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, …)	Done Paul
38	Simple	Return Type (void, int, float, pointer, …)	see comment in .ods file
39	TODO	**SmartDec (implement the same fixed point algorithm see SmartDec Paper)**	TODO
40		see git repo folder MA_Binary_Variable Type_Reconstrction	see comment in .ods file
41	TODO	**IDA Pro (as above)**	TODO
42		see git repo folder MA_Binary_Variable Type_Reconstrction and IDA API	see comment in .ods file
43	TODO	**angr tool (as above, everything in place but has this feature not)**	TODO
44		see git repo folder MA_Binary_Variable Type_Reconstrction and angr API	see comment in .ods file
45	TODO	**PIN (I do not know)**	TODO
46		see git repo folder MA_Binary_Variable Type_Reconstrction and PIN API	see comment in .ods file
47	TODO	**Other candiate TOOL and/or Algorithms, Please add**	TODO
48		add commnet	see comment in .ods file
49	**Medium**	**AddressTaken Analysis (II)**	**1 – 2 Weeks**
50	Medium	Vtable Identification	
51	**Medium**	**CallTarget Analysis (IV)**	**1 – 2 Weeks**
52	Medium	Identification of VcallTargets	
53	**Medium**	**Relative CallSite Analysis (IV)**	**1 – 2 Weeks**
54	Medium	Identification of VcallSites	
55	Medium	Pattern-matching based approach	
56	**Simple**	**Verification: Implementatin vs Ground Truth (llvm)**	**1 Day**
57	Simple	Vtable Identification, We will get also the code from Victor	
58		in June, I just have to send an email to him again,	
59		or we ask victor which exact versions of the servers he used (ID and date,	
60		and we use the same ones)	