

Reverse Engineering 101

Dozent: Prof. Dr. Michael Eichberg

Kontakt: michael.eichberg@dhw-mannheim.de

Version: 2024-03-26



Folien: <https://delors.github.io/sec-reversing101/folien.rst.html>

<https://delors.github.io/sec-reversing101/folien.rst.html.pdf>

Fehler auf Folien melden:

<https://github.com/Delors/delors.github.io/issues>

Vorerfahrungen?

- Wer hat schon einmal Software or Hardware Reverse Engineering betrieben?
- Wer kennt Java Bytecode?
- Wer hat Erfahrung mit Python?

Reverse Engineering

Reverse Engineering ist die Analyse von Systemen mit dem Ziel, ihren Aufbau und ihre Funktionsweise zu verstehen.

Typische Anwendungsfälle:

- die Rekonstruktion (von Teilen) des Quellcodes von Programmen, die nur als Binärabbild vorliegen.
- die Analyse von Kommunikationsprotokollen proprietärer Software

Vom Reverse Engineering ist das **Reengineering** zu unterscheiden. Im Fall von letzteren geht es „nur“ darum die Funktionalität eines bestehenden Systems mit neuen Techniken wiederherzustellen.

Zweck von Reverse Engineering

- Herstellung von Interoperabilität
- Untersuchung auf Schwachstellen
- Untersuchung auf Copyrightverletzungen
- Untersuchung auf Backdoors
- Analyse von Viren, Würmern etc.
- Umgehung von ungerechtfertigten(?) Schutzmaßnahmen (z.B. bei Malware)

Reverse Engineering - grundlegende Schritte

1. Informationsgewinnung zur Gewinnung aller relevanten Informationen über das Produkt
2. Modellierung mit dem Ziel der (Wieder-)Gewinnung eines (abstrakten) Modells der relevanten Funktionalität.
3. Überprüfung (审查 *review*) des Modells auf seine Richtigkeit und Vollständigkeit.

Informationsgewinnung - Beispiel

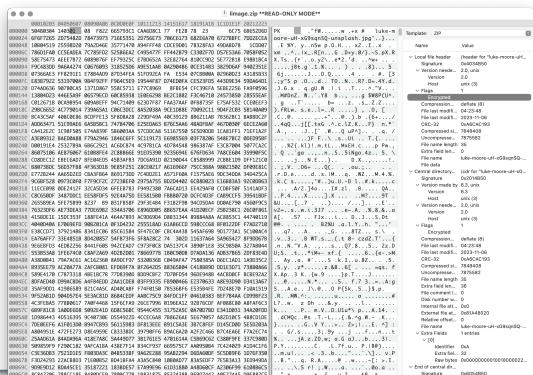
Gegeben sei eine App zum Ver- und Entschlüsseln von Dateien sowie ein paar verschlüsselte Dateien. Mögliche erste Schritte vor der Analyse von Binärcode:

- Die ausführbare Datei ggf. mit `file` überprüfen (z.B. wie kompiliert und für welches Betriebssystem und Architektur)

Beispiel:

```
$ file /usr/bin/openssl  
/usr/bin/openssl: Mach-O universal binary with 2 archi...  
/usr/bin/openssl (for architecture x86_64): Mach-O 64-bit  
/usr/bin/openssl (for architecture arm64e): Mach-O 64-bit
```

- Die Dateien mit einem (guten) Hexeditor auf Auffälligkeiten untersuchen.



Die Datei auf bekannte Viren und Malware überprüfen.

- Eine Datei mit einem bekannten Inhalt verschlüsseln und danach vergleichen.

Ist die Datei gleich groß?

Falls ja, dann werden keine Metainformationen gespeichert und das Passwort kann (ggf.) nicht (leicht) verifiziert werden.

- Eine Datei mit verschiedenen Passworten verschlüsseln.

Sind die Dateien gleich?

Falls ja, dann wäre die Verschlüsselung komplett nutzlos und es gilt nur noch den konstanten Schlüssel zu finden.

Gibt es Gemeinsamkeiten?

Falls ja, dann wäre es möglich, dass das Passwort (gehasht) in der Datei gespeichert wird.

