Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı

Ders İçerikleri

(Tüm dersler 3 krediliktir = 5 AKTS kredisi)

ZORUNLU DERSLER

MUH 500 Araştırma Yöntemleri (5 AKTS)

Çeşitli araştırma alanlarındaki sorunları anlamak ve çözümler üretmek üzere yapılacak araştırmalar için gerekli temel bilgilerin paylaşılmasıdır.

BGM 590 Proje Dersi (20 AKTS) (Tezsiz Yüksek Lisans Programı İçin)
Tezsiz YL öğrencisi tez danışmanının onayı ile bir proje konusu seçer ve proje önerisi hazırlar. Bu amaçla kaynak araştırması yapar, ilgili alanlardaki çalışmaları inceler, gerekli durumlarda deney / gözlem / benzetim / anket çalışmaları yapar. Dönem sonunda bir proje raporu hazırlayarak dersin öğretim üyesine sunar. Ayrıca proje dersi alanlara ve fakülteye açık bir sunum yapar. Bu derse Başarılı (S) veya Başarısız (F) harf notlarından birisi verilir.

BGM 591 Seminer Dersi (20 AKTS)

BGM 599 Yüksek Lisans Tezi (60 AKTS)

BGM 501 Kriptolojiye Giriş

Ders kapsamında kriptolojinin temel konuları yani gizlilik, veri bütünlüğü, mahremiyet, inkar edememe, erişebilirlik, bütünlük, kimlik asıllama gibi bilgi güvenliği problemlerine kriptografik açıdan getirilen çözümler anlatılacaktır. Ayrıca bu çözümlerin analizleri tartışılacaktır.

İçerik: Temel şifreleme tekniklerinin tarihi, Vernam şifreleme, Vigeneere şifreleme, modern blok şifreleme algoritmaları ve yapılarının incelenmesi, dizi şifreleme algoritmaları ve kullanılan matematiksel teknikler, DES ve güvenlik analizleri, AES ve güvenlik analizleri. Açık anahtarlı şifrelemenin teknikleri, Diffie Helman anahtar paylaşım protokolü, Discrete Logaritma Problemi, RSA, Çarpanlara ayırma problemi, sayısal imza, açık anahtar altyapısı, sertifika yönetimi. Bütünlük gereksimi ve çözüm yolları, özet fonksiyonlarının temel kullanım yerleri ve güvenlik ölçütleri, temel özet fonksiyonu örnekleri ve analizleri, MAK (Metin Asıllama Kodları) inşaları ve analizleri. Temel kriptografik protokol örnekleri ve analizleri, kimlik asıllama protokolleri,

Ön Şart: Yok

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Introduction to Cryptography-Principles and Applications by Hans Delfs and Helmut Knebl.

BGM 502 Siber Güvenliğe Giriş

Bilgi güvenliğinin temel kavramları, bilgisayar güvenliği ve bilgisayar ağlarında kullanılan protokol, cihaz ve teknolojilerin güvenliği ele alınacaktır.

İçerik: Bilgisayar uygulamaları ve işletim sistemi güvenliği, OSI (Open System Interconnection) referans modeli, bilgisayar ağ atakları, bilgisayar ağları risk değerlendirmesi, kimlik doğrulama, yetkilendirme ve kayıt mekanizmalar, yerel alan ağı güvenliği, sınır güvenliği cihazları, geniş alan ağı teknolojileri ve güvenliği, kablosuz iletişim güvenliği, veri mahremiyeti, bulut bilişim güvenliği.

Ön Şart: Bilgisayar Ağları (Computer Networks), İşletim Sistemleri (Operating Systems) arkaplanı.

Kaynak Kitap:

- Network Security Bible, Second Edition, Eric Cole, Wiley, 2009, ISBN: ISBN-13: 978-0470502495
- Seçilmiş kaynak okuma parçaları, makaleler ve sunumlar

SEÇMELİ DERSLER

BGM 505 Güvenli İmplementasyon ve Yan Kanal Analizi

Bu derste kriptografik fonksiyonların güvenli bir şekilde nasıl donanımsal olarak gerçeklenebileceği ve kripto anahtarları gibi korunacak varlıkların donanımda saklama yöntemleri işlenecektir.

İçerik: Bazı temel kripto algoritmalarının donanımsal gerçeklenmesi örnekleri: RSA, eliptik eğri, DES, AES implementasyonları, hafızada gizli bilgi okuma yöntemleri, gerçek rastgele sayı üreteçleri ve gürültü kaynakları. Yan kanal analizleri: Pasif yöntemlerden zaman analizi, basit güç/elektromanyetik analizi (Simple power/electromagnetic analysis - SPA/SEMA), farksal güç/elektromanyetik analizi (Differential

power/electromagnetic analysis - DPA/DEMA), korelasyon güç analizi (Correlation power analysis CPA), farksal kümeleme analizi (Differential Cluster analysis); aktif yöntemlerden hata yaptırma analizi (Differential fault analysis - DFA), gözetleme analizi (Probing analysis), hata hassaslık analizi (Fault sensitivity analysis) vb. yöntemler ve karşı önlemler.

Ön Şart: Sayısal Elektronik Devreler arkaplanı

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Power Analysis Attacks : Revealing the Secrets of Smart Cards by Stefan Mangard, Elisabeth Oswald and Thomas Popp, Springer, 2007.

BGM 532 Zararlı Yazılım Analizi

Ders kapsamında zararlı yazılımları incelemek için gerekli temel işletim sistemi bilgileri, zararlı yazılım analiz altyapısının kurulması.

