

## Meslek Yüksek Okullarında Bilgi Güvenliği Eğitimi

Ar. Gör. E. Karaarslan<sup>1</sup>, Prof. Dr. H. Şengonca<sup>2</sup>

<sup>1</sup>Ege Üniv. Uluslararası Bilgisayar Enst., <sup>2</sup>Ege Üniv. Bilgisayar Müh.  
Ege Üniversitesi, 35100 Bornova-İZMİR  
<sup>1</sup>[enis@bornova.ege.edu.tr](mailto:enis@bornova.ege.edu.tr), <sup>2</sup>[sengonca@bornova.ege.edu.tr](mailto:sengonca@bornova.ege.edu.tr)

### ÖZET

Bilişim sistemlerinde bilginin gizliliği, özgünlüğü ve bütünlüğü gibi özelliklerinin sağlanmasının önemi büyüktür. Bilişim alanında çalışacak olan kişiler, bilgisayar sistemlerine yapılan saldırılara karşı önlem alabilecek düzeyde bilgi sahibi olmalıdır. Meslek Yüksek Okulları'nda uygulanması önerilen bilgisayar güvenliği eğitiminde, lisans ve yüksek lisans düzeylerinde verilen benzer güvenlik derslerinin tersine konular ana başlıklar olarak ele alınmakta ve öğrencinin daha çok uygulamalar üzerinde yoğunlaşması hedeflenmektedir.

**Anahtar Kelimeler:** Bilgi Güvenliği Dersi, Bilişim Güvenliği Temelleri

### GİRİŞ

Günümüzde bilgi ile bu bilgiyi işleyen ve saklayan bilgisayar sistemlerinin saldırılara karşı korunması yaşamsal önem taşımaktadır. Teknolojinin gelişmesi ile bilgi kolaylıkla bir noktadan diğerine iletilebilmekte ve İnternet ortamı üzerinden paylaşılabilir. Teknolojinin her getirdiği yenilik aynı zamanda bir zayıflık ve saldırı açığı olarak karşımıza çıkabilmektedir. Bu teknolojileri izleyecek ve bilgi güvenliğini sağlayacak kişilere her geçen gün daha çok gereksinim duyulmaktadır. Bilgi güvenliği eğitimi, güvenlik konusundaki açığı kapatmaya yönelik programlar sunmaktadır.

Bilgi güvenliği eğitimi, farklı gereksinimleri gidermeye yönelik olarak dört ana grupta toplanabilir (Bishop, 2000):

- **Halkın bilinçlendirilmesi:** Halk, teknolojilerin ayrıntılarını bilmek istemez. Tek öğrenmek istediği bilgisini nasıl güvenli tutabileceğidir. Bu tür eğitimde, kullanıcının tehditler ve savunma yöntemleri hakkında bilinçlendirilmesi hedeflenmektedir.
- **Akademik Eğitim:** Bu eğitimde güvenliğin altında yatan temel prensipler üzerinde yoğunlaşmaktadır. Amaç öğrencileri bu prensipleri uygulayabilir, yenilerini geliştirebilir duruma (konuma) getirmektir.
- **Endüstriye Yönelik Eğitim:** Endüstri, kendi değerlerini koruyacak güvenlik düzenekleriyle ilgilenmektedir. Bu düzeneklerin etkin olarak güvenliği sağlaması önemlidir ve temelde yatan prensipler üzerinde pek yoğunlaşmaz. Uygulamaya yönelik eğitim esastır.

- **Ulusal Güvenliğe Yönelik Eğitim:** Devletin ulusal kaynakları korumak için kullandığı yöntemlerden birisi bilgi güvenliğidir. Yasaların uygulanması ve düzenlemelerin sağlanması için güvenlik politikalarının ve sistemlerin geliştirilmesi üzerinde yoğunlaşmaktadır. Sistemler geliştirilirken, sürecin endüstrinin önemseydiği kadar düşük maliyetli (cost-effective) olması üzerinde yoğunlaşmamaktadır.