5

- Eine Datei mit einem wohldefinierten Muster verschlüsseln, um ggf. den "Mode of Operation" (insbesondere ECB) zu identifizieren.

6

- Mehrere verschiedene Dateien mit dem gleichen Passwort verschlüsseln

Gibt es Gemeinsamkeiten?

Falls ja, dann wäre es möglich, dass die entsprechenden Teile direkt vom Passwort abgeleitet werden/damit verschlüsselt werden.

7

- ...

8

6

Rechtliche Aspekte des Reverse Engineering

- **unterschiedliche nationale Gesetzgebung**
- Rechtslage in Deutschland hat sich mehrfach geändert
- Umgehung von Kopierschutzmechanismen ist im Allgemeinen verboten
- Lizenz verbietet das Reverse Engineering häufig

Warnung

Bevor Sie Reverse Engineering von Systemen betreiben, erkundigen sie sich erst über mögliche rechtliche Konsequenzen.

1. SOFTWARE REVERSE ENGINEERING

Prof. Dr. Michael Eichberg

Ansätze

statische Analyse: Studieren des Programms ohne es auszuführen; typischerweise mittels eines Disassemblers oder eines Decompilers.

dynamische Analyse:

Ausführen des Programms; typischerweise unter Verwendung eines Debuggers oder eines instrumentations Frameworks (z.B. [Frida](#)).

hybride Analyse: Kombination aus statischer und dynamischer Analyse.

Ansätze wie [Unicorn](#), welches auf [QEmu](#) aufbaut, erlaubt zum Beispiel die Ausführung von (Teilen von) Binärcode auf einer anderen Architektur als der des Hosts.

Ein Beispiel wäre die Ausführung einer Methode, die im Code verschlüsselte hinterlegte Strings entschlüsselt ( *deobfuscation*), um die Analyse zu vereinfachen.

Disassembler

Überführt (maschinenlesbaren) Binärkode in Assemblercode

Beispiel:

- objdump -d
- gdb
- radare
- javap (für Java)

Hinweis

Für einfache Programme ist es häufig möglich direkt den gesamten Assemblercode mittels der entsprechenden Werkzeuge zu erhalten. Im Falle komplexer Binärdateien (z.B. im ELF (Linux) und PE (Windows) Format) gilt dies nicht und erfordert ggf. manuelle Unterstützung zum Beispiel durch das Markieren von Methodenanfängen.

Im Fall von Java `.class` ist die Disassembly immer möglich.

Decompiler

Überführt (maschinenlesbarem) Binärkode bestmöglich in Hochsprache (meist C oder Java). Eine *kleine* Auswahl von verfügbaren Werkzeugen:

- Hex-Rays IDAPro (kommerziell)
- **Ghidra** (unterstützt fast jede Platform; die Ergebnisse sind sehr unterschiedlich)
- JadX (Androids .dex Format)
- CFR (Java .class Dateien)
- IntelliJ
- decompiler.com