İçerik: Zararlı yazılımları incelemek için gerekli temel işletim sistemi bilgileri, zararlı yazılım analiz altyapısının kurulması, dinamik ve statik zararlı yazılım analiz yöntemleri, debugging ve tersine mühendislik teknikleri, zararlı yazılım inceleme için gerekli temel X86 assembly ve Windows API bilgisi, anti analiz tekniklerinin devre dışı bırakılması, hafıza dökümü inceleme.

Ön Şart: Yok

Kaynak Kitap:

- Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code by Michael Ligh, Steven Adair, Blake Hartstein, Matthew Richard, 2010.
- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software by Michael Sikorski, Andrew Honig, 2012.

BGM 533 Bilgisayar Adli Analizi

Bu derste hafıza dökümlerinden ulaşılabilecek bilgiler, belli bir tarih aralığında sistemde neler yapıldığının tespiti ile sistemdeki değişikliklerin zaman analizi konuları işlenecektir.

İçerik: Dosya sistemleri, windows ve linux işletim sistemi incelemeleri, bilgisayar adli analizi çalışmasında kullanılan araçlar, internet tarayıcıları geçmişi ve e-posta incelemeleri, hafıza dökümleri.

Ön Şart: Yok

Kaynak Kitap:

- Filesystem Forensics, Brian Carrier, Pearson Education, 2005, ISBN: 0-32-126817-2
- Guide to Computer Forensics and Investigations, 3. Edition, Bill Nelson, Amelia Philips, Christopher Steuart, Course Technology, 2010, ISBN: 978-1-435-49883-9

BGM 534 Ağ Trafik Analizi

Ders kapsamında ağ ortamında dijital adli analiz prensipleri geniş kapsamlı anlatılacaktır. Ağ altyapıları, ağ topolojileri ve protokoller tanıtılacak, ağ güvenliği ile ağ adli analizi ilkelerinin önemi tartışılacak, ağ trafiği üzerinden delillerin nasıl toplanacağı hakkında bilgiler verilecektir. Ağ uygulamalarının saklamış olduğu kayıt dosyalarından delillerin nasıl elde edileceği ile ilgili bilgiler verilecektir.

İçerik: Ağ altyapıları, ağ topolojileri ve protokoller, delillerin toplanması ve değerlendirilmesi sırasında uyulması gereken yasal zorunluluklar, zararlı ağ trafiği davranışlarının tespitine yönelik çalışmalar, kablolu ve kablosuz ortamlarda ağ trafiği analizi.

Ön Şart: Ağ güvenliği temelleri

Kaynak Kitap

- Network Forensics: Tracking Hackers through Cyberspace**,** S. Davidoff, J. Ham, Prentice Hall - 2012
- The Tao of Network Security Monitoring: Beyond Intrusion Detection, Richard Bejtlich, Addison-Wesley Professional – 2004
- Practical Intrusion Analysis: Prevention and Detection for the Twenty-First Century**,** Ryan Trost
  Addison-Wesley Professional – 2009

BGM 537 Mobil Güvenlik

Dersin amacı mobil platform temelleri ve güvenlik özellikleri bilgisini vererek ilgili sistemlere yönelik sızma testi ve zararlı yazılım analizi gerçekleştirme adımlarının öğrenilmesini sağlamaktır.

İşlenecek konular: Android, iOS, Blackberry ve Windows Phone platform temelleri, güvenlik özellikleri, Android uygulama sızma testi, iOS uygulama sızma testi, mobil zararlı yazılım inceleme ve kablosuz ağ güvenliği…

Ön Şart: Temel ağ ve bilişim sistemleri bilgisi

Kaynak Kitap: The Mobile Application Hacker's Handbook, ISBN-13: 978-1118958506, ISBN-10: 1118958500 First Edition.

BGM 539 E-İmza Uygulamaları

Kripto kapsamında, temel güvenlik özellikleri, simetrik kripto, asimetrik kripto, CMS zarf yapısı, şifreleme ve e-imza; Açık anahtar altyapısı kapsamında, Sertifika Makamı, Sertifikalar, Sertifika iptal listesi, çevirim için sertifika durum sorgulama protokolü, zaman damgası, sertifika doğrulamaları; imza çeşitleri kapsamında, ülkemizdeki imza profilleri ve diğer yoğun kullanılan imza profilleri; E-imza bileşenleri kapsamında, akıllı kart, akıllı kart işletim sistemleri, elektronik imza atma araçları; Elektronik sertifika hizmet sağlayıcılarının görevleri ve işleyişleri; 5070 sayılı elektronik imza mevzuatı; Elektronik imza standartları kapsamında, ETSI, ISO, RFC, FIPS standartları; İleri düzey elektronik imza teknolojileri; Elektronik imza ile Türkiye Cumhuriyeti Kimlik Kartı, Kayıtlı Elektronik Posta ve diğer kamu hizmetlerinin ilişkisi ve kullanımı anlatılacaktır.

Ön Şart: yok

Kaynak Kitap: www.kamusm.gov.tr

BGM 540 Kriptografik Protokoller

Bu derste genel olarak kripto protokolleri ve e-devlet uygulamaları anlatılacaktır.

