

Werkplan Masterproef

Naam student: Lennert Franssens

Datum: 22 oktober 2021

Titel: Boosting Multi-Variant Execution through Modern OS Extensions

Bedrijf of onderzoeksgroep

Naam: Computer Systems Lab

Tel: /

Promotors: prof. dr. Bart Coppens, prof. dr. ir. Bjorn De Sutter

mailadressen: Bart.Coppens@UGent.be, Bjorn.DeSutter@UGent.be

Begeleider: dr. ir. Bert Abrath

mailadres: Bert.Abrath@UGent.be

Bestaande situatie en probleemstelling

MVEE's bieden een techniek om veiligheidsproblemen met betrekking tot geheugencorruptie bij software te ontdekken. Ze voeren verschillende varianten (replicae) van eenzelfde programma uit en geven ze dezelfde invoer. Door de verschillende varianten te monitoren op het niveau van de *system calls*, kunnen MVEE's aanvallen een applicatie ontdekken. Als zo'n aanval ontdekt wordt, kan een programma, nog voor er schade toegericht wordt, gestopt worden. Om de *system calls* te kunnen monitoren, worden ze onderschept. Dat gebeurt vanuit een ander proces met een debug-API, wat voor een *overhead* zorgt.

ReMon biedt de optie om een aantal 'ongevaarlijke' *system calls* op een andere manier uit te voeren. De trage omweg wordt vervangen door een aparte component te injecteren in de adresruimte van het te testen programma. Op die manier worden *system calls* veel sneller afgehandeld. Deze specifieke implementatie is niet aanwezig in de reguliere Linux kernel maar moet via een kernelpatch toegevoegd worden, wat veel mensen liever niet doen. Daardoor wordt de ReMon applicatie en zijn snelle implementatie beperkt gebruikt.

Doelstelling van het project

In deze thesis gaan we ReMon aanpassen zodat de functionaliteit van de kernelpatch (en de interactie die de monitor daarmee heeft) wordt vervangen door functionaliteit die gebruik maakt van nieuwe technologieën in de Linux kernel. Het is belangrijk dat na die aanpassingen dezelfde snelheden behaald kunnen worden als de implementatie met de kernelpatch.

Planning en mijlpalen (per week – je mag weken toevoegen):

Week	Type	Beschrijving
27 sep – 3 okt	Planning	Literatuurstudie: <ul style="list-style-type: none"> Secure and Efficient Application Monitoring and Replication (ReMon) – paper Informatie opzoeken over eBPF en seccomp
	Scriptie	
	Deadline	
4 okt – 10 okt	Planning	Literatuurstudie: <ul style="list-style-type: none"> Brede context van MVEE's begrijpen Informatie opzoeken over eBPF en seccomp
	Scriptie	
	Deadline	
11 okt – 17 okt	Planning	Literatuurstudie: <ul style="list-style-type: none"> Brede context van MVEE's begrijpen Gebruik van eBPF in combinatie met seccomp
	Scriptie	
	Deadline	
18 okt – 24 okt	Planning	Literatuurstudie: <ul style="list-style-type: none"> Kernelpatches Hoe kan ik eBPF in deze technologie gebruiken? (seccomp en ptrace) Technologieverkenning: <ul style="list-style-type: none"> ReMon <ul style="list-style-type: none"> Installeren van applicatie Installeren van kernelpatch voor IP-MON <ul style="list-style-type: none"> Kernelpatch begrijpen
	Scriptie	
	Deadline	<ul style="list-style-type: none"> Werkplan indienen
25 okt – 31 okt	Planning	Literatuurstudie: <ul style="list-style-type: none"> Kernelpatches Advanced Techniques for Multi-Variant Execution en verwante literatuur Technologieverkenning: <ul style="list-style-type: none"> ReMon <ul style="list-style-type: none"> Code begrijpen
	Scriptie	
	Deadline	
1 nov – 7 nov	Planning	Literatuurstudie: <ul style="list-style-type: none"> Advanced Techniques for Multi-Variant Execution en verwante literatuur Syscall User Dispatch Technologieverkenning: <ul style="list-style-type: none"> ReMon