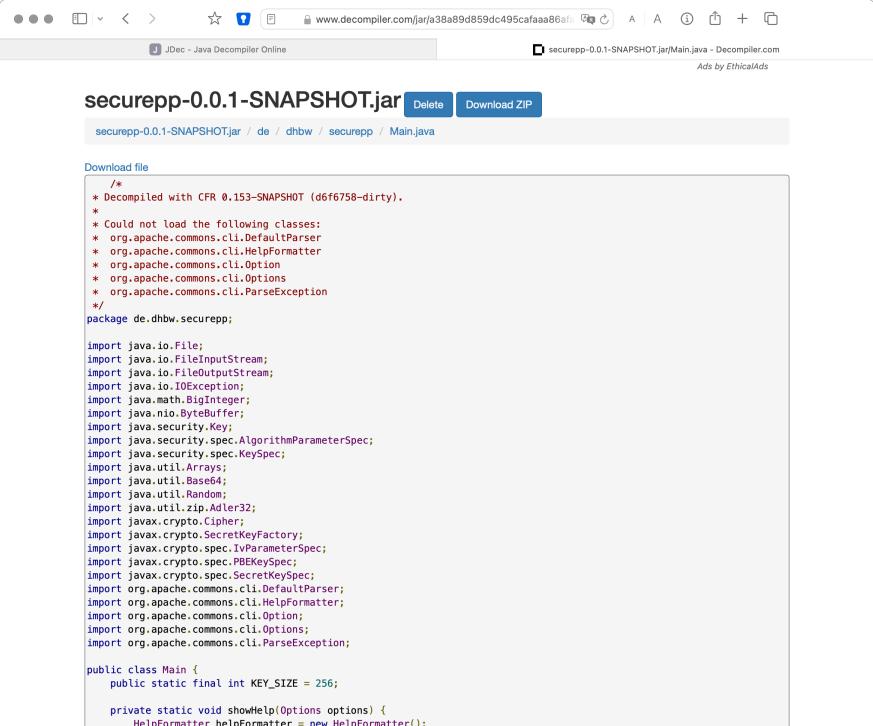
Hinweis

Generell sehr hilfreich, aber gleichzeitig auch sehr fehlerbehaftet. Vieles, dass im Binärkode möglich ist, hat auf Sourcecode Ebene keine Entsprechung. Zum Beispiel unterstützt Java Bytecode beliebige Sprünge. Solche, die

Mittels Decompiler ist es ggf. möglich Code, der zum Beispiel ursprünglich in Kotlin oder Scala geschrieben und für die JVM kompiliert wurde, als Java Code zurückzubekommen.

Die Ergebnisse sind für Analysezwecke zwar häufig ausreichend gut - von funktionierendem Code jedoch ggf. ((sehr) weit) entfernt.

cfr Decompiler



The screenshot shows a web-based Java decompiler interface. At the top, it displays the URL www.decompiler.com/jar/a38a89d859dc495cafaaa86af. Below the URL, the page title is "securepp-0.0.1-SNAPSHOT.jar>Main.java - Decompiler.com". A small note "Ads by EthicalAdz" is visible. There are buttons for "Delete" and "Download ZIP". The main content area shows the decompiled Java code for the Main class:

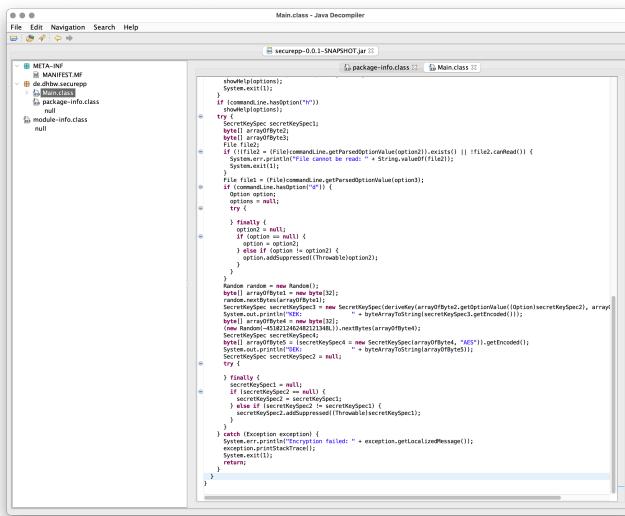
```
/*
 * Decompiled with CFR 0.153-SNAPSHOT (d6f6758-dirty).
 *
 * Could not load the following classes:
 * org.apache.commons.cli.DefaultParser
 * org.apache.commons.cli.HelpFormatter
 * org.apache.commons.cli.Option
 * org.apache.commons.cli.Options
 * org.apache.commons.cli.ParseException
 */
package de.dhbw.securepp;

import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import java.io.OutputStream;
import java.nio.ByteBuffer;
import java.security.Key;
import java.security.spec.AlgorithmParameterSpec;
import java.security.spec.KeySpec;
import java.util.Arrays;
import java.util.Base64;
import java.util.Random;
import java.util.zip.Adler32;
import javax.crypto.Cipher;
import javax.crypto.SecretKeyFactory;
import javax.crypto.spec.IvParameterSpec;
import javax.crypto.spec.PBEKeySpec;
import javax.crypto.spec.SecretKeySpec;
import org.apache.commons.cli.DefaultParser;
import org.apache.commons.cli.HelpFormatter;
import org.apache.commons.cli.Option;
import org.apache.commons.cli.Options;
import org.apache.commons.cli.ParseException;

public class Main {
    public static final int KEY_SIZE = 256;

    private static void showHelp(Options options) {
        HelpFormatter helpFormatter = new HelpFormatter();
    }
}
```

