Secure Programming

Mehmet Tahir SANDIKKAYA

Spring 2022

Istanbul Technical University
Computer Engineering Department

Syllabus

Week	Date	Rct	Covers	Subject	Announcement	Submit
1	22nd Feb		7	Fundamental concepts of security	TP-A	
2	01st Mar		1, 7	Compilation and Execution		
3	08th Mar		1, 7	Stack overflow and its mitigation	Asg1-A	
4	15th Mar		1, 7	Dynamic memory management		
5	22nd Mar	R	3, 7	Canonicalization attacks and mitigation	Asg2-A	Asg1-S
6	29th Mar		2, 7	Injection attacks	Asg1-G	
7	05th Apr	R	2, 7	Injection mitigation	Asg3-A	Asg2-S
8	12th Apr		4	Reverse engineering and obfuscation	Asg2-G	
9	19th Apr		5	Fundamental cryptography		Asg3-S
A	26th Apr	R	5	Principles of computer communication	Asg3-G	MT
-	03rd May			Spring break		
B	10th May		5	XSS & CSRF attacks and mitigation	Asg4-A	
C	17th May	R	5	Race conditions	MT-G	
D	24th May		6	Permission and authorization mechanisms in contemporary languages		Asg4-S
E	31st May		7	Test and static analysis tools	Asg4-G	TP-S

Course Information

What's the aim of this course?

This course aims to teach how to write secure code by exemplifying possible security vulnerabilities or presenting exploits in detail.

This course is not intended to teach any unethical behavior. Please follow IEEE/ACM code of ethics if you feel in doubt. Do not forget that your actions might have legal consequences. The instructor, the department, the faculty or the university has no legal binding of your actions with respect to you have learned in this lecture.

Course Material Ownership

All of the written, published, broadcast, recorded material of this course belongs to the instructor and produced with the permission of the department.

It is prohibited to copy, share, publish any of the course material without written permission of the instructor. The course material includes and not limited to slides, lecture notes, assignments, homework, in-class instructions, recitations; audio or video recordings of any part of the course; midterm, final or quiz examinations, and their solutions; as well as any written material or source code that is prepared by the instructor or by the students registered to the class.

Follow the Oath

As a registered student of ITU Computer Engineering Department BLG460E course, I hereby declare that I willfully accept the following principles:

- ✔ I willfully registered to the course and have been informed of the course principles
- ✔ The instructor, the department, the faculty or the university has no legal binding of my actions with respect to what I have learned in this lecture
- ✔ I am aware that I could unregister/drop the course if I do not agree these principles
- ✔ In my lifetime, I shall never develop stalkerware or any other technology that may disturb people's life and/or privacy
- ✔ In my lifetime, I shall follow Kerckhoffs's principle [Kerckhoffs, 1883] in my designs
- ✔ In my lifetime, I shall design transparent security systems that are auditable & reproducible
- ✔ In my lifetime, I shall never roll out my own cryptographic algorithm/software/library without public & scientific inspection

Date, location, name and signature

Send a text file that contains "I agree on the course criteria and the provided oath" via Ninova.

Kerckhoffs's Principle

1. The system must be practically, if not mathematically, indecipherable
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will
4. It must be applicable to telegraph communications
5. It must be portable, and should not require several persons to handle or operate
6. Given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules

Hints for Success

Be careful about your communication, especially during written exams.

- ✔ Comprehension is your responsibility, be concise
- ✔ Keep in mind; the answers that are sound, consistent and non-false receive points
- ✔ Arguing from anecdote
- ✔ See (mis)-communication examples among class files
- ✔ Never forget the transfer of Kevin Großkreutz while submitting your homework, see the video among class files
- ✔ Do incremental uploads
- ✔ Listen, take notes, and take some rest [Hopkin, 2021]
- ✔ Ask in advance!

