UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2024-2025

Veilige softwaresystemen (E017950)

Cursusomvang *(nominale waarden; effectieve waarden kunnen verschillen per opleiding)*

Studiepunten 6.0 **Studietijd 180 u**

Aanbodsessies in academiejaar 2024-2025

A (semester 2) Engels Gent

Lesgevers in academiejaar 2024-2025

Coppens, Bart TWO6 Verantwoordelijk lesgever

Aangeboden in onderstaande opleidingen in 2024-2025	stptn	aanbodsessie
Brugprogramma Master of Science in Bioinformatics(afstudeerrichting Engineering)	6	A
Master of Science in Bioinformatics(afstudeerrichting Engineering)	6	A
Master of Science in Computer Science Engineering	6	A
Master of Science in de industriële wetenschappen: informatica	6	A
Master of Science in de informatica	6	A
Master of Science in de ingenieurswetenschappen: computerwetenschappen	6	A
Uitwisselingsprogramma industriële wetenschappen: informatica	6	A
Uitwisselingsprogramma informatica (niveau master)	6	A

Onderwijstalen

Engels

Trefwoorden

kwetsbaarheden, software-aanvallen, exploits, veilige code, code-injectie, remote code-execution, defensieve en offensieve beveiligingstechnieken, beveiligingsbeleid, wettelijke beperkingen, internetbeveiliging, nevenkanalen, beveiligingsanalyse, security by design, veilige softwareontwikkeling

Situering

Softwaresystemen beheersen een groot deel van ons leven en de samenleving in het algemeen, en verwerken een steeds grotere hoeveelheid persoonlijke gegevens en privégegevens. De beveiliging van deze systemen is dus van het grootste belang: een kleine ontwerpfout of implementatiefout in de code van een dergelijk systeem kan leiden tot een verlies van vertrouwelijkheid (bijvoorbeeld het uitlekken van privégegevens), een verlies van integriteit (bijvoorbeeld dat een aanvaller de controle over het systeem kan overnemen) en beschikbaarheid (zodat legitieme gebruikers geen toegang meer hebben tot het systeem). Helaas zit de meeste software vol met dergelijke bugs. Het is dus van het grootste belang om de exploitatie van bugs of gebreken te voorkomen. Daartoe moeten we begrijpen hoe een aanvaller welke bugs kan omzetten in werkende exploits. Dit geeft inzicht in hoe we de gevolgen van dergelijke exploits moeten beperken, en hoe we kunnen voorkomen dat deze bugs kunnen worden uitgebuit. Door de programmeerconstructies die bij de ontwikkeling van software worden gebruikt op de juiste manieren te beperken, kunnen sommige klassen van exploiteerbare bugs zelfs volledig worden geëlimineerd.
In deze cursus zullen we kwetsbaarheden in softwaresystemen exploiteren, beperken en voorkomen. We concentreren ons op (op afstand) exploiteerbare gebreken en bugs in softwareontwerpen en -implementaties waardoor een aanvaller (meer) controle over een systeem kan krijgen (verhoging van rechten/escalation of privilege, uitvoering van code op afstand/remote code execution, ...), of ongeoorloofde toegang tot informatie kan krijgen. We bestuderen de hoofdoorzaken van ontwerpfouten en implementatiebugs, en bestuderen hoe

deze door een aanvaller kunnen worden uitgebuit om de vertrouwelijkheid, integriteit en beschikbaarheid van een systeem te schenden. Hierbij zullen we in het bijzonder aandacht besteden aan fouten die vaak veroorzaakt worden door het gebruik van lagereniveauprogrammeertalen zoals C en C++. Verder bestuderen we hoe we tijdens het testen kwetsbare constructies in code kunnen vinden. We bestuderen en passen methodes toe waarmee we code kunnen maken die inherent minder kwetsbaarheden bevat. We vergelijken verschillende manieren om de impact van aanvallen te beperken (eventueel geholpen door uitbreidingen van het besturingssysteem), waaronder het voorkomen van hele aanvalsklassen.
Deze cursus vormt een aanvulling op de cursus Software Hacking and Protection, die zich richt op man-at-the-end aanvalstechnieken, die worden ingezet door partijen die (bijna) volledige controle hebben over de toestellen waarop ze de software aanvallen en analyseren, zodat ze voor hun aanvallen en analyses niet afhankelijk zijn van exploiteerbare kwetsbaarheden; en de cursus Network Security, die zich richt op aanvallen waarmee netwerkinfrastructuren worden binnengedrongen.
Deze cursus bouwt voort op de kennis die is opgedaan in eerdere cursussen over computerarchitectuur (in het bijzonder over x86 assembly), besturingssystemen en programmeren in low-level programmeertalen (C, C++).

Inhoud

- kwetsbaarheden: classificaties, bugs vs. gebreken, opvolgen van kwetsbaarheden, openbaarmakingsprocessen, ongedefinieerd gedrag
- technieken voor de exploitatie van kwetsbaarheden: aanvallen met controlegegevens, aanvallen zonder controlegegevens, met inbegrip van kwetsbaarheden en exploitatie op basis van hardware (heimelijke kanalen, tijdsgebaseerde nevenkanalen, Spectre, Meltdown, ...)
- exploitatiebeperkingstechnieken (op basis van diversificatie, integriteit, sandboxing, hardware-gebaseerde beperkingstechnieken, ...)
- veilige softwarearchitectuur, -ontwikkeling en -beheer; het principe van de minste privileges
- onveilige en veilige programmeertalen, veilige programmeerpatronen, richtlijnen voor veilige codering
- hulpmiddelen en technieken voor het opsporen van kwetsbaarheden: fuzzingtechnieken, sanitizers, testen, model checking, symbolische en concolische technieken, ...
- technieken voor het handhaven en certificeren van systeemintegriteit
- beveiliging en privacy by design toegepast op software en systemen
- aspecten van de levenscyclus van veilige softwareontwikkeling, maturiteitsmodellen, DevSecOps, Shift Left, ...
- modellering van bedreigingen tegen een systeem, beveiligingseisen
- economische en juridische aspecten van hacking en beveiligingskwesties, bug bounties, ...

