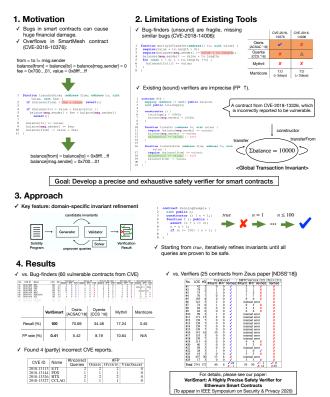
소프트웨어 분석 연구실

http://prl.korea.ac.kr 지도교수 오학주

* 연구 분야: 소프트웨어 분석 및 보안 / 소프트웨어 취약점 자동 검출

* 최근 연구 주제

소프트웨어 보안 취약점 자동 검출



AI 기반 고성능 소프트웨어 분석 기술

• Selective application of high precision (and soundness):







cheap but imprecise

precise but expensive

cheap and precise

Data-driven, automatic generation of selection heuristics:

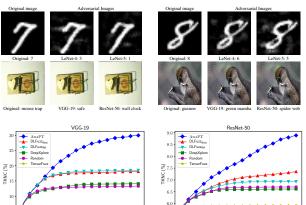


Heuristics for deciding when to apply high precision

소프트웨어 취약점 자동 패치

Error Report of Facebook Infer	Results of Existing Fixing Tools	Our Goals
Image is a second of the second of	Execution of Existing Fixing Fixing Fools LeadKir.(UCSF15) * for (mode = forceds = forder.) * forceds = forceds = forceds = forceds.) * forceds = forceds = forceds.) * forceds = forceds = forceds.) * forceds = forceds = forceds = forceds.) * forceds = forceds = forceds = forceds.) * forceds = forceds = forceds = forceds = forceds.)	Developing a practical technique for fixing memory-leak by achieving: Repairability - Conditional deallocation e.g., insult flips (Treegep) - Safety - No new errors introduced e.g., double-free and use-after fre - Scalability - Working on real-reporting - generation and the safety free - generation and
i3) "Object allocated at line 9 is unreachable at line	Failed to generate a fix (unscalable)	12 il[append_data(), dptr) == -1) free(dptr); 13 }
. Key Idea		
p = walkci): //n Imp if (0) Imp i = q = n; Imp	Labeling Operators Labeling Operators () survey (***) () survey (***)	Program Siling φt=ss Selective Path-Sensitivity μ = molect_1, μ μ = molect_1, μ φ(T) μ = 1, μ width y = molect_1, μ φ(T) μ = 1, μ width y = to φ(T) μ = 1, μ width y = to φ(T) μ = 1, μ width y = to φ(T) μ = 1, μ width y = to φ(T) μ = 1, μ width y = to
Phase 1: Constructing C	biect-flow Graph	Phase 2: Patch Generation
Program Program Slicer Program Access Analysis Access Analysis	Program Program Program Path-Merging Heuristics	Graph Re-Labeling
. Results		

AI 소프트웨어 취약점 자동 검출



3600

1800 2400 3000 time (s) 360

1200

1800 2400 3000 time (s)

1200

* 연구 성과: IEEE S&P, PLDI, ICSE 등 SW 보안 및 분석 분야 최우수 학술대회 >15편 (최근5년)