Ingredients

- ✔ You may use any **spare** computer for the exercises
- ✔ If you don't have one, I advise you install a virtual box `https://www.virtualbox.org/`
- ✔ You can download a ready-to-use image `https://drive.google.com/file/d/16vVBs0pk0cC-Ok_ryNrFOB6lF89tR8j_/view?usp=sharing`
- ✔ Username and password for this image is: `blg460e`
- ✔ You can also follow the instructions for this course if you want to use vagrant `https://github.com/itublg/itucs-vmimage`
- ✔ Username and password for this image is: `vagrant`

Who's in charge of the course?

The course will be held on Tuesdays @ 15:30 local time in EEB 5204.

Instructor Asst. Prof. Dr. Mehmet Tahir SANDIKKAYA
e-mail sandikkaya@itu.edu.tr
Room EEB 5310

Teaching Assistant Ayşe SAYIN
e-mail sayinays@itu.edu.tr
Room EEB 5211

Course objectives

1. Teaching possible security flaws that may be encountered during software implementation
2. Students can produce software that does not be affected by known development-time vulnerabilities
3. Students will gain defensive development style to be less affected by future development-time vulnerabilities
4. Students will gain the technical abilities to produce secure software

Learning outcomes

1. Write programs who can resist memory overflows 16/46
2. Protect the programs they write against the improbable effects of malicious user input 20/46
3. Know the protection by sanitizing non-standard components 18/46
4. Obfuscate their code 7/46
5. Write programs against well-known Internet vulnerabilities 23/46
6. Know how to use permissions and authorization 11/46
7. Obtain defensive programming style to mitigate future vulnerabilities 43/46

How to save the princess?

- ✔ At least 7/24 from 4 assignments (> 7/24 or VF)
- ✔ Collect at least 24/70 (or VF)
- ✔ Collect at least 40/110 during the course (or FF)

How to collect points?

Quantification	Contribution	Time
Homework	$4 \times 06\% = 24/110$	Weeks 5, 7, 9, D
Quiz	$1 \times 10\% = 10/110$	Surprise!
Mid-term	$1 \times 26\% = 26/110$	Week A
Term-project	$1 \times 10\% = 10/110$	Week E
Final	$1 \times 40\% = 40/110$	Week F

Resources

1. [Wheeler, 2015]
2. [Long et al., 2013]
3. [Seacord, 2013]
4. [Erickson, 2008]
5. [Howard and LeBlanc, 2003]
6. Check the provided bilingual glossary among course slides

Review 15 / 36

Instructor Review

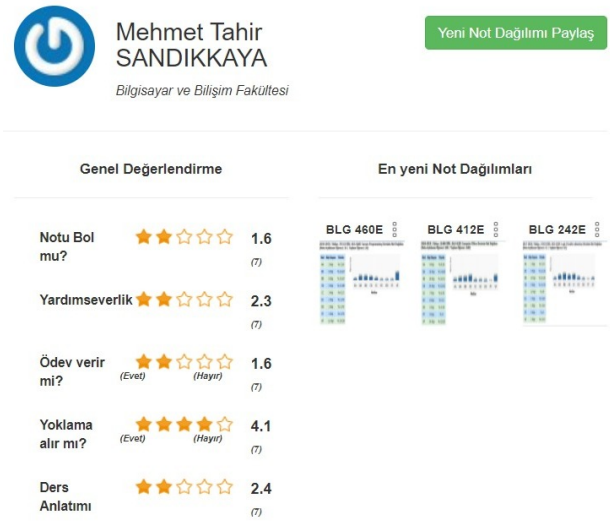
- ✔ garip bir şey kendileri aynı anda kıl olup hoş adam da diyebiliyorsunuz
- ✔ ya ben hayatımda daha korkunç bi asistan görmedim ya hayır elektrik-elektronik fak.den olmamama rağmen heryerde yemekhanede bile mütemadiyyen gördüğüm bişahsiyet:) ya korkuyorum ya allaam elektrik koridorundan geçerken çattt diye kapı açılıyo arkasından çıkıyo rahmetli barış manço karşıma dikiliyo sanki besmele çekmekten canım çıktı:) burdan elektrik fak.dekanına itü rektörlüğüne sesleniyorum hoca yapmasınlar bu adamı ya sevimli bi şekle girmeden