		<ul style="list-style-type: none"> ○ Testen van programma ○ Code begrijpen
	Scriptie	<ul style="list-style-type: none"> • Overleaf <ul style="list-style-type: none"> ○ Juiste .latex-bestand (UGent, fea, masterproef) ○ Structuur van scriptie vastleggen ○ Opmaak
	Deadline	
8 nov – 14 nov	Planning	<p>Literatuurstudie:</p> <ul style="list-style-type: none"> • Advanced Techniques for Multi-Variant Execution en verwante literatuur • Syscall User Dispatch • System call monitoring <ul style="list-style-type: none"> ○ Snelheid en verschillende technieken <p>Technologieverkenning:</p> <ul style="list-style-type: none"> • ReMon <ul style="list-style-type: none"> ○ Code begrijpen
	Scriptie	<ul style="list-style-type: none"> • Inleiding schrijven
	Deadline	
15 nov – 21 nov	Planning	<p>Literatuurstudie:</p> <ul style="list-style-type: none"> • Advanced Techniques for Multi-Variant Execution en verwante literatuur • Syscall User Dispatch • System call monitoring <ul style="list-style-type: none"> ○ Security <p>Technologieverkenning:</p> <ul style="list-style-type: none"> • Experimenteren met eBPF: <ul style="list-style-type: none"> ○ Hoe schrijf ik een programma voor eBPF? ○ Hoe voer ik een programma in eBPF uit?
	Scriptie	<ul style="list-style-type: none"> • Doelstelling beschrijven
	Deadline	
22 nov – 28 nov	Planning	<p>Literatuurstudie:</p> <ul style="list-style-type: none"> • Verschil in implementatietechnologieën van eBPF <ul style="list-style-type: none"> ○ Snelheid in ontwikkeling ○ Snelheid in gebruik ○ Veiligheid? <p>Technologieverkenning:</p> <ul style="list-style-type: none"> • Experimenteren met eBPF <ul style="list-style-type: none"> ○ Voorbeelden uitvoeren (seccomp en ptrace)
	Scriptie	<ul style="list-style-type: none"> • Literatuurstudie beschrijven
	Deadline	
29 nov – 5 dec	Planning	<p>Literatuurstudie:</p> <ul style="list-style-type: none"> • Syscall User Dispatch, seccomp, eBPF en ptrace <ul style="list-style-type: none"> ○ Security m.b.t. system calls <p>Technologieverkenning:</p>

		<ul style="list-style-type: none"> • Experimenteren met eBPF <ul style="list-style-type: none"> ◦ System calls uitvoeren in verschillende contexten
	Scriptie	<ul style="list-style-type: none"> • Literatuurstudie beschrijven
	Deadline	
6 dec – 12 dec	Planning	Presentatie: <ul style="list-style-type: none"> • Tussentijdse presentatie maken <ul style="list-style-type: none"> ◦ Inleiding en egingsituatie schetsen.
	Scriptie	<ul style="list-style-type: none"> • Literatuurstudie beschrijven • Technologieverkenning beschrijven
	Deadline	
13 dec – 19 dec	Planning	Presentatie: <ul style="list-style-type: none"> • Tussentijdse presentatie maken <ul style="list-style-type: none"> ◦ Wat heb ik tot nu toe gedaan? Wat ga ik doen in het tweede semester? Hoe zal ik dat aanpakken? Aan welke resultaten kan ik me verwachten na inwerking en literatuurstudie?
	Scriptie	<ul style="list-style-type: none"> • Technologieverkenning beschrijven
	Deadline	
20 dec – 26 dec	Planning	Presentatie: <ul style="list-style-type: none"> • Tussentijdse presentatie inoefenen
	Scriptie	
	Deadline	<ul style="list-style-type: none"> • Scriptie: Literatuurstudie laten nalezen • Tussentijdse presentatie over vorderingen
7 feb – 15 feb	Planning	Ontwerp: <ul style="list-style-type: none"> • Ontwerp van implementatie aanpassen zodat bepaalde system calls, die niet gemonitord moeten worden, door Syscall User Dispatch (eBPF en seccomp) worden afgehandeld.
	Scriptie	
	Deadline	
14 feb – 20 feb	Planning	Ontwerp: <ul style="list-style-type: none"> • Ontwerp van implementatie aanpassen zodat bepaalde system calls, die niet gemonitord moeten worden, door Syscall User Dispatch (eBPF en seccomp) worden afgehandeld.
	Scriptie	
	Deadline	<ul style="list-style-type: none"> • Ontwerp nieuwe implementatie afhebben voor controle.
21 feb – 27 feb	Planning	Ontwerp: <ul style="list-style-type: none"> • Overleg nieuw ontwerp/architectuur van de implementatie met begeleider en promotor.
	Scriptie	
	Deadline	<ul style="list-style-type: none"> • Ontwerp nieuwe implementatie (met Syscall User Dispatch i.p.v. kernel patch) klaar.
28 feb – 6 mrt	Planning	Implementatie: <ul style="list-style-type: none"> • Nieuw ontwerp in bestaande ReMon-applicatie implementeren <ul style="list-style-type: none"> ◦ IP-MON uit het systeem halen