İçerik: Çoklu Sır Paylaşımı ve uygulamaları, Homomorfik Şifreleme, Taahhüt Şemaları, Sıfır Bilgi Protokolleri, Güvenli Çoklu hesaplamalar (Temelde mahremiyetin korunarak istenilen uygulamaların güvenli yapılması), gizlilik, mahremiyet, e-devlet uygulamaları (Güvenli arama yapma, e-seçim, e-müzayede, e-noter vb.), endüstride protokol örnekleri ve analizleri: WEP ve WPA protokolleri, SSL ve TLS protokolleri, IPSec protokolü. Neodem Schroeder protokolü ve analizleri, IPSec protokolü ve analizleri, SSL/TLS protokolleri ve analizleri, WEP/WPA protokolleri ve analizler. Anahtar yönetiminin temel kavramları, anahtar üretimi.

Ön Şart: **Kriptolojiye giriş**

Kaynak Kitap**:**

- Introduction to Modern Cryptography, by Jonathan Katz and Yehuda Lindell, Chapman and Hall/CRC Press, August 2007.
- Oded Goldreich: The Foundations of Cryptography - Volume 2, Basic Applications. Cambridge University Press 2004.

BGM 541 Açık Anahtarlı Kripto Sistemleri

Bu derste açık anahtarlı kripto algoritmalarından ve bu algoritmalara yapılan ataklardan bahsedilecektir.

İçerik: RSA, PKCS #1 standardı, Diffie-Hellman, ElGamal Şifreleme sistemleri, DSA, Sayısal İmzalama, Bütünlük, Schnorr imzalama, DSS (Sayısal İmza Standardı), Pratikte Asimetrik şifreleme kullanımı: anahtar uzunlukları, eliptik eğri kriptosu, NTRU ve latis tabanlı şifreleme ve güvenlik analizleri, hata düzeltme kodlaması ve McElliece şifrelemesi ve güvenlik analizleri.

Ön Şart: Yok

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Introduction to Cryptography-Principles and Applications by Hans Delfs and Helmut Knebl.
- Oded Goldreich: The Foundations of Cryptography - Volume 1, Basic Techniques. Cambridge University Press

BGM 542 Özet fonksiyonları ve Mesaj Asıllama Kodları

Ders kapsamında kriptografik özet fonksiyonları, MAKlar ve bunlara yapılan ataklardan bahsedilecektir.

İçerik: Özet fonksiyonları ve kullanım yerleri. Güvenlik kriterleri, çakışma atakları, ters görüntü atakları, ikinci ters görüntü atakları. Tasarım felsefesi, sıkıştırma fonksiyonları. Merkle-Damgard inşası ve güvenlik analizleri: Çoklu çakışma atakları, uzun mesaj ikinci ters görüntü atağı, Nostradamus atağı. MD5 ve SHA-1 ve güvenlik durumları, MD-5 ve SHA-1'e yapılan çakışma atakları, Wang atakları. Mesaj Asıllama Kodları (MAK) ve analizleri. Uzatma atağı, Sahte Mesaj Asıllama Kodu atağı. HMAC ve güvenlik durumu, OMAC ve güvenlik durumu, CBCMAC ve XCBMAC ve güvenlik durumları. Özet fonksiyonların ve MAK'ların protokollerdeki kullanımları.

Ön Şart: Yok

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Cryptography Theory and Practice, Douglas R. Stinson, CRC Press 2nd edition.
- Practical Cryptography, N.Ferguson, B. Schneier, John Wilwy and Sons.

BGM 543 Kriptoloji için Sayılar Teorisi

Matematiksel kriptolojinin ve açık anahtar kriptoloji için kullanılan algoritmaların güvenliğinin temellerini oluşturan cebir, sayılar teorisi, cebirsel eğriler ve bilgisayar cebiri kavramları. Asal sayı üretimi, indirgenemez polinomlar, çarpanlara ayırma problemi ve ayrık logaritma problemleri. Bu problemlerin çözümü için geliştirilen algoritmaların verimlilik ve hesaplamalarının karmaşıklığı açısından tartışılması. Eliptik eğri kriptografisi hakkında temel bilgiler.

İçerik: Sonlu gruplar, devirsel gruplar ve özellikleri, tam sayılarda temel algoritmalar, hesaplama karmaşıklığı ve sonlu gruplarda verimlilik, halkalar, sonlu ve öklid halkaları ve özellikleri, polinom halkaları, Çin kalanları teoremi. Cisimler, sonlu cisimler genişlemeleri ve varlık teoremleri. Asal sayı üretimi için eleme, Sollovay-Strassen, Miller-Rabin, N-1 ve N+1 testleri. RSA ve güvenliği, çarpanlarına ayırma problemi, polinomlarda çarpanlarına ayırma, kuadratik cisim genişlemeleri ve diofantin denklemler. Grup tabanlı kriptoloji, ayrık logaritma problemi ve algoritmalar. Eliptik Eğriler ve eğri tabanlı kriptolojiye giriş, sonlu cisimler üzerinde eliptik eğriler, Hasse teoremi. Eşleme tabanlı kriptoloji temel kavramları.

Ön Şart: BGM 501 veya öğretim üyesinin onayı.

BGM 544 Kuantum Hesaplama ve Bilgi Teorisine Giriş

Bu derste kuantum bilgi teorisi ve kuantum karmaşıklığı anlatılacaktır.

İçerik: Klasik Bilgi Teorisi Özeti, Kuantum bilgi teorisinin temelleri ve uygulamaları, Kuantum bilgisinin gürültülü kanallarda transferi, kuantum dolaşıklılık, kuantum kriptoloji, klasik komplekslik teorisi, kuantum komplekslik, kuantum algoritmaları, kuantum hata düzeltme kodları ve fiziksel uygulamaları.

Ön Şart: Yok

Kaynak Kitap:

- Quantum Computation and Quantum Information, M. A. Nielsen, I. L. Chuang, Cambridge University press, 2010.