Instructor Review

- ✔ Derste işlenenlerin uygulanabileceği bir ortamın öğrenciler ile paylaşımı da güzel olabilirdi, örneğin owaspwba diye bir şey görmüştüm bu tarz uygulamalar da(çoğu kişinin bakmayacağından emin olsam da) istekli kişilerin daha iyi öğrenmesi açısından daha iyi olur diye düşünüyorum. Ayrıca bu dersin ITU'de zorunlu ders olması gerektiğini düşünüyorum, belki de çok kişi dersi geçemez diye yapmıyorlardır :) .
- ✔ Her şey harika

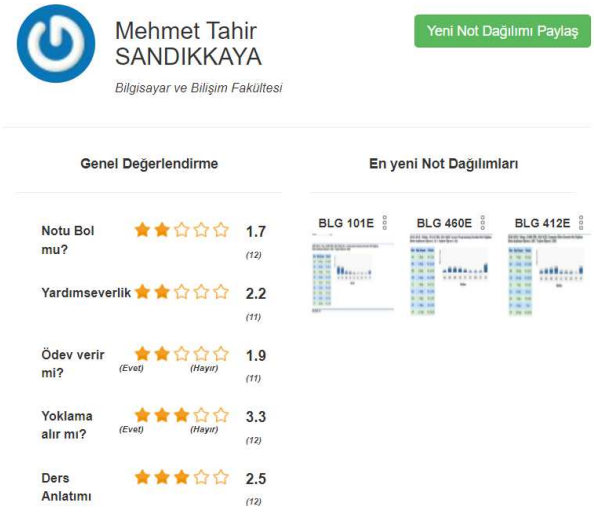
Instructor Review

2021

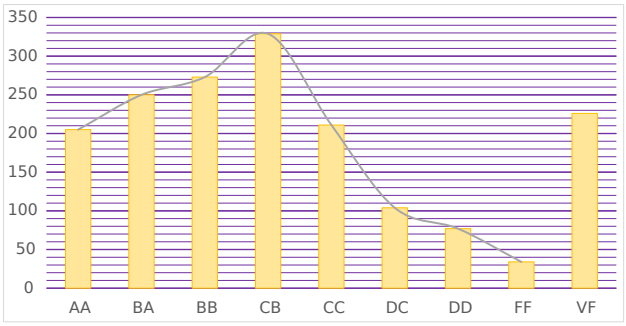


Instructor Review

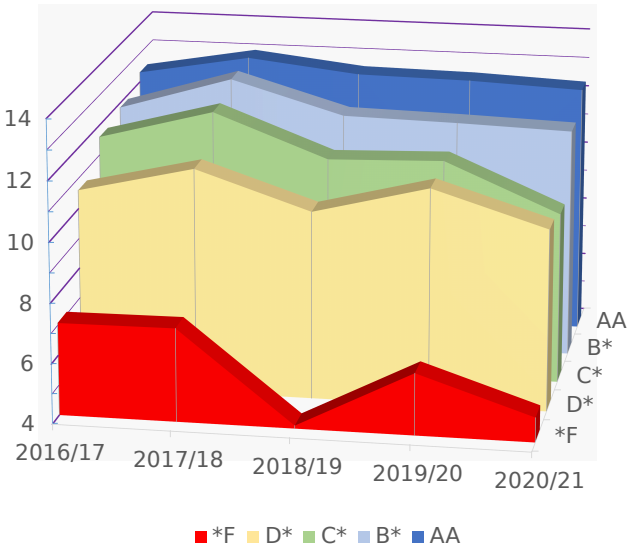
2022



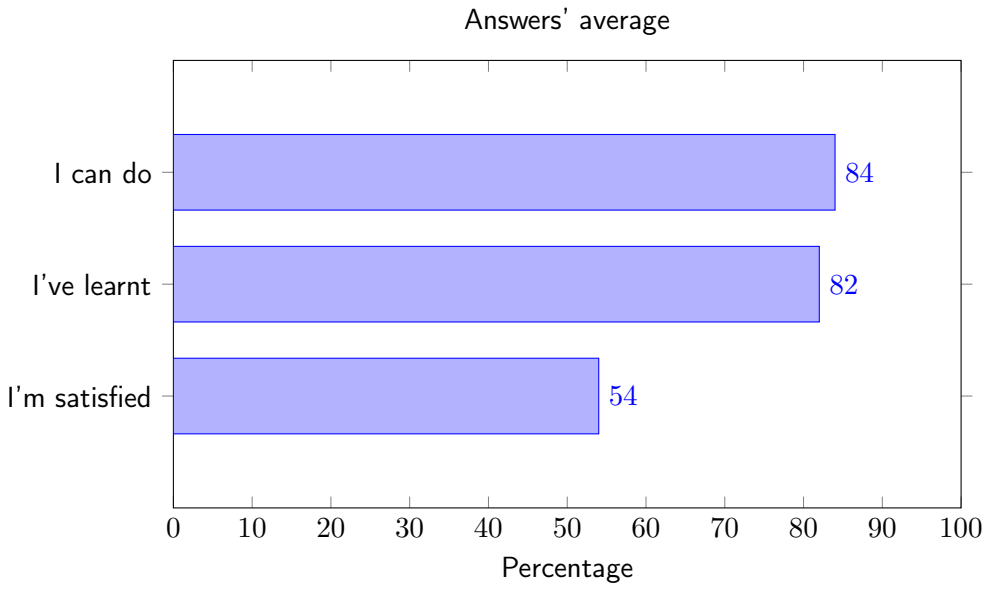
Instructor Grading



Attendance Review



Course Review



Course Review

Rated 5/5 previous year!

Previous years' remarks

- ✔ Do you have any comments about the quality of the course and its instructors?
- ✔ Ders içeriği ilgi çekici ve günümüz için değerli olsa da inatla öğrencilere kaynak verilmemeye çalışılması dersin kalitesini büyük ölçüde düşürdü. Ders sözlü olarak yeterli seviyede işlendiğini düşünüyorum. Ancak yazılı kaynak olmadan genel olarak dersten alınacak verim çok düşüyor. Dersin içerisinde yapılan sınavlar bilgi ölçme kapasitesine sahip olmayan vasat değerlendirmelerdi. [...] Sınava yönelik olan çalışma sorularının sınavda çıkabilecek sorulardan oluşmuyordu. [...]

Previous years' remarks

- ✔ Do you have any more suggestions for improving the course?
- ✔ increase the pace make it more interesting with applications and visiual aids, show us some techniques live in the class
- ✔ I am not sure if it is possible, but adding few homeworks or expanding them for practical purposes would be appreciated. I think applying the related issues is so essential. Other point is lecture slides, I took notes in this semester and worked well for me but if I missed a class, that would be a big problem. Lecture slides should include all the material in general or at least titles and headings.
- ✔ The resources are not egough to study the exams.

Previous years' remarks

- ✔ Do you have any more suggestions for improving the course? [Cont'd]
- ✔ I think course slides could be more illuminave [sic]. I mean, they look like presentation slides instead of being course slides. They only include headers of the subject. I know you expect students to come to the course and take notes but, if the aim of the course is teaching students how to program securely, I believe slides should have enough information for students to work on their own.
- ✔ Dersin slaytları düzgün olarak hazırlanmalı. Kaliteli yazılı kaynaklar verilmeli. Sınavlar titizlikle hazırlanmalı ve süreleri uzatılmalı. Ödev tamamlama süreleri uzatılmalı. Sınava yönelik olarak çözülen soruların sınavda benzerleri çıkmalı.