	Scriptie	<ul style="list-style-type: none"> Analyse beschrijven <ul style="list-style-type: none"> Ontwerp van implementatie Motivatatie van keuze
	Deadline	
7 mrt – 13 mrt	Planning	Implementatie: <ul style="list-style-type: none"> Nieuw ontwerp in bestaande ReMon-applicatie implementeren <ul style="list-style-type: none"> De doorgestuurde system calls uit IK-B ophalen in eBPF
	Scriptie	
	Deadline	
14 mrt – 20 mrt	Planning	Implementatie: <ul style="list-style-type: none"> Nieuw ontwerp in bestaande ReMon-applicatie implementeren <ul style="list-style-type: none"> Met Syscall User Dispatch (eBPF en seccomp) de doorgestuurde system calls uit IK-B afhandelen
	Scriptie	
	Deadline	
21 mrt – 27 mrt	Planning	Implementatie: <ul style="list-style-type: none"> Nieuw ontwerp in bestaande ReMon-applicatie implementeren <ul style="list-style-type: none"> Met Syscall User Dispatch (eBPF en seccomp) de doorgestuurde system calls uit IK-B afhandelen Andere stukken van de ReMon-applicatie op nieuwe manier implementeren (eBPF) voor meer snelheidswinst
	Scriptie	
	Deadline	
28 mrt – 3 apr	Planning	Implementatie: <ul style="list-style-type: none"> Controlleren of nieuwe implementatie werkt zoals het hoort <ul style="list-style-type: none"> Implementatie bijsturen Bugs uit code halen Andere stukken van de ReMon-applicatie op nieuwe manier implementeren (eBPF) voor meer snelheidswinst Presentatie: <ul style="list-style-type: none"> (Tussentijdse) presentatie maken <ul style="list-style-type: none"> Waarover vertel ik? Inleiding. Beginsituatie schetsen.
	Scriptie	
	Deadline	<ul style="list-style-type: none"> Scriptie: Laten nalezen van ±25 pag. Invullen gegevens op Plato
4 apr – 10 apr	Planning	Implementatie: <ul style="list-style-type: none"> Afronden concrete implementatie (in grote lijnen) Presentatie: <ul style="list-style-type: none"> (Tussentijdse) presentatie maken <ul style="list-style-type: none"> Mijn oplossing uitleggen.
	Scriptie	<ul style="list-style-type: none"> Uitschrijven van concrete implementatie (corpus)
	Deadline	<ul style="list-style-type: none"> Werkend prototype
11 apr – 17 apr	Planning	Praktisch: <ul style="list-style-type: none"> Benchmarks schrijven <ul style="list-style-type: none"> Voor randgevallen