BGM 545 Biyometrik Sistemler ve Kimlik Doğrulama

Bu derste çeşitli biyometrik sistemlerden ve bu sistemlerin kimlik doğrulamada nasıl kullanıldığından bahsedilecektir.

İçerik: Biyometrik sistemlerin temel özellikleri ve güvenlik yönleri, Parmakizi, yüz, iris, ses, imza tanıma ve diğerleri, Çoklu biyometriklerin tasarımı, gerçeklenmesi ve değerlendirilmesi, Biyometrik sistem güvenliği, Biyometrik standartlar ve veritabanları, Güncel uygulamalar, kriptolojiyle bağlantıları, biyometrik kimlik doğrulama.

Ön Şart: Yok

Kaynak Kitap:

- A.K. Jain, P. Flynn, A. Ross, "Handbook of Biometrics", Springer, 2008.
- D. Maltoni, D. Maio, A.K. Jain, and S. Prabhakar, "Handbook of Fingerprint Recognition", Second Edition, Springer, 2009
- R.O. Duda, P.E. Hart, and D.G. Stork, "Pattern Classification", Second Edition, Wiley, 2001.
- Ross, K. Nandakumar, and A.K. Jain, "Handbook of Multibiometrics", Springer Verlag, 2006.

BGM 546 Veri Sıkıştırma ve Metin Algoritmaları

Ders kapsamında veri sıkıştırma ve desen arama algoritmalarından bahsedilecektir.

İçerik: Veri sıkıştırma teknikleri, bilişim teorisi ve kodlama algoritmaları, Huffman ve aritmetik kodlama, dil modelleme, sözlük tabanlı veri sıkıştırma, metin algoritmaları, dizi eşleme, bilgi çıkarımı, dizi eşlemede temel algoritmalar, desen arama.

Ön Şart: Yok

Kaynak Kitap:

- Introduction to Algorithms, T. H. Cormen, C. E. Leiserson, R. L. Rivest and C. Stein, MIT Press and McGraw-Hill, 2001.
- Seçilmiş okuma parçaları ve sunumlar.

BGM 547 Kuantum Kriptoloji ve Uygulamaları

Bu derste kriptolojide kuantum mekaniğinin nasıl kullanıldığı ve kuantum protokollerinin güvenlik ispatları anlatılacaktır.

İçerik: Kuantum mekaniğin temel prensipleri, bit ve kübit kavramları, fiziksel karşılıkları (polarizasyon ve faz gösterimleri), Kuantum anahtar dağıtımı, Protokoller (BB84 ve E92), Güvenlik ispatları, Saldırılar ve Karşı önlemler, Var Olan Sistemlerin karşılaştırılması, Gelecek ve Kuantum Ağları.

Ön Şart: Yok

Kaynak Kitap:

- Quantum Cryptography and Secret Key Distillation by Gilles van Assche, Cambridge Univ. press, 2006.

BGM 548 Eşleme Tabanlı Kriptografi

Ders kapsamında kimlik tabanlı şifreleme, ikili-doğrusal eşlemeler (bilinear pairings) ve Tate eşlemesi anlatılacaktır.

İçerik: Diffie-Hellman 2 parti ve 3 parti anahtar anlaşma protokolü, ikili-doğrusal eşlemeler, kimlik tabanlı şifrelemeler, Weil Pairing, Tate Pairing.

Ön Şart: Yok

Kaynak Kitap:

- Elliptic Curves-Number Theory and Cryptography, Lawrence C. Washington.
- Seçilmiş Sunumlar.

BGM 549 Simetrik Şifreleme Algoritmalarının Güvenliği

Bu derste dizi ve blok şifreleme algoritmaları ve bu algoritmalara yapılan saldırılar anlatılacaktır.

İçerik: Dizi şifreleme algoritmaları, LFSR tabanlı olan algoritmalar. GSM'de kulllanılan A5 ve güvenlik durumu, Bluetooth'da kullanılan E0 ve güvenlik durumu. İlinti atakları, hızlı ilinti atakları, Berlakamp Massey algoritması. RC4 ve güvenlik durumu. Blok şifreleme algoritmaları genel teorisi, karıştırım ve yayılım, SAC özelliği, dallanma sayısı, MDS kodlar, aktif S kutuları. Bazı blok şifreleme algoritmaları ve güvenlik durumları: DES, AES, RC6, Serpent. Analiz metotları: Diferansiyel atak ve türevleri, doğrusal atak, kare atak, cebirsel atak ve küp atak.

Ön Şart: Yok

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Introduction to Cryptography-Principles and Applications by Hans Delfs and Helmut Knebl.

BGM 550 Siber-Fiziksel Sistemler ve Nesnelerin Internetinde Siber Güvenlik

Dünyada giderek önem kazanan Siber-Fiziksel Sistemler ve Nesnelerin Interneti'nde siber güvenlikle ilgili problemleri, siber savunma önlemlerini, güvenlik gereklerini, güvenlik mimarisini ve güvenli tasarım örüntülerini öğrenmektir.

BGM 551 Yazılım Güvenliği

Yazılım geliştirme ekipleri hassas bilgilerin korunmasında kritik bir role sahiplerdir. Yazılım konusundaki güvenlik problemlerini anlamak, güvenli yazılım geliştirebilmenin ilk adımıdır. Bu ders, yazılımcılara güvenliğin tüm yazılım sürecinin temel bir parçası olduğunu anlatmak ve onların güvenli yazılım geliştirme yaşam döngüsüne aşinalık sağlamaları yolunda tasarlanmıştır. Bu derste hem baştan itibaren tüm safhalarıyla güvenli yazılım geliştirmeyi, hem de mevcut yazılımlar içindeki güvenlik problemleri öğrenilecek, hem de sürekli değişen ve gelişen güvenlik tehditlerine efektif çözümler bulmak için donanım kazanılacaktır.