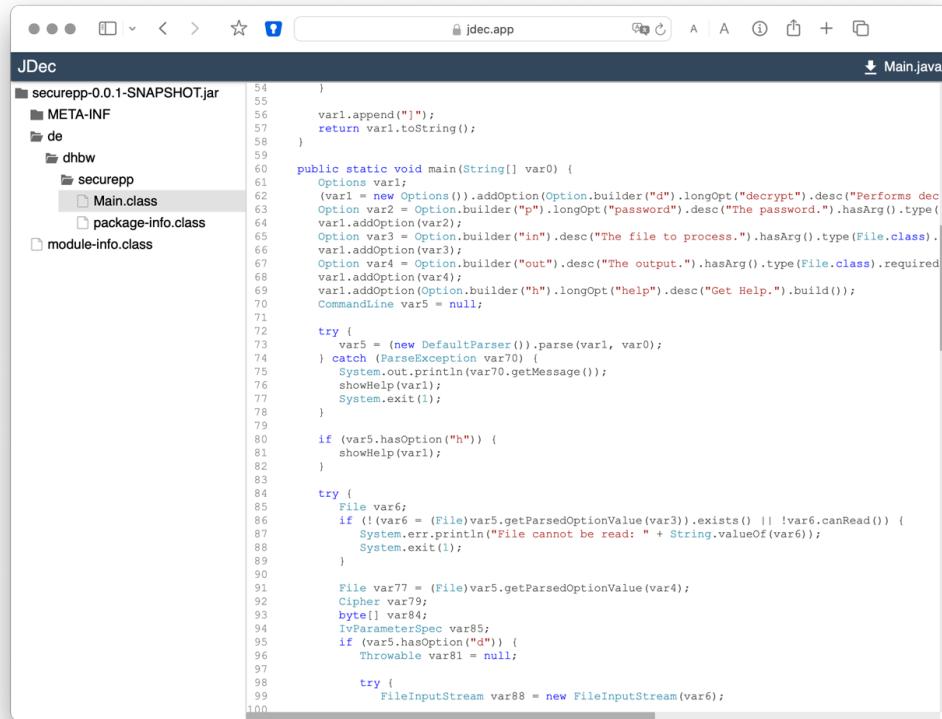
JD Decompiler



```
SecretKeySpec secretKeySpec2 = null;
try {
} finally {
    secretKeySpec1 = null;
    if (secretKeySpec2 == null) {
        secretKeySpec2 = secretKeySpec1;
    } else if (secretKeySpec2 != secretKeySpec1) {
        secretKeySpec2.addSuppressed((Throwable)secretKeySpec1);
    }
}
```