Previous years' remarks

- ✔ Do you have any advice for students taking this course in the future?
- ✔ There is no clear and enough resources so listen carefully in the class and maybe take notes. It is not clear what kind of questions will be in the exams
- ✔ Do homeworks and take notes in class because there would be no lecture slides :) and you will be just fine
- ✔ Ödevlere çok titizlikle yapsınlar.
- ✔ Should have taken notes :)

Previous years' remarks

- ✔ Do you have any other comments?
- ✔ İTÜ kişisel egoların tatmin edildiği bir üniversiteden ziyade öğrencilerin maksimum seviyede eğitim alabildiği bir üniversiteye dönüşmesi, bu dersi veren öğretim görevlileri gibi çalışanlardan dolayı mümkün olmayacaktır. Son döneminde olan öğrencilere düşük notlar vermek onlarda ters etki yapıp onları ileri götürmeyecektir. Bu dersi alan öğrencilerin %80 inin dersi mecburen aldığını düşünüyorum. Ders kaydında kontenjanı dolu olan yapay zeka derslerini o dersin öğretim görevlisi kabul etse dahi verilmemesi, bu ders gibi derslerin yeterli sayıya zorla getirilmesi için olduğu gözüküyor. [...] dersin öğretim görevlisi yoklama almasına rağmen derse düşük katılım ve kontenjanın yarısının dahi dolmaması farkı gösteriyor. [...] Bu yapıldıktan sonra bir öğretim görevlisi yeterli sayıda öğrenci tarafından seçilmiyorsa dersi açmasına izin verilmemeli ve bunun tekrarında okuldan gönderilmelidir. Bunları yapmadıkça kaliteli bir okul olamayız.

Previous years' remarks

- ✔ Do you have any other comments? [Cont'd]
- ✔ Öncelikleri öğrenci geribildirimlerini önemsediğiniz ve bunları sınıfta öğrencilerle paylaştığınız için teşekkür ederim. İTÜ'deki eğitim hayatım boyunca bunu yapan tek öğretim görevlisi sizdiniz.
  Ders anlatım tarzınız aslında sıkıcı olan bir konuyu sıkıcı olmaktan çıkarıyor. Ders anlatırken öğrenciyle sürekli iletişime geçmeniz çok olumlu. Slaytlar dersi dinlerken yeterli geliyor ancak not alınmazsa aradan zaman geçtikten sonra slaytlara bakarak sınava çalışmanın neredeyse imkansız olduğunu düşünüyorum. Belki zaten bunun böyle olmasını istediniz, bilemiyorum.
  Arkadaşlarım beni İTÜ Bilgisayar bölümündeki çoğu hocayı ağır eleştirmemle bilirler. Bölümdeki bir elin parmağını geçmeyecek nadir hocalardan olduğunuzu düşünüyorum.

Previous years' remarks

- ✔ Do you have any other comments? [Cont'd]
- ✔ [Cont'd] En son finalim olmasına rağmen ilk açıklanan finalim oldu bu ders. Üstelik sınav klasik olmasına rağmen. Gerçekten çok etkileyici, tebrik ediyorum. Ancak aynısını asistan için söyleyemeyeceğim. Bir ödevi okuması aylar aldı, bu hafta açıklıyorum demesine rağmen 2 hafta daha açıklayamadı.
  Quiz ağırlıkları hakkında bir eleştirim olacak. Quiz'lerin ağırlığını bu sene fazla arttırdığınızı düşünüyorum. Sadece dersi dinleyerek yapılacak bir iş değil, araştırma gerekiyor tıpkı bir ödev gibi. Günlerce uğraştığımız bir ödev 1 saatlik quiz ile aynı ağırlığa sahipti, birbirine yakın formatlar olmasına rağmen.
  Emeğiniz için çok teşekkürler. Mezun olurken böyle hocaların olduğunu bilmek İTÜ Bilgisayar'dan umudumu kesmememi sağlayacak.