Bilgi güvenliği eğitimi müfredat programlarında ayrı dersler olarak verilebileceği gibi, var olan derslerle de bütünleştirilebilir. İdealde, bilgi güvenliği konularının ayrı uygulanmasındansa müfredattaki uygun konulara bütünleştirilmesinin gerektiği ama bunun henüz kitaplar, kurs materyalleri ve pratik labratuvar uygulamalarında etkin olarak gerçekleşmediği gözükmektedir (Irvine ve ark., 1998). Bishop, programlama derslerinde yazılım güvenliğinin anlatılmasının önemine değinmektedir (Bishop, 1997). ACM'in iki yıllık bölümler için önerdiği ders programında işletim sistemi ve ağ temelleri derslerinde bir bölüm güvenlik konularına ayrılmıştır (ACM, 2002).

Bilgi güvenliği eğitiminin içerdiği konuların çeşitliliği, kapsamlı olması ve her geçen gün değişen bir alan olmasının eğitime getirdiği bazı zorluklar bulunmaktadır. Bu nedenle iki saatlik bir güvenlik dersinin hazırlığının on veya daha fazla saat alabileceği belirtilmiştir (Yurcuk ve Doss, 2001).

Bilgisayar güvenliği dersleri, Türkiye'de çoğunlukla bilgisayar mühendisliği ve enformatik bölümlerinin yüksek lisans ve ender olarak lisans düzeyinde

verilmektedir. Meslek Yüksek Okulları veya başka bir deyişle iki yıllık üniversite programlarında bilgisayar güvenliği eğitimi olarak önerilen programda, endüstriye yönelik eğitim yöntemi üzerinde yoğunlaşmaktadır. Konunun ayrıntılarına girilmemekte, ana fikrinin verilmesi amaçlanmaktadır. Öğrencinin uygulamalar aracılığıyla konuyu anlaması hedeflenmektedir.

Bildiride öncelikle iki yıllık bölümlerde uygulanması önerilen ders programı verilecek, sonra bilgi güvenliği dersleri verilirken uygulanabilecek yöntemler anlatılacaktır.

## DERS PROGRAMI

Bu eğitimin Meslek Yüksek Okulları'nda "Bilgisayar Donanımı" ve "Bilgisayar Programcılığı" dallarında iki ayrı program olarak okutulması önerilmektedir.

"Bilgisayar Donanımı" bölümüne uygulanması önerilen ve daha çok sistem güvenlik elemanı yetiştirmeye yönelik olarak tasarlanan program dört ana bölümden oluşmaktadır. Bu programda ilk iki bölüme ağırlık verilmiş, son iki bölümün uygulanıp uygulanmaması Meslek Yüksek Okulu'na bırakılmıştır. Son iki konunun her birinin üniversitelerde ayrı dersler olarak okutulduğu unutulmamalı, öğrencinin konuyu ana başlıklarıyla (hatlarıyla) anlaması hedeflenmelidir. Bu program için önerilen bölümler aşağıdaki gibidir:

- Bilişim Güvenliği Temelleri
- Temel Bilgisayar Güvenliği
- Ağ Güvenliği
- Şifreleme

"Bilgisayar Programcılığı" bölümünde uygulanması önerilen, daha güvenli yazılımlar geliştirebilecek programcı yetiştirmeye yönelik program üç ana bölümden oluşmaktadır. Günümüzde birçok yazılımın ağ üzerinden iletişim kurarak çalıştığı göz önüne alındığında, ağ güvenliği ve ağ üzerinden geçen verilerin şifrenmesi gerekliliği ve yöntemleri üzerinde durulması gerekmektedir. Bu nedenle "Bilgisayar Donanımı" bölümü için önerilen "Ağ Güvenliği" ve "Şifreleme" bölümleri birleştirilerek daha öz "Ağ Üzerinden İletişim ve Şifreleme" bölümünün uygulanması önerilmiştir. Bu program için önerilen bölümler aşağıdaki gibidir:

- Bilişim Güvenliği Temelleri
- Yazılım Güvenliği
- Ağ Üzerinden İletişim ve Şifreleme

Konuların ne kadar detayına girilebileceği mevcut zamana ve öğrencilerin seviyesine göre değişecektir. Her iki programın en az iki ders dönemi olarak okutulması daha etkin olacaktır.