Beispiel fehlgeschlagener Dekompilierung

JDec Decompiler



The screenshot shows the JDec Decompiler interface. On the left, there's a file tree for a JAR file named "securepp-0.0.1-SNAPSHOT.jar". The tree includes the META-INF directory, a de directory, and a dhbw directory containing sub-directories like securepp, Main.class, package-info.class, and module-info.class. The Main.java file is currently selected and shown in the main decompiler window on the right. The code is as follows:

```
54     }
55     var1.append("]");
56     return var1.toString();
57 }
58
59
60 public static void main(String[] var0) {
61     Options var1;
62     (var1 = new Options()).addOption(Option.builder("d").longOpt("decrypt").desc("Performs dec
63     Option var2 = Option.builder("p").longOpt("password").desc("The password.").hasArg().type(
64     var1.addOption(var2);
65     Option var3 = Option.builder("in").desc("The file to process.").hasArg().type(File.class).
66     var1.addOption(var3);
67     Option var4 = Option.builder("out").desc("The output.").hasArg().type(File.class).required
68     var1.addOption(var4);
69     var1.addOption(Option.builder("h").longOpt("help").desc("Get Help.").build());
70     CommandLine var5 = null;
71
72     try {
73         var5 = (new DefaultParser()).parse(var1, var0);
74     } catch (ParseException var70) {
75         System.out.println(var70.getMessage());
76         showHelp(var1);
77         System.exit(1);
78     }
79
80     if (var5.hasOption("h")) {
81         showHelp(var1);
82     }
83
84     try {
85         File var6;
86         if (!var6 = (File)var5.getParsedOptionValue(var3)).exists() || !var6.canRead()) {
87             System.err.println("File cannot be read: " + String.valueOf(var6));
88             System.exit(1);
89     }
89
90
91     File var77 = (File)var5.getParsedOptionValue(var4);
92     Cipher var79;
93     byte[] var84;
94     IvParameterSpec var85;
95     if (var5.hasOption("d")) {
96         Throwable var81 = null;
97
98         try {
99             FileInputStream var88 = new FileInputStream(var6);
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
159
160
161
162
163
164
165
166
167
168
169
169
170
171
172
173
174
175
176
177
178
179
179
180
181
182
183
184
185
186
187
188
189
189
190
191
192
193
194
195
196
197
198
199
199
200
200
201
202
203
204
205
206
207
208
209
209
210
211
212
213
214
215
216
217
217
218
219
219
220
221
222
223
224
225
225
226
227
227
228
228
229
229
230
230
231
231
232
232
233
233
234
234
235
235
236
236
237
237
238
238
239
239
240
240
241
241
242
242
243
243
244
244
245
245
246
246
247
247
248
248
249
249
250
250
251
251
252
252
253
253
254
254
255
255
256
256
257
257
258
258
259
259
260
260
261
261
262
262
263
263
264
264
265
265
266
266
267
267
268
268
269
269
270
270
271
271
272
272
273
273
274
274
275
275
276
276
277
277
278
278
279
279
280
280
281
281
282
282
283
283
284
284
285
285
286
286
287
287
288
288
289
289
290
290
291
291
292
292
293
293
294
294
295
295
296
296
297
297
298
298
299
299
300
300
301
301
302
302
303
303
304
304
305
305
306
306
307
307
308
308
309
309
310
310
311
311
312
312
313
313
314
314
315
315
316
316
317
317
318
318
319
319
320
320
321
321
322
322
323
323
324
324
325
325
326
326
327
327
328
328
329
329
330
330
331
331
332
332
333
333
334
334
335
335
336
336
337
337
338
338
339
339
340
340
341
341
342
342
343
343
344
344
345
345
346
346
347
347
348
348
349
349
350
350
351
351
352
352
353
353
354
354
355
355
356
356
357
357
358
358
359
359
360
360
361
361
362
362
363
363
364
364
365
365
366
366
367
367
368
368
369
369
370
370
371
371
372
372
373
373
374
374
375
375
376
376
377
377
378
378
379
379
380
380
381
381
382
382
383
383
384
384
385
385
386
386
387
387
388
388
389
389
390
390
391
391
392
392
393
393
394
394
395
395
396
396
397
397
398
398
399
399
400
400
401
401
402
402
403
403
404
404
405
405
406
406
407
407
408
408
409
409
410
410
411
411
412
412
413
413
414
414
415
415
416
416
417
417
418
418
419
419
420
420
421
421
422
422
423
423
424
424
425
425
426
426
427
427
428
428
429
429
430
430
431
431
432
432
433
433
434
434
435
435
436
436
437