Previous years' remarks

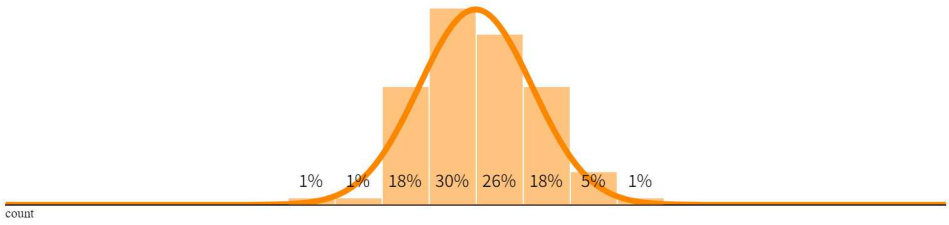
- ✔ Do you have any other comments? [Cont'd]
- ✔ Dersi öğretmek açısından bence çok güzel bir yöntem izliyorsunuz, bilgi ve birikiminizi öğrenciye güzel bir şekilde aktardığınızı düşünüyorum. İngilizceńizin akıcılığı da dilden kaynaklı dersin anlaşılmasında sıkıntı oluşturabilecek olası pürüzleri temizliyor. Pandemi sürecini de başarıyla yönettiğinizi düşünüyorum. Ve ayrıca derslerimizin %90'ının aksine notlarımızı büyük bir hızla okuduğunuz için teşekkür ediyorum. Öğrettiğiniz bütün bilgiler için teşekkür ederim, ezber değil öğrenme yoluna soktuğunuz için teşekkür ederim. Çok güzel ve eğitici bir ders oldu benim için.

Previous years' remarks

- ✔ Do you have any comments on the course?
- ✔ Dersten genel olarak memnun idim. Recitationlar biraz daha uygulama odaklı olsa daha güzel olabilirdi.
- ✔ Benim açımdan tek sorun grup olarak yapılan dönem ödevi idi. Grup çalışması olan ödevi tek başıma yapmak durumunda kaldım.bir arkadaş ödevi yapmayıp dersi bıraktı. Diğeri de yapmasını söylediğim bölümü yarım bir şekilde yaptı. Bence grup üyelerinin ödeve katkısı ayriyrten değerlendirilmeli.
- ✔ Mediocre

A glimpse of CLT

- ✔ Browse to `https://seeing-theory.brown.edu/probability-distributions/index.html`
- ✔ Choose *central limit theorem*
- ✔ Set sample size to the number of questions (7 items or more)
- ✔ Set draw count to the population of the class



Anonymous feedback

- ✔ You might want to send anonymous remarks
- ✔ I provide an anonymous feedback form where you can submit your remarks `https://www.sandikkaya.name.tr/aff.php`
- ✔ Careful! Only alphanumeric input and few punctuation is allowed
- ✔ You need the course password to submit a remark:
- ✔ In case you want me to respond, keep remark ID and check it after a while.

Bibliography 35 / 36

References

[Erickson, 2008] Erickson, J. (2008). *Hacking: The Art of Exploitation*. No Starch Press, 2nd edition.

[Hopkin, 2021] Hopkin, K. (2021). *Your Brain Does Something Amazing between Bouts of Intense Learning*. Accessed on 18.02.2022, `https://www.scientificamerican.com/podcast/episode/your-brain-does-something-amazing-between-bouts-of-intense-learning/`.

[Howard and LeBlanc, 2003] Howard, M. and LeBlanc, D. (2003). *Writing Secure Code*. Microsoft Press, 2nd edition.

[Kerckhoffs, 1883] Kerckhoffs, A. (1883). La cryptographic militaire. *Journal des sciences militaires*, pages 5–38.

[Long et al., 2013] Long, F., Mohindra, D., Seacord, R. C., Sutherland, D. F., and Svoboda, D. (2013). *Java Coding Guidelines: 75 Recommendations for Reliable and Secure Programs*. Pearson Education.

[Seacord, 2013] Seacord, R. C. (2013). *Secure Coding in C and C++*. Pearson Education, 2nd edition. ISBN: 978-0-32182-213-0.

[Wheeler, 2015] Wheeler, D. A. (2015). *Secure programming for Linux and Unix HOWTO*. `http://www.dwheeler.com/secure-programs`.