Begincompetenties

- Programmeren in C en C++
- Kennis van computerarchitectuur
- Kennis van assembler (x86)
- Kennis van de interne aspecten van besturingssystemen
- Basiskennis van softwareengineeringpraktijken en -paradigma's
- Basiskennis van databanken, programmeren in SQL

Eindcompetenties

1 Inzicht hebben in, en gebruik kunnen maken van de terminologie van de basisaspecten van systeem- en softwarebeveiliging, van risico's, beveiligingseisen, behandeling van beveiligingsproblemen, beleidsopties, wettelijke beperkingen (ethisch hacken, white hat vs. black hat, verantwoord omgaan met, en openbaar maken van gevoelige informatie, ...).
2 Diepgaand begrip van kwetsbaarheden in software, in staat zijn deze te vinden, de impact ervan te analyseren en er exploits voor te construeren.
3 Diep inzicht in preventieve maatregelen en detectiemethoden, in staat zijn gepaste beschermingen te kiezen en toe te passen en te combineren.
4 Het creëren van softwaresystemen die minder kwetsbaarheden bevatten en beter bestand zijn tegen exploits.

5 Kennis van security-by-design softwareontwikkelingsprincipes.
6 Inzicht hebben in aanvallen op basis van systemen die op specifieke hardwareplatforms worden geïmplementeerd (nevenkanaalaanvallen) en in beveiligingen om die aanvallen tegen te gaan.
7 Communiceren en presenteren van domeinspecifieke kennis op een correcte en duidelijke manier, met de juiste taalvaardigheid, inclusief het juiste gebruik van terminologie.

Creditcontractvoorwaarde

Toelating tot dit opleidingsonderdeel via creditcontract is mogelijk mits gunstige beoordeling van de competenties

Examencontractvoorwaarde

Dit opleidingsonderdeel kan niet via examencontract gevolgd worden

Didactische werkvormen

Groepswerk, Hoorcollege, Practicum, Zelfstandig werk

Toelichtingen bij de didactische werkvormen

- In een aantal van de practica gaan we x86-64 software exploiteren. Studenten moeten dus x86-64 virtuele machines kunnen draaien.

Studiemateriaal

Type: Slides

Naam: Slides met lesnota's voorzien door de lesgever
Richtprijs: Gratis of betaald door opleiding
Optioneel: nee
Taal : Engels
Beschikbaar op Ufora : Ja

Type: Andere

Naam: Artikels voor leesopdrachten
Richtprijs: Gratis of betaald door opleiding
Optioneel: nee
Taal : Engels
Beschikbaar op Ufora : Ja

Referenties

- Security Engineering: A Guide To Building Dependable Distributed Systems, Third Edition, by Ross Anderson, 2020. ISBN 978-1-119-64278-7
- Threat Modeling: Designing for Security, by Adam Shostack, 2014. ISBN 978-1-118-80999-0
- The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, by Mark Dowd, John McDonald, and Justin Schuh, 2007. ISBN 978-0-321-44442-4
- Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin, by Paul C. Van Oorschot, 2021. ISBN 978-3-030-83410-4

Vakinhoudelijke studiebegeleiding

- Interactieve begeleiding en coaching via de elektronische leeromgeving
- Lesgevers en assistenten zijn beschikbaar voor en na lessen, en via chat en conf calls voor extra uitleg
- Gebruik van technieken "flipping the classroom" en "blended learning"

Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Schriftelijke evaluatie

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijke evaluatie

Evaluatievormen bij niet-periodegebonden evaluatie

Mondelinge evaluatie, Participatie, Presentatie, Peer en/of self assessment, Schriftelijke evaluatie, Werkstuk

Tweede examenkans in geval van niet-periodegebonden evaluatie

Examen in de tweede examenperiode is enkel mogelijk in gewijzigde vorm

Toelichtingen bij de evaluatievormen

- Periodegebonden evaluatie: schriftelijk examen met open en gesloten vragen over theorie en praktijk (oefeningen), met gesloten boek.
- Niet-periodegebonden evaluatie: beoordeling van practicumwerk (inclusief verslagen en mogelijk evaluatiegesprek), projectwerk, participatie aan activiteiten "flipping the classroom"

Eindscoreberekening

- 50% periode-gebonden evaluatie (PE), 50% niet-periodegebonden evaluatie (NPE)
- Ongewettigde afwezigheid op een niet-periodegebonden evaluatie wordt vertaald in 0 voor dat onderdeel.
- Bij groepswerk krijgen de groepsleden normaalgezien dezelfde punten. Enkel indien er een duidelijk verschil is in hun bijdrage wordt daarvan afgeweken.
- De student moet slagen (>= 10/20) voor zowel de PE als de NPE. Indien de student voor één van de twee faalt maar gemiddeld wel >=10/20 scoort, wordt de finale totaalscore 9/20.

Faciliteiten voor werkstudenten

Mogelijkheid tot vrijstelling van aanwezigheid met vervangende opdracht na overleg met verantwoordelijke lesgever. Mogelijkheid tot mondeling examen met schriftelijke voorbereiding op ander tijdstip binnen het academiejaar. Mogelijkheid tot feedback na afspraak tijdens en na kantooruren.