## Bilişim Güvenliği Temelleri

Programın bu bölümünde güvenlik tehditleri ve bilgi güvenliği kavramlarına değinilmektedir. Bilişim sistemlerinin tuttıkları (store), ilettikleri (transmit) ve işledikleri (process) bilginin gizliliği, bütünlüğü gibi özelliklerinin korunmasının önemi ve yöntemleri anlatılmalıdır. Bilgisayar teknolojisinin kötüye kullanılmasının gerçek yaşamdan örnekler verilerek şekillendirileceği bu bölümde öğrencinin "hacker", virus, ateş duvarı (firewall) ... vb gibi kavramları tanınması da hedeflenmektedir. Güvenlik sürecinin önleme (prevention), saptama (detection) ve kurtarma (recovery) gibi aşamalardan oluştuğu anlatılmalıdır. Güvenlik politikalarının ve güvenlik sürecinde yazılı kurallar bulunmasının önemi üzerinde durulmalıdır. Bilgisayar güvenliğinin hukuksal boyutu Türkiye'den ve dünyanın çeşitli yerlerinden örnekler verilerek gösterilmelidir.

## Yazılım Güvenliği

"Bilgisayar Programcılığı" dalında uygulanması önerilen yazılım güvenliği bölümünde; istemci/sunucu sistemler için geliştirilen uygulamalarda güvenlik, kimlik denetimi (authentication) ve erişim denetiminin nasıl gerçekleştirilebileceği konuları verilmelidir.

Kapsamlı olarak sınanmış (test) ve yanlışları ayıklanmış (debug) sağlam (robust) kod geliştirilmesi, güvenli sistemler oluşturmak için esastır. Bu nedenle programlama sınıflarında bilgisayar güvenliği eğitiminin verilmesinin faydaları olacaktır (Bishop, 1997).

Bölümlerde daha önceki derslerde verilen programlama dillerinde uygulama yapılabilir. Programın bu bölümü için Java programlama dilinin uygulanması önerilmektedir. Özellikle iletişim protokolleri kullanacak istemci/sunucu uygulamalarında, Java dilinin getirdiği socket programlama ve hazır kütüphaneler gibi kolaylıklar önemli bir artı olarak ortaya çıkmaktadır.

Cornell üniversitesi bilgisayar güvenliği dersi<sup>1</sup> ve Portland üniversitesi bilgisayar güvenliği pratiği<sup>2</sup> dersi örnek olarak verilebilir.

## Temel Bilgisayar Güvenliği

Sistem yöneticilerinin uğraştığı temel konulardan biri temel bilgisayar güvenliğidir. Alınan önlemlerin kapsamlı olması kadar kullanıcıların da bilgilendirilmesinin önemli olduğu vurgulanmalıdır.

<sup>1</sup> CS513: Bilgisayar Güvenliği Dersi Sayfası  
<http://www.cs.cornell.edu/html/cs513-sp99/>

<sup>2</sup> Bilgisayar Güvenliği Pratiği (Computer Security Practicum) Dersi Sayfası  
<http://www.cs.pdx.edu/~markem/CLASSES/Security/Practicum/index.html>

Ana sistem (host) tabanlı güvenliğin anlatılacağı bu bölüm şu alt kısımlardan oluşmaktadır:

- **Fiziksel Güvenlik:** Sistemlerin fiziksel güvenliği sağlanmazsa üzerinde uygulanacak güvenlik önlemlerinin hiçbir önemi kalmamaktadır. Genel fiziksel güvenlik yöntemleri bu kısımda ayrıntılı olarak anlatılmalıdır.
- **İşletim Sistemi Güvenliği:** Windows ve Unix/Linux işletim sistemlerinde güvenliğin sağlanma yöntemleri anlatılmalıdır.
- **Uygulama Güvenliği:** Kurulan uygulamalar ile birlikte gelebilecek güvenlik açıkları ve bu açıkların saptanmasında ve önlenmesinde nelere dikkat edilmesi gerektiği anlatılmalıdır.
- **Antivirüs Sistemleri:** Virüsler, Truva Atları (Trojan) ve benzeri saldırılara karşı korunma yöntemleri anlatılmalıdır.
- **Ana Sistem Tabanlı Güvenlik Duvarları:** Özellikle sunucu sistemlerinde kurulacak güvenlik duvarları ile o sistemin korunma yöntemleri anlatılmalıdır.
- **Kullanıcı Yönetimi:** Sistemde var olan kullanıcıların güvenliğinin ve denetiminin sağlanmasının önemi anlatılmalıdır.