437
438
438
439
439
440
440
441
441
442
442
443
443
444
444
445
445
446
446
447
447
448
448
449
449
450
450
451
451
452
452
453
453
454
454
455
455
456
456
457
457
458
458
459
459
460
460
461
461
462
462
463
463
464
464
465
465
466
466
467
467
468
468
469
469
470
470
471
471
472
472
473
473
474
474
475
475
476
476
477
477
478
478
479
479
480
480
481
481
482
482
483
483
484
484
485
485
486
486
487
487
488
488
489
489
490
490
491
491
492
492
493
493
494
494
495
495
496
496
497
497
498
498
499
499
500
500
501
501
502
502
503
503
504
504
505
505
506
506
507
507
508
508
509
509
510
510
511
511
512
512
513
513
514
514
515
515
516
516
517
517
518
518
519
519
520
520
521
521
522
522
523
523
524
524
525
525
526
526
527
527
528
528
529
529
530
530
531
531
532
532
533
533
534
534
535
535
536
536
537
537
538
538
539
539
540
540
541
541
542
542
543
543
544
544
545
545
546
546
547
547
548
548
549
549
550
550
551
551
552
552
553
553
554
554
555
555
556
556
557
557
558
558
559
559
560
560
561
561
562
562
563
563
564
564
565
565
566
566
567
567
568
568
569
569
570
570
571
571
572
572
573
573
574
574
575
575
576
576
577
577
578
578
579
579
580
580
581
581
582
582
583
583
584
584
585
585
586
586
587
587
588
588
589
589
590
590
591
591
592
592
593
593
594
594
595
595
596
596
597
597
598
598
599
599
600
600
601
601
602
602
603
603
604
604
605
605
606
606
607
607
608
608
609
609
610
610
611
611
612
612
613
613
614
614
615
615
616
616
617
617
618
618
619
619
620
620
621
621
622
622
623
623
624
624
625
625
626
626
627
627
628
628
629
629
630
630
631
631
632
632
633
633
634
634
635
635
636
636
637
637
638
638
639
639
640
640
641
641
642
642
643
643
644
644
645
645
646
646
647
647
648
648
649
649
650
650
651
651
652
652
653
653
654
654
655
655
656
656
657
657
658
658
659
659
660
660
661
661
662
662
663
663
664
664
665
665
666
666
667
667
668
668
669
669
670
670
671
671
672
672
673
673
674
674
675
675
676
676
677
677
678
678
679
679
680
680
681
681
682
682
683
683
684
684
685
685
686
686
687
687
688
688
689
689
690
690
691
691
692
692
693
693
694
694
695
695
696
696
697
697
698
698
699
699
700
700
701
701
702
702
703
703
704
704
705
705
706
706
707
707
708
708
709
709
710
710
711
711
712
712
713
713
714
714
715
715
716
716
717
717
718
718
719
719
720
720
721
721
722
722
723
723
724
724
725
725
726
726
727
727
728
728
729
729
730
730
731
731
732
732
733
733
734
734
735
735
736
736
737
737
738
738
739
739
740
740
741
741
742
742
743
743
744
744
745
745
746
746
747
747
748
748
749
749
750
750
751
751
752
752
753
753
754
754
755
755
756
756
757
757
758
758
759
759
760
760
761
761
762
762
763
763
764
764
765
765
766
766
767
767
768
768
769
769
770
770
771
771
772
772
773
773
774
774
775
775
776
776
777
777
778
778
779
779
780
780
781
781
782
782
783
783
784
784
785
785
786
786
787
787
788
788
789
789
790
790
791
791
792
792
793
793
794
794
795
795
796
796
797
797
798
798
799
799
800
800
801
801
802
802
803
803
804
804
805
805
806
806
807
807
808
808
809
809
810
810
811
811
812
812
813
813
814
814
815
815
816
816
817
817
818
818
819
819
820
820
821
821
822
822
823
823
824
824
825
825
826
826
827
827
828
828
829
829
830
830
831
831
832
832
833
833
834
834
835
835
836
836
837
837
838
838
839
839
840
840
841
841
842
842
843
843
844
844
845
845
846
846
847
847
848
848
849
849
850
850
851
851
852
852
853
853
854
854
855
855
856
856
857
857
858
858
859
859
860
860
861
861
862
862
863
863
864
864
865
865
866
866
867
867
868
868
869
869
870
870
871
871
872
872
873
873
874
874
875
875
876
876
877
877
878
878
879
879
880
880
881
881
882
882
883
883
884
884
885
885
886
886
887
887
888
888
889
889
890
890
891
891
892
892
893
893
894
894
895
895
896
896
897
897
898
898
899
899
900
900
901
901
902
902
903
903
904
904
905
905
906
906
907
907
908
908
909
909
910
910
911
911
912
912
913
913
914
914
915
915
916
916
917
917
918
918
919
919
920
920
921
921
922
922
923
923
924
924
925
925
926
926
927
927
928
928
929
929
930
930
931
931
932
932
933
933
934
934
935
935
936
936
937
937
938
938
939
939
940
940
941
941
942
942
943
943
944
944
945
945
946
946
947
947
948
948
949
949
950
950
951
951
952
952
953
