UNIVERSITEIT GENT

Studiefiche

Vanaf academiejaar 2020-2021

Softwarehacking en -protectie (E017941)

Wegens Covid19 kan mogelijk afgeweken worden van de onderwijs- en evaluatievormen. Dergelijke afwijkingen zullen via Ufora worden gecommuniceerd.

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

Studiepunten 6.0 Studietijd 180 u Contacturen 60.0 u

Aanbodsessies en werkvormen in academiejaar 2020-2021

A (semester 1)	Engels	Gent	zelfstandig werk	2.5 u
			begeleide zelfstudie	2.5 u
			hoorcollege: response college	6.25 u
			hoorcollege	10.0 u
			microteaching	3.75 u
			practicum	23.75 u

Lesgevers in academiejaar 2020-2021

De Sutter, Bjorn	TW06	Verantwoordelijk lesgever
Coppens, Bart	TW06	Medelesgever

Aangeboden in onderstaande opleidingen in 2020-2021	stptn	aanbodsessie
Master of Science in de informatica	6	A
Master of Science in de ingenieurswetenschappen: computerwetenschappen	6	A
Master of Science in Computer Science Engineering	6	A
Uitwisselingsprogramma informatica (niveau master)	6	A

Onderwijstalen

Engels

Trefwoorden

Beveiligingslekken, reverse engineering, software-aanvallen, veilige code, code-injectie, aanvalstechnieken, softwarebeschermingstechnieken, malware, defensieve technieken, offensive technieken, beveilingsbeleid, legale beperkingen

Situering

Voor steeds meer aspecten van ons leven worden we afhankelijk van software die draait op online toestellen. Daarmee neemt het risico om slachtoffer te worden van kwaadaardige activiteiten toe. Het betreft bv. malware en het illegaal kopiëren, veranderen of kraken van software. Om veilige, beschermde software te kunnen ontwikkelen die minder vatbaar is voor aanvallen en minder kwetsbaarheden vertoont, is het belangrijk inzichten te verwerven in bestaande aanvalsvectoren en -methodes, alsook in verdedigingsmechanismen.

Dit opleidingsonderdeel vormt een aanvulling op meer traditionele cursussen over cryptografie, dat bescherming biedt tegen zogenaamde man-in-the-middle aanvallen op communicatiekanalen. In dit opleidingsonderdeel gaat de focus naar technieken voor en tegen man-at-the-end aanvallen, waarbij de software en toestellen aangevallen worden aan beide zijden van de communicatie.

Inhoud

- Algemene introductie over softwarebeveiliging, risico's, omgang met problemen, beveiligingsvereisten
- Reverse-engineering van binaire code, incl. overzicht statische en dynamische technieken, debuggen en disassembleren
- Kwetsbaarheden in software en aanvallen daarop
- Methodes voor het ontwerpen en ontwikkelen van veilige software

- Dynamische aanvallen op software
- Obfuscatie en de-obfuscatie
- Anti-tampering en anti-debugging
- Online softwareprotectietechnieken
- Internetbeveiliging, incl. browser-, server-, en netwerkkwetsbaarheden
- Penetration testing
- Nevenkanalen en foutinjectie: aanvallen en beveiligingen
- Ontwerp van op veilige hardware gebaseerde systemen
- Malware: classificatie, detectie, beschermingen

Begincompetenties

- Programmeren in C
- Basiskennis computerarchitectuur
- Kennis interne werking besturingssystemen
- Kennis paradigma's en praktijken software engineering
- Kennis over databanken, programmeren in SQL
- Basiskennis computernetwerken en Internettechnologie

Eindcompetenties

1. Begrip hebben en terminologie kunnen hanteren van basisaspecten van computer- en softwarebeveiliging, van risico's, van beveiligingsvereisten, van omgang met beveiligingsproblemen, van beleidsmogelijkheden, van legale beperkingen.
2. Man-at-the-end aanvallen kunnen kaderen en uitvoeren (reverse engineering, debuggen, tampering, ...). Het hebben van diepgaand begrip van hulpmiddelen en technieken gebruikt in man-at-the-end software-aanvallen. Het kunnen gebruiken van die middelen en toepassen van de technieken.
3. Diepgaand begrip hebben van softwarekwetsbaarheden, exploits ervan, preventieve tegenmaatregelen, en detectiemethodes. Gebruik kunnen maken van tools en techieken daarvoor. Kennis van security-by-design principes in software-ontwikkeling.
4. Kennis van softwareprotectietechnieken tegen man-at-the-end aanvallen, en inzichten in hun beperkingen en de noodzaak om meerdere technieken te combineren om nuttige bescherming te verkrijgen. Basisvaardigheden in het gebruik van tools en technieken daartoe.
5. Inzicht in online beveiligingsvereisten. Inzicht in de diverse aspecten van penetratietestmethodes en het testen van online beveiligingen. Het kunnen gebruik van populaire tools daarvoor en het toepassen van technieken daarvoor.
6. Begrip van ethisch hacking (white hat vs. black hat) en verantwoord omgaan met en vrijgeven van gevoelige informatie.
7. Begrip van hardwaregebaseerde aanvalsmogelijkheden (nevenkanalen en foutinjectie) en beschermingsmaatregelen daartegen.
8. Inzicht in de verschillende soorten malware en detectiemethodes. Kunnen toepassen van analysetechnieken en -tools.

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

Begeleide zelfstudie, hoorcollege, microteaching, practicum, zelfstandig werk, hoorcollege: response college

Toelichtingen bij de didactische werkvormen

- Online filmpjes en oefeningen (principe van "flipping the classroom")
- Hoorcollege, voor het grootste gedeelde Q/A lessen (response college)
- Labo's/Practica (on campus if COVID-19 allows it)
- De gewone practica worden individueel afgewerkt. Elke samenwerking tussen studenten is daarbij verboden.
- Peer presentaties met begeleide voorbereiding worden in kleine groepjes gemaakt.
- Omwille van COVID19 kunnen gewijzigde werkvormen uitgerold worden indien dit noodzakelijk blijkt

Leermateriaal

- Cursuswebsite
- Online filmpjes
- Online oefeningen
- Opgaven practica
- Beschrijving te kennen terminologie
- Academische publicaties (gratis beschikbaar)
- Nota's en presentaties cursus, gratis ter beschikking gesteld op de elektronische

leeromgeving (Engelstalig)

Referenties

- Surreptitious Software: Obfuscation, Watermarking, and Tamperproofing for Software Protection, by Christian Collberg & Jasvir Nagra, 2009, ISBN-13: 978-0321549259
- Software Security - Building Security In, by Gary McGraw, 2006, ISBN-13: 978-0321356703

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 uit "flipping the classroom" en "blended learning"

Evaluatiemomenten

periodegebonden en niet-periodegebonden evaluatie

Evaluatievormen bij periodegebonden evaluatie in de eerste examenperiode

Schriftelijk examen met open vragen

Evaluatievormen bij periodegebonden evaluatie in de tweede examenperiode

Schriftelijk examen met open vragen

Evaluatievormen bij niet-periodegebonden evaluatie

Mondeling examen, participatie, werkstuk, peer-evaluatie, verslag

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 (verslagen en mogelijk evaluatiegesprek), participatie aan activiteiten "flipping the classroom", evaluatie (met ingebrip van peer assessment) van peer presentaties

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 (peer presentations) krijgen de groepsleden normaal gezien dezelfde punten. Enkel indien er een duidelijk verschil is in hun bijdrage aan de oplossing of het verslag 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.