### Ağ Güvenliği

Temel ağ kavramı verilerek ağ üzerinde iki aygıtın nasıl birbiriyle iletişim kurabildiği, TCP/IP protokol yığıtı konusunda temel bilgi verilmelidir. Özellikle IP versiyon 4 (ipv4)'ün zayıflıkları ve IP versiyon 6 (ipv6)'nın bu zayıflıklara karşı sunduğu çözümlere değinilmelidir.

Dış ağlardan gelen saldırılara karşı kullanılan Ağ Güvenlik Duvarı ve Sunucu Tabanlı Güvenlik Duvarı ayrımı belirgin olarak yapılmalıdır. Saldırı Saptama Sistemleri ve benzeri saldırı saptama düzeneklerine değinilmeli ve sistem güvenlik yöneticisinin görevleri belirtilmelidir.

### Şifreleme

Kriptografi yani şifre biliminin ana hatları anlatılarak önemi vurgulanmalıdır. Simetrik Şifreleme ile Asimetrik Şifrelemenin (Genel – özel *Anahtarlar*) farklarına konunun ayrıntısına inilmeden değinilmelidir.

### Ağ Üzerinden İletişim ve Şifreleme

“Ağ Güvenliği” ve “Şifreleme” bölümlerinin özetlenerek “Bilgisayar Programcılığı” dalına yönelik hazırlanmış halidir. Bu konuların özü anlatıldıktan sonra programlamada uygulaması üzerinde yoğunlaşılmalıdır.

### EĞİTİM YÖNTEMLERİ

Bilgi güvenliği eğitimi verilirken birçok değişik yöntem bir arada uygulanabilir. Yurcuk ve Doss'un ayrıntılı olarak anlattığı yöntemler şu şekilde özetlenebilir (Yurcuk ve Doss, 2001):

- **Pratik (Hands-on) Uygulamalar:** Uygulama yapılarak temel kavramların keşfedilmesi hedeflenmektedir.
- **Eğlendirici Etkinlikler:** Şifrelerin sınıfta kırılması veya bulmaca şeklinde hazırlanmış şifrelerin çözülmesi gibi etkinliklerle konunun daha iyi anlaşılması sağlanmaktadır.
- **Gerçek Yaşam Örnekleri:** Konuyla ilgili ilgi çekici, tarihi veya olabilirse güncel örnekler verilerek ders renklendirilmektedir.
- **Uzman Kişi Katılımı:** Bilişim sektöründen bu işi yapan kişilerin derse katılıp kendi uzmanlıkları konusunda öğrencileri bilgilendirmeleri sağlanmaktadır.
- **Proje Tabanlı Eğitim:** Öğrencilere projeler verilerek deney yapmaları, sunum yapmaları veya rapor sunmaları istenmektedir. Uygulamaya yönelik projeler seçilmelidir.
- **Araştırmaya Yönelten Eğitim:** Öğrenciye araştırma yöntemleri tanıtılmakta ve teknolojiyi yaşamsal önem taşıdığı vurgulanmaktadır.
- **Saldırı /Savunma Esaslı Lab Çalışması:** Öğrencilerin saldıran (offensive) ve savunan (defensive) gruplara ayrılarak sistemler üzerinde çalışma yapması sağlanmaktadır.

Çeşitli üniversitelerde okutulan kriptografi ve güvenlik derslerine <http://avirubin.com/courses.html> adresinden ulaşılabilir.

### LABRATUVAR UYGULAMA ÖNERİLERİ

Labratuvar uygulamalarının önemi açıktır. Irvine, labratuvar uygulamalarının önemini ve güvenlik eğitiminin etkinliğinin nasıl artırılabileceğini bildirisinde detaylı olarak anlatmıştır (Irvine, 1999). Öğrenci labratuvar uygulamalarıyla konuları daha iyi kavrayabilmekte ve öğrendiği bilgiler daha kalıcı olmaktadır.