953
954
954
955
955
956
956
957
957
958
958
959
959
960
960
961
961
962
962
963
963
964
964
965
965
966
966
967
967
968
968
969
969
970
970
971
971
972
972
973
973
974
974
975
975
976
976
977
977
978
978
979
979
980
980
981
981
982
982
983
983
984
984
985
985
986
986
987
987
988
988
989
989
990
990
991
991
992
992
993
993
994
994
995
995
996
996
997
997
998
998
999
999
1000
1000
1001
1001
1002
1002
1003
1003
1004
1004
1005
1005
1006
1006
1007
1007
1008
1008
1009
1009
1010
1010
1011
1011
1012
1012
1013
1013
1014
1014
1015
1015
1016
1016
1017
1017
1018
1018
1019
1019
1020
1020
1021
1021
1022
1022
1023
1023
1024
1024
1025
1025
1026
1026
1027
1027
1028
1028
1029
1029
1030
1030
1031
1031
1032
1032
1033
1033
1034
1034
1035
1035
1036
1036
1037
1037
1038
1038
1039
1039
1040
1040
1041
1041
1042
1042
1043
1043
1044
1044
1045
1045
1046
1046
1047
1047
1048
1048
1049
1049
1050
1050
1051
1051
1052
1052
1053
1053
1054
1054
1055
1055
1056
1056
1057
1057
1058
1058
1059
1059
1060
1060
1061
1061
1062
1062
1063
1063
1064
1064
1065
1065
1066
1066
1067
1067
1068
1068
1069
1069
1070
1070
1071
1071
1072
1072
1073
1073
1074
1074
1075
1075
1076
1076
1077
1077
1078
1078
1079
1079
1080
1080
1081
1081
1082
1082
1083
1083
1084
1084
1085
1085
1086
1086
1087
1087
1088
1088
1089
1089
1090
1090
1091
1091
1092
1092
1093
1093
1094
1094
1095
1095
1096
1096
1097
1097
1098
1098
1099
1099
1100
1100
1101
1101
1102
1102
1103
1103
1104
1104
1105
1105
1106
1106
1107
1107
1108
1108
1109
1109
1110
1110
1111
1111
1112
1112
1113
1113
1114
1114
1115
1115
1116
1116
1117
1117
1118
1118
1119
1119
1120
1120
1121
1121
1122
1122
1123
1123
1124
1124
1125
1125
1126
1126
1127
1127
1128
1128
1129
1129
1130
1130
1131
1131
1132
1132
1133
1133
1134
1134
1135
1135
1136
1136
1137
1137
1138
1138
1139
1139
1140
1140
1141
1141
1142
1142
1143
1143
1144
1144
1145
1145
1146
1146
1147
1147
1148
1148
1149
1149
1150
1150
1151
1151
1152
1152
1153
1153
1154
1154
1155
1155
1156
1156
1157
1157
1158
1158
1159
1159
1160
1160
1161
1161
1162
1162
1163
1163
1164
1164
1165
1165
1166
1166
1167
1167
1168
1168
1169
1169
1170
1170
1171
1171
1172
1172
1173
1173
1174
1174
1175
1175
1176
1176
1177
1177
1178
1178
1179
1179
1180
1180
1181
1181
1182
1182
1183
1183
1184
1184
1185
1185
1186
1186
1187
1187
1188
1188
1189
1189
1190
1190
1191
1191
1192
1192
1193
1193
1194
1194
1195
1195
1196
1196
1197
1197
1198
1198
1199
1199
1200
1200
1201
1201
1202
1202
1203
1203
1204
1204
1205
1205
1206
1206
1207
1207
1208
1208
1209
1209
1210
1210
1211
1211
1212
1212
1213
1213
1214
1214
1215
1215
1216
1216
1217
1217
1218
1218
1219
1219
1220
1220
1221
1221
1222
1222
1223
1223
1224
1224
1225
1225
1226
1226
1227
1227
1228
1228
1229
1229
1230
1230
1231
1231
1232
1232
1233
1233
1234
1234
1235
1235
1236
1236
1237
1237
1238
1238
1239
1239
1240
1240
1241
1241
1242
1242
1243
1243
1244
1244
1245
1245
1246
1246
1247
1247
1248
1248
1249
1249
1250
1250
1251
1251
1252
1252
1253
1253
1254
1254
1255
1255
1256
1256
1257
1257
1258
1258
1259
1259
1260
1260
1261
1261
1262
1262
1263
1263
1264
1264
1265
1265
1266
1266
1267
1267
1268
1268
1269
1269
1270
1270
1271
1271
1272
1272
1273
1273
1274
1274
1275
1275
1276
1276
1277
1277
1278
1278
1279
1279
1280
1280
1281
1281
1282
1282
1283
1283
1284
1284
1285
1285
1286
1286
1287
1287
1288
1288
1289
1289
1290
1290
1291
1291
1292
1292
1293
1293
1294
1294
1295
1295
1296
1296
1297
1297
1298
1298
1299
1299
1300
1300
1301
1301
1302
1302
1303
1303
1304
1304
1305
1305
1306
1306
1307
1307
1308
1308
1309
1309
1310
1310
1311
1311
1312
1312
1313
1313
1314
1314
1315
1315
1316
1316
1317
1317
1318
1318
1319
1319
1320
1320
1321
1321
1322
1322
1323
1323
1324
1324
1325
1325
1326
1326
1327
1327
1328
1328
1329
1329
1330
1330
1331
1331
1332
1332
1333
1333
1334
1334
1335
1335
1336
1336
1337
1337
1338
1338
1339
1339
1340
1340
1341
1341
1342
1342
1343
1343
1344
1344
1345
1345
1346
1346
1347
1347
1348
1348
1349
1349
1350
1350
1351
1351
1352
1352
1353
1353
1354
1354
1355
1355
1356
1356
1357
1357
1358
1358
1359
1359
1360
1360
1361
1361
1362
1362
1363
1363
1364
1364
1365
1365
1366
1366
1367
1367
1368
1368
1369
1369
1370
1370
1371
1371
1372
1372
1373
1373
1374
1374
137
```

