Leerlijnbeschrijving

Leerlijn Advanced Software Security (15 EC)

V-1.0

Inhoudsopgave

Leerlijn Advanced Software Security

Kenmerken	Code:	ADS
	Studiepunten:	15 EC
	Aantal cursussen:	2
	Aantal bijeenkomsten:	9
	Toetsvorm:	Integrale eindopdracht
Leerlijnbeschrijving	Software is een onmisbare bouwsteen van onze digitale wereld. Van mobiele applicaties tot embedded toepassingen: alles draait op code, maar veel van die code is niet zomaar te lezen. Hoe kun je dan achterhalen wat software precies doet, waar kwetsbaarheden zitten of welke verborgen functionaliteiten aanwezig zijn? In deze leerlijn kijken we naar software vanuit het diepste technisch perspectief. Je leert software te analyseren en te ontleden zonder toegang tot de broncode. Dit is niet alleen belangrijk voor het opsporen van kwetsbaarheden in goedaardige applicaties, maar ook voor het begrijpen en ontmantelen van malware. Waar pentesten zich hoofdzakelijk richt op netwerkanalyse, infrastructuur en webapplicaties, richt deze leerlijn zich volledig op het analyseren van gecompileerde software door middel van reverse engineering. Reverse engineering is een unieke tak van sport binnen de securitywereld, waarbij de nadruk ligt op machine code, binary-analyse en andere methodes om te doorgronden wat er op het laagste niveau van een systeem gebeurt. Debuggers, decompilers en emulatoren worden ingezet om tot de kern van de werking van software te komen, zelfs als dit niet de intentie was van de makers. De leerlijn bestaat uit twee samenhangende cursussen: Reverse Engineering en Mobile & IoT Application Analysis. Deze cursussen komen samen in een integrale eindopdracht waarbij je een mobiele applicatie gaat analyseren en een onbekende malware binary gaat onderzoeken. De opdrachten vereisen technische diepgang, een veilige werkwijze en zorgvuldige documentatie, dus schrijf je ook een onderzoeksplan vooraf.	
Cursussen	1. Reverse Engineering (10 EC) 2. Mobile and IoT Application Analysis (5 EC)	

Cursus 1: Reverse Engineering

Leeruitkomst	De student analyseert op systematische wijze en volgens geldende richtlijnen onbekende software (malware) en brengt de werking ervan in kaart.
Toelichting cursus	Reverse Engineering analyseert en onderzoekt een software object om de interne werking en het ontwerp van het object zichtbaar te maken. De reverse engineer draagt in verschillende vakgebieden bij aan het begrip over en de impact van mogelijk kwaadaardige software en kan verschillende andere cyber security vakgebieden ondersteunen met waardevolle informatie die enkel door technische onderzoek mogelijk zijn.
Prestatie indicatoren	• De student analyseert en reconstrueert de werking, het ontwerp en het gedrag van onbekende softwareobjecten op basis van statische analysemethoden, waaronder low-level code en assembler. • De student zet een veilige analyseomgeving op en verantwoordt de inrichting voor het werken met potentieel gevaarlijke software (malware). • De student zet reverse-engineeringtools, zoals debuggers, decompilers en emulators, effectief in volgens geldende methodieken.
Omvang	10 EC, 6 bijeenkomsten

Cursus 2: Mobile and IoT Application Analysis

Leeruitkomst	De student analyseert mobiele applicaties analyseren op basis van reverse engineeringtechnieken en rapporteert over gevonden kwetsbaarheden en gedragingen.
Toelichting cursus	Mobiele applicaties spelen een steeds grotere rol in ons dagelijks leven. Ze verwerken gevoelige gegevens, communiceren met externe systemen en hebben vaak uitgebreide rechten. In deze cursus leert je hoe mobiele apps (APK-bestanden) gedecompileerd en geanalyseerd worden. Aan de hand van emulatie en reverse engineering wordt het gedrag van de app inzichtelijk gemaakt. Daarbij worden er handvaten gegeven om aan de hand van een haalbaarheidsstudie te bepalen waarom een specifieke app wel of niet geschikt is voor een interessant onderzoek.
Prestatie indicatoren	• De student herkent softwareformaten van mobiele applicaties en zet deze om naar leesbare code. • De student onderbouwt op basis van een haalbaarheidsanalyse waarom een specifieke mobiele applicatie geschikt is voor een uitgebreide analyse. • De student onderzoekt het gedrag van een mobiele applicatie met dynamische analysemethoden. • De student rapporteert diens bevindingen op logische en reproduceerbare wijze in een verslag.
Omvang	5 EC, 3 bijeenkomsten