Id	Est. Difficulty	Feature Name	Est. Time
1	**Simple**	**AddressTaken Analysis**	**½ – 1 Week**
2	Simple	Collection of addresses in program memory	Done
3	Medium	Analysis of the runtime linker (libld)	
4	**Medium**	**CallTarget Analysis (I)**	**2 Weeks**
5	Simple	Collection of CallTargets	Done
6	Medium	Identification of the expected parameter count	
7	Medium	Pathwise forward function CFG liveness analysis	
8	Simple	Merging of Paths	
9	**Medium**	**Relative CallSite Analysis (I)**	**2 Weeks**
10	Simple	Collection of relative CallSites	Done
11	Medium	Identification of the provided parameter count	
12	Medium	Pathwise backward function CFG liveness analysis	
13	Simple	Merging of Paths	
14	**Medium**	**Binary Patching**	**½ – 1 Week**
15	Medium	CallTarget tags	
16	Simple	Tag-based CallSite vs CallTarget checks (generic!)	
17	Simple	Scrambling unused register values (methodology!)	
18	**Simple**	**Verification: Dynainst vs Ground Truth (llvm)**	**1 Day**
19	Simple	Parameter count	
20	**Medium**	**CallTarget Analysis (II)**	**2 Weeks**
21	Medium	Identification of the provided return type	
22	Medium	type ::= provides | does not provide	
23	**Medium**	**CallSite Analysis (II)**	**2 Weeks**
24	Medium	Identification of the expected return type	
25	Medium	type ::= expects | does not expect	
26	**Simple**	**Verification: Dyninst vs Ground Truth (llvm)**	**1 Day**
27	Simple	Return type (void | non-void)	
28	**High**	**CallTarget Analysis (III)**	**4 Weeks**
29	High	Identification of the expected parameter types	
30	Medium	Dyninst-based analysis	
31	High	BAP-based analysis	
32	**High**	**Relative CallSite Analysis (III)**	**4 Weeks**
33	High	Identification of the provided parameter types	
34	Medium	Dyninst-based analysis	
35	High	BAP-based analysis	
36	**Simple**	**Verification: Dyninst vs BAP vs Ground Truth (llvm)**	**1 Day – 2 Days**
37	Simple	Parameter Type (int, float, pointer, …)	
38	Simple	Return Type (void, int, float, pointer, …)	
39	**Medium**	**AddressTaken Analysis (II)**	**1 – 2 Weeks**
40	Medium	Vtable Identification	
41	**Medium**	**CallTarget Analysis (IV)**	**1 – 2 Weeks**
42	Medium	Identification of VcallTargets	
43	**Medium**	**Relative CallSite Analysis (IV)**	**1 – 2 Weeks**
44	Medium	Identification of VcallSites	
45	Medium	Pattern-matching based approach	
46	**Simple**	**Verification: Implementatin vs Ground Truth (llvm)**	**1 Day**
47	Simple	Vtable Identification	