Dick Scuglik'in<sup>3</sup> bir röportajda belirttiği gibi; güvenlik eğitiminde, öğrenciye bir sistemi nasıl savunacağını öğretebilmek için önce bir sisteme nasıl girilebileceğini öğretmek gerekebilecektir. Geleceğin olası bilgisayar suçlularını yetiştirmeden nasıl güvenlik eğitimi verileceği bir sorun olarak karşımıza çıkmaktadır.

Öğrenciler iki gruba ayrılmalı; bir grup korunması istenen bir bilgisayar sistemi için savunma işlevini yerine getirirken, diğer grup o makinaya saldırıp ele geçirmeyi veya ağa bağlanamaz hale getirmeyi denemelidir. Bilgisayar sayısına göre bu gruplardaki kişi sayısı ayarlanabilir.

<sup>3</sup> “Computer Security sees as next hot job; demand strong for Network, Web professionals”, Nicolet News & Events, <http://198.150.165.138/press/compsecur.html>

Bu süreçte öğrencilere benzeri saldırıları ders dışında uygulamaları belirtilmeli, olabilirse bu saldırı uygulaması sırasında laboratuvar ortamı dışarıdan ayrılmalıdır. Derste öğretilenlerin savunma amaçlı olduğu unutulmamalı, bu tür bilgilerin izinsiz ve saldırı amaçlı kullanımında oluşabilecek suç ve hukuksal boyut konusunda öğrenci bilgilendirilmeli ve uyarılmalıdır.

Labratuvar uygulamalarında kullanılabilir ürünler iki ana grupta incelenebilir:

- **Ticari Ürünlerin Kullanımı:** Gerçek sistemlerde kullanılan ticari ürünlerin kullanımı sağlanarak öğrencinin bu sistemler hakkında bilgi kazanması hedeflenebilir. Okullar bu ticari ürünleri sağlayan firmalarla, ürünü sadece laboratuvar ortamında kullanmak gibi özel anlaşmalar yapmaları durumunda, ücretsiz olarak bu ürünleri temin edebilir (Irvine, 1996).
- **Ücretsiz Ürünlerin Kullanımı:** Ücretsiz olarak temin edilebilen ve ihtiyaca göre değiştirilebildikleri için esnek bir ortam sağlayan ürünler tercih edilebilir. Bildiride bu tür ürünlerin kullanılması tavsiye edilmiştir.

İşletim güvenliği uygulamaları için Unix tabanlı bir işletim sistemi olan Linux'un kullanılması önerilmektedir. Linux, istenilen değişikliklerin yapılmasında esnek bir ortam sağladığı için tercih edilmektedir. Linux işletim sisteminde güvenlik uygulamalarına ilişkin ayrıntılı bilgi için bakınız (Çınar ve Bıçak, 2003).

Ağ güvenliği uygulamasında bilgisayarlar bir hub aygıtı aracılığıyla birbirine bağlanmalı ve bilgisayarlar birbirine veri gönderirken bir makinada koklayıcı (sniffer) programı çalıştırılmalıdır. Böylece verinin aktığı bazı yerlerde istendiğinde nasıl kolaylıkla koklayıcı programları aracılığıyla iletişimin dinlenebileceği ve geçen bilginin elde edilebileceği gösterilmelidir.

Şifreleme uygulamasında PGP<sup>4</sup> yazılımı kullanılması önerilmektedir. E-posta gönderiminde başkasının genel (public) şifresiyle şifreleyip gönderme, kendi özel (private) şifresiyle sayısal imza kullanma gibi uygulamalar öğrenciye yaptırılmalıdır. PGP programının kullanımına ilişkin ayrıntılı bilgi için bakınız (Özaydemir, 2001). Verinin şifrelendiğinde iletişimi dinleyenlerin ancak anlamsız karakterler yakalayabildikleri gösterilerek güvenlikte şifrelemenin önemi vurgulanmalıdır.