İçerik: BT güvenliği ve ana çatı alanlarına hakimiyet, hata ve istisna yönetimi, güvenli tasarım, OWASP top 10 güvenlik tehditleri, modelleme ve risk tahmini analizi, yazılım tehdit modellemesi, güvenli kodlama, girdi ve çıktı için geçerleme, loglama ve takip teknolojileri, güvenli test, yazılım sızma testleri, test sonuçlarının değerlendirilmesi.

Ön Şart: Yok

Kaynak Kitap:

- 1. Secure Software Development: A Security Programmer's Guide , Jason Grembi
- 24 Deadly Sins of Software Security: Programming Flaws and How to Fix Them, Michael Howard
- Writing Secure Code, Second Edition, Michael HowardPower Analysis Attacks : Revealing the Secrets of Smart Cards by Stefan Mangard, Elisabeth Oswald and Thomas Popp, Springer, 2007.

BGM 552 Blokzincir ve Dijital Paralar

İçerik: Bu dersin temel amacı bitcoin ve akıllı kontratların temelini oluşturan dağıtık ve merkezi olmayan veri tabanı teknolojisini öğretmektir. Bunun yanında, herhangi bir dijital parayı veya emtiayı (değeri) kaydetmek ve aktarmak için kullanılabilen açık, izinli ve özel blokzincirlerin temelleri anlatılacaktır. Başta Bitcoin, Ethereum olmak üzere kripto paraların özelikleri, madencilik, ve bunların varlık transferinin blokzincir üzerinde gerçekleştirilmesi anlatılacaktır. Bu ders, potansiyel olarak yıkıcı olan blokzincir teknolojisinin temelini oluşturan iş modellerini tanıtacaktır. Finansal hizmetler, kamu kurumları, bankacılık ve kontratlar üzerindeki potansiyel etkisi tartışılacaktır.

1- Blokzincir kavramını, temellerini ve iş modellerini anlayabilecek
2- Blokzincir güvenlik ve mahremiyetlerinin analiz edebilecek ve altındaki kriptografik yapıtaşlarını anlayabilecek
3- Gerçek hayattaki uygulamalarda blokzincirin rolünü kavrayabilecek
4- Kripto paralar kavramını anlayabilecek, özellikle Bitcoin ve Ethereum temellerini ve mimari yapısını kavrayabilecek
5- Cüzdan kavramını ve güvenliğini analiz edebilecek, ICO modellerini kavrayabilecek

Önşart: Yok

Kaynak Kitap:

1- Henning Diedrich, Ethereum: Blockchains, Digital Assets, Smart Contracts, Decentralized Autonomous Organizations, 2016.

2- David Gerard, Attack of the 50 Foot Blockchain : Bitcoin, Blockchain, Ethereum & Smart Contracts, 2017.

3- Charles Jensen, Blockchain : Ethereum and Security Technology Explained, 2017.

4- Andreas M. Antonopoulos, Mastering Bitcoin: Unlocking Digital Cryptocurrencies, 2014.

5-Roger Wattenhofer, The Science of the Blockchain, 2016.

BGM 531 Sızma Testleri ve Güvenlik Denetlemeleri

Kurumsal iç ağında çalışan servislere ve cihazlara yönelik güvenlik sızma testleri konularında bilgi ve yetkinlik edinilmesi hedeflenmektedir.

İçerik: Sızma testi ve güvenlik denetlemeleri ile ilgili tanımlar, standartlar ve anaçatılar, güvenlik testleri kapsamında ağ ve Linux temelleri, ağ taraması ve keşif, aktif cihaz sızma testleri, açıklıkların İstismarı, fiziksel sızma testleri, Windows ortamları ve etki alanı sızma testleri, kablosuz ağ sızma testi, hizmet dışı bırakma güvenlik testleri, endüstriyel kontrol sistemleri güvenlik testleri

Ön Şart: Temel TCP/IP, Linux ve Windows işletim sistemi bilgisi, temel ağ bilgisi

Kaynak Kitap:

- Hacking Exposed 7: Network Security Secrets & Solutions**,** Seventh Edition, Stuart McClure, Joel Scambray, ISBN 978-0-07-178028-5
- Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide, Lee Allen, 2012, Packt Publishing, ISBN 978-1-84951-774-4
- CISecurity Audit Checklists
- Seçilmiş kaynak okuma parçaları, makaleler ve sunumlar

BGM 555 Kablosuz Ağlarda Güvenlik ve Mahremiyet

Hücresel ağlar, telsiz yerel ağ ve kişisel alan ağları, mobil tasarsız ağlar, taşıt ağları, telsiz örgü ağları, duyarga ağları ve RFID sistemleri gibi telsiz ağ ve sistemlerinde güvenlik ve mahremiyet konularını kapsar. Çeşitli katmanlardaki ataklar ve önerilen yöntemler, kimlik tanıma, anahtar dağıtımı ve yönetimi, güvenli yol atama, bencil ve kötü niyetli davranışlar ile güvenli grup iletişimi konuları uygun telsiz ağ tipleri için analiz edilecektir. Dersin başında kriptografi ve telsiz ağ prensipleri ile ilgili kısa bir giriş yapılacaktır.

