Analyzing and securing binaries through static disassembly

Andriesse, D.A.

2017

document version
Publisher's PDF, also known as Version of record

Samenvatting

Disassembly is het identificeren van machinecode in binaire programma's, en het vertalen hiervan in een vorm die geschikt is voor analyse door mensen, of verdere verwerking door een computer. Het is een cruciale stap in vrijwel alle vormen van binaire analyse, waaronder malware-analyse en beveiligingstechnieken voor binaire programma's. Het belang van beveiliging voor bestaande binaire programma's groeit naarmate nieuwe exploitatietechnieken voor onbeschermde programma's worden ontwikkeld. Het is vaak geen optie om een programma opnieuw te compileren, omdat de broncode (of zelfs symbolische informatie) in veel gevallen niet meer beschikbaar is; in zulke gevallen is er dus geen andere keus dan het direct toepassen van binaire beveiligingstechnieken. Helaas is disassembly een onbeslisbaar probleem, waardoor ieder systeem dat niet-triviale binaire programma's verwerkt met zekerheid te maken krijgt met incomplete of foutieve disassembly.

In dit proefschrift onderzoeken we methodes voor het veilig implementeren van binaire beveiligingstechnieken met imperfecte disassembly als basis. We ontwikkelen nieuwe verdedigingsmechanismes tegen meerdere geavanceerde aanvallen, waaronder aanvallen op de stack, zogenaamde "control-flow hijacking" aanvallen, en aanvallen waarbij de integriteit van het programma zelf bedreigd wordt. Onze verdedigingsmechanismes implementeren een aantal strategieën die het mogelijk maken een gebalanceerde afweging te maken tussen het gewenste beveiligingsniveau, de resulterende vertraging van het programma, en de mate van waarschijnlijkheid van crashes door disassemblyfouten.

Daarnaast bevat dit proefschrift een gedetailleerd onderzoek naar het disassemblyproces zelf op het x86/x86-64-platform, waarbij aandacht wordt besteed aan de meest foutgevoelige gevallen, en waarbij we afwijkingen constateren tussen de betrouwbaarheid van disassembly in de praktijk, en de verwachtingen betreffende deze betrouwbaarheid in de wetenschappelijke literatuur. Hiermee ontwikkelen we een stabielere basis voor toekomstig onderzoek, door te verduidelijken welke problemen het meest waarschijnlijk zijn, en dus speciale aandacht behoeven. Gebaseerd op onze analyse implementeren we ook een verbeterde methode voor functiedetectie, hetgeen op het moment van schrijven de meest onbetrouwbare component van het disassemblyproces is.