## KAYNAK

Saldırı ve savunma yöntemleri her geçen gün değişmektedir. Bu değişime hiçbir basılı yayının

<sup>4</sup> PGP: Pretty Good Privacy, ücretsiz temin edilebilecek şifreleme ve sayısal imza programı

yetişemeyeceği açıktır. O yüzden bu eğitimin temel kaynağı, içeriği sürekli güncellenen ve çeşitli kaynaklar sunan İnternet olmaktadır. İnternette bulunabilecek bu konuyla ilgili kaynakların çoğunun İngilizce olması öğrenciler için bir engeldir. Güvenlik konusunda Türkçe belgeleme projesi yürüten <http://security.ege.edu.tr> önemli başvuru kaynaklarından biri olarak karşımıza çıkmaktadır.

Bilgisayar güvenliği eğitiminde, eğitmenin güvenlik bilgisinin tam olması gerekmektedir. Burada kaynak olarak verilecek kitaplar hem eğitmenin hem de öğrencilerin eksiklerini gidermesinde yararlı olabilecektir:

1. Marshall D. Abrams, Sushil Jajodia, Harold J. Podell, eds. "Information Security: An Integrated Collection of Essays. IEEE Computer Society Press", 1995, Baskısı tükenen bu kitaba aşağıdaki adresten ulaşılabilir: <http://www.acsac.org/secshelf/book001/book001.html>.
2. Applied Cryptography, John Wiley & Sons, Bruce Schneier, ISBN: 0471117099
3. Network Security Essentials, Applications and Standards, Prentice Hall , William Stallings, ISBN: 0130160938
4. Computer Networks, Prentice Hall, Andrew S. Tanenbaum, ISBN: 0-13-394248-1
5. Building Secure Software, John Viega and Gary, McGraw Addison-Wesley, ISBN: 0-201-72152-X

## SONUÇ

Her geçen gün artan güvenlik gereksiniminin bilgisayar güvenlik uzmanı gibi yeni iş alanları açtığı ve güvenliği sağlamanın öneminin her geçen gün daha da artarak anlaşılacağı unutulmamalıdır. Günümüzde, sistem açıklarını bulan ve çözümleri anlatan kişilerden çok daha fazla personel, sistemleri yönetmek ve ayrı sistemlerde bu çözümleri uygulamak için gereklidir. Bu nedenle, bilgi güvenliği eğitiminin Meslek Yüksek Okulları'nda başlatılması için gereken altyapı çalışmalarının önemi açıktır.

## KAYNAKÇA

ACM Two Year College Education Committee & IEEE Computer Security Association, *Computing Curricula 2003, 2002, Guidelines for Associate-Degree Curricula in Computer Science*, [http://www.acmtvc.org/2003CurriculumRe\\_ports.cfm](http://www.acmtvc.org/2003CurriculumRe_ports.cfm)

Bishop M., 1997, *Computer Security in Introductory Programming Classes*, Workshop on Education in Computer Security

- Bishop M., 2000, *Academia and Education in Information Security: Four Years Later*, Proceedings of the Fourth National Colloquium on Information System Security Education
- Çınar Ç., Bıçak M., 2003, *Linux Güvenlik Raporu*, <http://security.ege.edu.tr/dokumanlar.php>
- Irvine, C.E., 1996, *Goals for Computer Security Education*, Proceedings of the IEEE Symposium on Security and Privacy, pp. 24-25
- Irvine, C.E., Chin, S-K., and Frincke, D., 1998, *Integrating Security into the Curriculum*, *IEEE Computer*, pp. 25—30.
- Irvine C. E., 1999, Amplifying Security Education in the Laboratory, Invited talk in the *Proceeding IFIP TC11 WC 11.8 First World Conference on Information Security Education*, Kista, Sweden, pp 139--146
- Özaydemir A., 2001, PGP ile Sayısal İmza ve Şifreleme, <http://security.ege.edu.tr/dokumanlar.php>
- Yurcik W., Doss D., 2001, *Different Approaches in the Teaching of Information Systems Security*, 18th Annual Information Systems Security Education Conference, <http://colton.byuh.edu/isecon/2001/04a/Yurcik.Doss.sec.pdf>