Ön Şart: Yok

Kaynak Kitap: Ders notları ve makaleler

Referans Kitaplar:

- Guide to Wireless Network Security, by Vacca
- Network Security: Current Status and Future Directions, by Douligeris and Serpanos
- Security for Wireless Sensor Networks, by Liu and Ning
- Security and Cooperation in Wireless Networks, by Buttyan and Hubaux

BGM 556 Siber Savunma Teknikleri ve Kontrol Mekanizmaları

Dersin amacı sistem ve ağ güvenliği denetimlerini teknik uygulamalarla açıklayarak, olası siber saldırıların kurum işleyişine etkisini minimuma çekecek kontrol mekanizmalarının teknik ve yönetimsel seviyede anlaşılmasını sağlamaktır.

Sistem ve ağ güvenliği denetim metodolojileri ve standartları, bilgi güvenliği yönetiminde denetimlerin rolü, sistem denetimleri en iyi uygulama pratiklerinin ele alınması, etkili denetleme, risk yönetimi ve raporlama yöntemleri, ağ ve sınır güvenliği denetimleri, web uygulama denetimleri, veritabanı denetimleri, Windows tabanlı İşletim Sistemleri denetimi, Unix tabanlı İşletim Sistemleri

Ön Şart: Temel ağ ve bilişim sistemleri bilgisi.

Kaynak Dersler haftalık olarak kitap bölümlerinden ve akademik makalelerden işlenecektir.
Bazı kaynaklar: ISO/IEC 27001:2013, SANS AUD 507 Courseware, NIST SP 800 serisi denetim politikaları

BGM 557 Kritik Kimlik Doğrulama Alt Yapıları ve Uygulamaları

Bu derste kimlik doğrulamanın ve tanımanın temel konularına uygulama ve kullanım bakış açısından yaklaşılmaktadır. Gerektiği yerlerde kimlik doğrulamanın teorik ve matematiksel yönden ele alınarak nasıl çalıştığı gösterilecektir. Şifre tabanlı, kart tabanlı, sertifika tabanlı, biyometrik tabanlı vb. kimlik doğrulama yöntemlerine girilecektir. Türk Kimlik Kartı ile pratik yapılarak uygulama örnekleri gösterilecektir. Mobil Kimlik doğrulama yöntemleri teorisi ile gösterilecek ve uygulaması yapılacaktır. Bulutta Kimlik Doğrulama yöntemleri işlenecek ve lab ortamında kurulu bir bulut üzerinde pratikleri gösterilecektir. Bu alanlarda biyometrik kimlik doğrulamanın nasıl uygulanabileceği ele alınarak literatürdeki çalışmalar ile zenginleştirilecektir. Ayrıca bu alanda Avrupa'da neler yapıldığına dair projelerimizden (eCODEX, Stork, eSENS, FutureID v.b.) örnekler vererek bilgilendirilecektir.

Son olarak başarılı bir kimlik doğrulamanın kurumsal ve bireysel yönleri ele alınarak ülkemizde ve Dünyada hukuk ve bilgi gizliği açısından konular işlenecektir. Ülkemiz için bunun nasıl ele alındığı ve kanun/yönetmelik ve mevzuat çalışmaları ile masaya yatırılacaktır. Örnek uygulama olarak MASAK'ın Finans Sektörü için düzenlemeleri ve değişimler ele alınarak kullanılabilir güvenlik nasıl olur tartışılacaktır.

İçerik: Kimlik Doğrulama Teorisi, Kimlik Doğrulama Alt Yapıları, Akıllı Kart ile Kimlik Doğrulama Yöntemleri, Mobil Kimlik Doğrulama Yöntemleri, Bulutta Kimlik Doğrulama Alt Yapıları, AB Ülkeler Arası Uygulamalarda Kimlik Doğrulama Alt Yapıları (Stork, eCOdex, eSENs, v.b),

Kimlik Doğrulama Biyometrik Unsurların Rolü, Kurumların Kimlik Doğrulamada İzleyici Süreçler, Mevzuatla İlgili Süreçler, Teknik Süreçler, Entegrasyon Yöntemleri

Ön Şart: Yok

Kaynak Kitap: Digital Identity Management: Perspectives on the Technological, Business and Social Implications edited by David G.W. Birch, 2007.

BGM 558 Akıllı Kart Uygulamaları

Bu derste akıllı kartların ne olduğu, nasıl kullanıldığı, kullanılan güvenlik öğeleri, algoritmaları ve akıllı kart uygulamalar ile ilgili bilgi verilecektir.

İçerik: Akıllı kartın tarihçesi, akıllı kart tipleri, fiziksel ve elektriksel özellikleri, dosya yapıları, akıllı kart işletim sistemi, ve çeşitleri, komut yapıları, kullanılan kriptoloji teknikleri, kart erişim cihazları, ödeme sistemlerinde, haberleşmede kullanımı.

