber saldırılar için ideal bir hedef haline getirdi. Ayrıca, birçok IoT düğümü özel bilgileri toplayıp işlerken, kötü niyetli aktörler için adeta altın madeni haline geliyor. Bu nedenle, güvenlik ve özellikle tehlike altındaki düğümleri algılama yeteneği, bir saldırı veya kötü niyetli faaliyetlerin kanıtlarının toplanması ve korunması ile birlikte, IoT ağlarının başarılı bir şekilde dağıtılmasında öncelik olarak ortaya çıkmaktadır.

CYS522 IoT Forensics and Security

The Internet of Things (IoT) envisions pervasive, connected, and smart nodes interacting autonomously while offering all sorts of services. Wide distribution, openness and relatively high processing power of IoT objects made them an ideal target for cyber attacks. Moreover, as many of IoT nodes are collecting and processing private information, they are becoming a goldmine of data for malicious actors. Therefore, security and specifically the ability to detect compromised nodes, together with collecting and preserving evidences of an attack or malicious activities emerge as a priority in successful deployment of IoT networks.

SIB523 Siber Güvenlik için Linux Temelleri

Öncelikle, öğrenciler en iyi güvenliği sağlamak için Linux'u nasıl kuracaklarını öğreneceklerdir. Daha sonra, öğrenciler hesapları, cihazları, hizmetleri, işlemleri, verileri ve ağları güvenli bir şekilde yönetmek için en iyi uygulamalarda uzmanlaşacaklar. Daha sonra öğrenciler ayak izi, penetrasyon testi, tehdit tespiti, günlüğe kaydetme, denetim, yazılım yönetimi ve daha fazlası için güçlü araçlar ve otomatik komut dosyası teknikleri konusunda uzmanlaşacaklar.

CYS523 Linux Essentials for Cybersecurity

First, students will learn how to install Linux to achieve optimal security upfront. Next, students will master best practices for securely administering accounts, devices, services, processes, data, and networks. Then, students will master powerful tools and automated

scripting techniques for footprinting, penetration testing, threat detection, logging, auditing, software management, and more.

SIB524 Siber Güvenlikte Yapay Zeka

Öğrenciler siber güvenlik ve yapay zeka temelleri hakkında temel bilgi alacaklardır. Ders konuları: makine öğrenimi ve uyarlanabilir zeka, ölçeklenebilir makine öğrenmesi, metin işleme, doğal dil işleme, temel güvenlik özellikleri ve mekanizmaları, güvenli yazılım geliştirme, siber tehdit avcılığı ve adli bilişim, kontrol ve gömülü sistemlerin güvenliği.

CYS524 AI in Cybersecurity

Students will receive a grounding in the fundamentals of cybersecurity and AI. Course topics are: machine learning and adaptive ıntelligence, scalable machine learning, text processing, natural language processing, fundamental security properties and mechanisms, development of secure software, cyber threat hunting and digital forensics, security of control and embedded systems.

SIB525 Veri Sıkıştırma

Kayıpsız veri sıkıştırmanın kuramsal temelleri. Huffman kodlama, aritmetik kodlama, sözlük yöntemleri. Kayıplı veri sıkıştırmanın kuramsal temelleri. Skaler nicemleme, vektör nicemleme, öngörüsel kodlama, dönüşüm kodlama. Video kodlamaya giriş.

EEE514 Data Compression

Information theoretic fundamentals of lossless data compression. Huffman coding, arithmetic coding, dictionary methods. Information theoretic fundamentals of lossy data compression. Scalar quantization, vector quantization, predictive coding, transform coding. Introduction to video coding.

SIB526 Sayısal İmgelerden Adli Kanıt Toplama

Sayısal imgenin oluşumu ve insan görme sistemi. Veri saklama, damgalama ve gizliyazı analiz yöntemleri. Kaynak tanılama. Sayısal imgelerin tamlığı ve tahrifat sezimi.

EEE515 Digital Image Forensics

Digital image formation and human visual system. Steganography, watermarking and steganalysis techniques. Source identification, integrity and manipulation detection of digital images.

SIB595 Yüksek Lisans Tezi

CYS595 Master's Thesis

SIB594 Yüksek Lisans Dönem Projesi

CYS594 Master's Term Project