		<ul style="list-style-type: none"> ○ Om overhead goed te kunnen meten Presentatie: <ul style="list-style-type: none"> • (Tussentijdse) presentatie maken <ul style="list-style-type: none"> ○ Is mijn oplossing goed? Reflectie en resultaten bespreken.
	Scriptie	<ul style="list-style-type: none"> • Kort abstract schrijven (5-10 lijnen in html voor Plato) • Extended abstract schrijven
	Deadline	<ul style="list-style-type: none"> • Tussentijdse presentatie voor onderzoeksgroep
18 apr – 24 apr	Planning	Praktisch: <ul style="list-style-type: none"> • Benchmarking op kleine (bestaande) programma's <ul style="list-style-type: none"> ○ Om bugs op te sporen ○ Om snelheidsmetingen (overheadsmetingen) te doen
	Scriptie	<ul style="list-style-type: none"> • Inventaris van alle software en technologie beschrijven • Duurzaamheidsreflectie (sdgs en global goals) – reflectie
	Deadline	
25 apr – 1 mei	Planning	Praktisch: <ul style="list-style-type: none"> • Benchmarking op grote (bestaande) programma's <ul style="list-style-type: none"> ○ Om bugs op te sporen ○ Om snelheidsmetingen (overheadsmetingen) te doen
	Scriptie	<ul style="list-style-type: none"> • Beschrijven van resultaten (benchmarking) • Nieuwe bronnen toevoegen
	Deadline	
2 mei – 8 mei	Planning	Praktisch: <ul style="list-style-type: none"> • Benchmarking van grote (bestaande) programma's <ul style="list-style-type: none"> ○ Met nieuwe implementatie ○ Met oude implementatie ○ Met gewone MVEE
	Scriptie	<ul style="list-style-type: none"> • Beschrijven van resultaten (benchmarking) • Moeilijkheden beschrijven
	Deadline	Klaar met alle benchmarks om resultaten uit te kunnen schrijven in scriptie
9 mei – 15 mei	Planning	
	Scriptie	<ul style="list-style-type: none"> • Beschrijven van vergelijkende resultaten (benchmarking) • Uitschrijven van alle tests die gebruikt werden om oplossing te evalueren • Eigen beoordeling van het geleverde werk – reflectie
	Deadline	
16 mei – 22 mei	Planning	
	Scriptie	<ul style="list-style-type: none"> • Besluit uitschrijven • Woord vooraf uitschrijven • Nalezen
	Deadline	
23 mei – 29 mei	Planning	
	Scriptie	<ul style="list-style-type: none"> • Nalezen
	Deadline	Scriptie: 1 ^e versie laten nalezen
	Planning	

30 mei – 5 jun	Scriptie	<ul style="list-style-type: none"> • Laatste correcties in scriptie
	Deadline	<ul style="list-style-type: none"> • Afgewerkte implementatie doorgeven aan promotors en begeleider
6 jun – 12 jun	Planning	
	Scriptie	<ul style="list-style-type: none"> • Laatste correcties in scriptie
	Deadline	Scriptie: Indienen op Plato
	Planning	Presentatie: <ul style="list-style-type: none"> • Presentatie afwerken <ul style="list-style-type: none"> ○ Feedback tussentijdse presentatie gebruiken om openbare verdediging op punt te zetten.
13 jun – 19 jun	Scriptie	
	Deadline	
	Planning	Presentatie: <ul style="list-style-type: none"> • Presentatie afwerken <ul style="list-style-type: none"> ○ Controle: juiste grafieken en grammaticale fouten verbeteren
	Scriptie	
20 jun – 26 jun	Deadline	
	Planning	Presentatie: <ul style="list-style-type: none"> • Inoefenen • Voorbereiden door alles nogmaals grondig door te nemen
	Scriptie	
	Deadline	<ul style="list-style-type: none"> • Logboek/e-mailrapportering indienen op Plato • Presentatie indienen op Plato • Openbare verdediging
27 jun – 3 jul		