Ön şart: Yok

Kaynak Kitap: Smartcard Handbook 3rd Edition, Wolfgang Rankl, Wolfgang Effing, John Wiley Press & Sons, 2003

BGM 559 Büyük Veride Güvenlik ve Mahremiyet

Büyük Veri Nedir ve Büyük Veri Modeli, Büyük Veride Güvenlik ve Mahremiyet Kavramları, Mahremiyet neden önemlidir? Veri Mahremiyeti, Büyük Veride Saldırı ve Güven Modeli, Gerekli Altyapılar: Taahhüt Şemaları, Gerekli Altyapılar: Mahremiyet için Sıfır Bilgi Protokolleri, Büyük Verinin Güvenli İşlenebilmesinde Homomorfik Sistemler, Çoklu Sır Paylaşımı ve Büyük Verideki Uygulamaları, Anonimleştirme ve Kimliksizleştirme, Kimlik ve Nesne Tabanlı Şifrelemenin Büyük Veride Kullanımı, Güvenli Veri Tabanı ve Güvenli Bilgi Arama (Güvenlik Gerekleri, Veri İfşası, Çok Katmanlı Güvenli Veritabanı), Diferansiyel Mahremiyet, Çok Taraflı Güvenli Hesaplama Yöntemleri, Yao'nun Bozuk Devrelerine giriş, Güvenli Veri Madenciliğinde Yao'nun Bozuk Devrelerinin Kullanımı

BGM 560 Uygulamalı Kriptoanaliz

Ders kapsamında temel kripto algoritmaları ve analiz uygulamaları anlatılacaktır.

İçerik: Temel kripto algoritmaları ve analizleri: Sezar şifrelemesi ve uygulamalı frekans analizi, Vigenere şifreleme ve Kasiski testi, Indeks Çakışma Testi, Enigma ve ataklar, Purple ve ataklar, LFSR ve Berlekamp Massey algoritması, Jeffe üreteci ve korelasyon atakları, RC4 WEP ilklendirme atağı ve karşı önlemleri, PKZip şifreleme ve analizi, doğum günü atakları, Wang'ın MD5 çakışma bulma atağı, RSA çarpanlara ayırma algoritmaları: Dixon'un algoritması, ikinci dereceli elek, ayrık logaritma problem, bebek adımı dev adımı atağı, indeks kalkulus atağı.

Ön Şart: Yok

Kaynak Kitap:

- Handbook of Applied Cryptography by A. Menezes, P. van Oorschot and S. Vanstone, CRC Press, 1996.
- Applied Cryptography by Bruce Scheiner.

BGM 561 Bilgi Endinme Teknikleri

Bu derste, bilgi edinme tekniklerine giriş yapılarak bu tekniklerden haberleşme bilgi edinme (COMINT) ve açık kaynak bilgi edinme teknikleri (OSINT) üzerine yoğunlaşılacaktır. Haberleşme bilgi edinme tekniklerinde sensörden alınan bir işaretten başlayarak farklı kaynaktan alınan bilgilerin birleştirilip günümüzün ihtiyaçlarına uygun bir haberleşme bilgi edinme sistemi nasıl oluşturulacağı anlatılacaktır. Derste katılımcılardan açık kaynak bilgi edinme tekniklerine yönelik son yıllarda yapılmış tez, makale ve raporların ders projesi olarak hazırlanması ve sunması istenecektir.

BGM 563 Bulut Bilişimde Güvenlik ve Mahremiyet İçin Kriptografi

Bulut Bilişim Güvenliği altında servis-olarak-güvenlik önemli bir başlık olarak karşımıza çıkmaktadır. Derste konu başlıkları olarak kimlik doğrulama ve erişimi, kimlik yönetimi, güvenlik kriptografik bulut depolama ve veri güvenliği, kimlik doğrulamalı veri yapıları, veri mahremiyeti, güvenli ve şifreli arama, doğrulamalı hesaplama (örn. RAM programları), Kısmi/Tam Homomorfik Şifreleme (tam homomorfik ve indirgeme (bootstrapping) teknikleri), Bulut Bilişimde güvenli ve mahremiyet tabanlı denetim mekanizmaları, Hesaplamayı Buluta Tevdi Etme, Mobil Bulut Güvenliği, CloneCloud ve Cloudlet temaları ele alınacaktır. Dersin başında kriptografi ile ilgili kısa bir giriş yapılacaktır.

Ön Şart: Yok

Kaynak Kitap: Ders notları ve makaleler

- William Stallings – Cryptography and Network Security
- Stefan Rass, Daniel Slamanig - Cryptography for Security and Privacy in Cloud computing
- Above the Clouds: A Berkeley View of Cloud Computing

BGM 565 Siber Güvenlik için Makine Öğrenme Yöntemleri

Mahremiyet korumalı veri analizi: mahrem kişisel veriler ifşa edilmeden veri üzerinde analiz, k-anonymity, t-closeness,l-diversity, differential privacy

İçerik: Büyük veri analitiği, siber güvenlik alanında yer alan birçok problemin çözümünde kullanılabilmektedir. Dersin amacı, makine öğrenmesi alanında yer alan temel yöntemlerin (yapay sinir ağları, destek vektör makinesi, derin öğrenme gibi) siber güvenlik alanında sızma tespiti, ağ trafiğinin analiz edilmesi, veri kaçağı önleme (dlp), botnet tespiti, oltalama saldırısı, sosyal ağlarda zararlı hesapların tespiti gibi konularda kullanımını içermektedir. Diğer üniversitelerde benzer ders verilmektedir.

Ön Şart: Yok

Kaynak Kitap:

BGM 566 Kriptolojik Yöntemler

Intel işlemci mimarisi, XILINX FPGA mimarisi, Modüler Aritmetik (Montgomery, Barrett), Büyük sayı aritmetiği, RSA donanım tasarımı, RSA yazılım tasarımı, Eliptik Eğri tabanlı donanım tasarımı, Eliptik Eğri tabanlı yazılım tasarımı, SHA256-512 donanım tasarımı, SHA256-512 yazılım tasarımı, AES donanım tasarımı, AES komut seti, AES yazılım tasarımı, CRC yazılım tasarımı, CRC donanım tasarımı.

Ön Şart: Yok

Kaynak Kitap: Ders notları ve makaleler

BGM 570 Bilgi Teknolojileri Proje Yönetimi

Bu derste bir kuruluşa özgü bilgi teknolojisi amaçlarının planlanması, düzenlenmesi, yürütülmesi, ve denetlenmesi süreçlerinin tasarımı işlenecektir. Derste proje yönetimi, iletişim, analitik araçlar, güvenlik hedeflerinin belirlenmesi, paydaşların sürece dahil edilmesi, metriklerin tanımlanması, veri kalitesi gibi kavramlar ve konular işlenecektir. Uygulama pratiğine yönelik araçlar, tablolar ve örneklerle konular işlenecektir.

Ön Şart: Yok

Kaynak Kitap:

- Information Technology Project Management, Kathy Schwalbe, Cengage Learning.
- Seçilmiş kaynak okuma parçaları, makaleler ve sunumlar.

BGM 574 Bilgi Güvenliği Yönetimi

Bir organizasyonda toplam bilgi güvenliğinin kurulum ve işletiminde yapılması gerekenler anlatılacaktır.

İçerik: Bilgi sistemleri güvenlik yönetimi, güvenlik politikaları, varlık envanterleri, risk analizi, erişim kontrolü ve kimlik doğrulama, güvenlik mimarisi ve modelleri, işlem güvenliği, uygulama ve sistem geliştirme, iş sürekliliği ve felaket kurtarımı planlaması, bilgi güvenliği ile ilgili yasalar, bilişim sistemlerinin fiziksel güvenliği ve personel güvenliği.

Ön Şart: Bilgisayar Ağları (Computer Networks) arkaplanı

Kaynak Kitap:

- All in One CISSP 6. Editon, Shon Harris, McGraw Hill, 2013, ISBN: 970-0-07-178172-8
- Seçilmiş kaynak okuma parçaları, makaleler ve sunumlar

BGM 576 Yazılım Test ve Kalite Değerlendirme Teknikleri

Bu derste, yazılım testi ve yazılım kalitesi konularında (Doğrulama ve Geçerleme Süreci, Statik Kod Analizleri, Yazılım Test Seviyeleri, Teknikleri ve Türleri, Yazılım Test Araçları, Gereksinimler vb.) temel kavramlar, teknikler ve yöntemler işlenecektir.

İçerik:

Yazılım Test Mühendisliği ve Yazılım Kalitesi - Temel Kavramlar(Yazılım ve Yazılım Test Mühendisliği, Yazılım Felaketleri, Neden test ve analiz ederiz?), Gereksinimler (Neden önemli, nasıl olmalıdır?), Yazılım Geliştirme Süreçleri ve Doğrulama ve Geçerleme Süreci, Yazılım Test Seviyeleri, Teknikleri ve Türleri ve Gözden Geçirmeler, Hata Yaşam Döngüsü ve Yazılım Test Metrikleri, Yazılım Test Dokümantasyonu, Yazılım Test Organizasyonları ve Test Yönetimi, Yazılım Test Araçları ve Test Otomasyonu, Yazılım Kalitesi, Kalite Faktörleri, Kalite Metrikleri ve Statik Kod Analizleri ve Araçları, Kullanılabilirlik Değerlendirmeleri ve Testleri ve Araçları, Performans Testleri ve Araçları, Yazılım Test ve Kalite Standartları, Yazılım Güvenilirliği ve Güvenilir Yazılım Geliştirme Süreçleri.

Ön Şart: Yoktur.

Kaynak Kitap:

- Sommerville I.," Software Engineering", Addison Wesley, 2009
- Rick D. Craig, Stefan P. Jaskiel, "Systematic Software Testing", Artech House Publishers, 2002

BGM 580 Siber Güvenlik Hukuku

Bu bir hukuk ve politika dersidir. Sanal uzayda güvenlik konusundaki düzenleme araçları işlenecektir. Bilişim suçları ceza hukuku ve fikri mülkiyet hukuku düzenlemeleri bu düzenleme araçlarından sadece ikisidir. Konuyla ilgili uluslararası hukukun yeri ve rolü; kimlik denetleme ve kimlik yönetimi; özgürlük, mahremiyet ve genele açık kaynaklar; siber güvenlik stratejileri, konuyla ilgili dünyada ve ülkemizde yapılan çeşitli hukuki düzenlemeler bu derste işlenecek konular arasındadır.

Kaynak Kitap:

- Goldsmith, Who Controls the Internet? Illusions of a Borderless World, ISBN 9780195340648 Oxford University.
- Zittrain, The Future of the Internet -- And How to Stop It, ISBN 9780300151244, Yale University.
- Seçilmiş kaynak okuma parçaları, makaleler ve sunumlar.

BGM 585 Stratejik Siber Güvenlik

Uluslararası ilişkiler ve hukuk alanında kullanılan temel terim, kavram ve tanımlar. Siber uzaydaki temel aktörler ve internet yönetişimi. Ulusal siber güvenlik yönetişim altyapıları ve ulusal siber güvenlik politikaları/stratejileri. Uluslararası örgütlerin gerçekleştirdiği siber güvenlik faaliyetleri. Askeri alanda siber güvenlik ve siber-savaş. Siber espiyonaj ve siber terörizm. Kritik bilgi sistem altyapılarının korunması

Siber diplomasi. Siber alandaki mahremiyet konuları. Siber güvenlik ekonomisi.

Kaynak Kitap: Çeşitli kitaplardan seçilen bölümler ve farklı kaynaklardan alınacak makaleler ve sunumlar.