Debugger

Dient der schrittweisen Ausführung des zu analysierenden Codes oder Hardware; ermöglichen zum Beispiel Speicherinspektion und Manipulation.

- gdb
- lldb
- x64dbg (Windows, Open-Source)
- jdb (Java Debugger)

Auch für das Debuggen von Hardware gibt es entsprechende Werkzeuge, z.B. [Lauterbach Hardware Debugger](#). Mittels solcher Werkzeuge ist es möglich die Ausführung von Hardware Schritt für Schritt ( *'single step mode'*) zu verfolgen und den Zustand der Hardware (Speicher und Register) zu inspizieren. Dies erfordert (z.Bsp.) eine JTAG Schnittstelle.

2. ERSCHWERUNG DES REVERSE ENGINEERING

Prof. Dr. Michael Eichberg

Obfuscation (☞ Verschleierung)

- Techniken, die dazu dienen das Reverse Engineering zu erschweren.
- Häufig eingesetzt ...
 - von Malware
 - Adware (im Kontext von Android ein häufig beobachtetes Phänomen)
 - zum Schutz geistigen Eigentums
 - für DRM / Durchsetzung von Kopierrechten
 - zur Prävention von „Cheating“ (insbesondere im Umfeld von Online Games)
 - Wenn das Programm als Source Code vertrieben wird (JavaScript)
- Arbeiten auf Quellcode oder Maschinencode Ebene
- Grenze zwischen *Code Minimization*, *Code Optimization* und *Code Obfuscation* ist fließend.
- Mögliche Werkzeuge (ohne Wertung der Qualität/Effektivität):
 - [Java] Proguard / Dexguard
 - [C/C++] Star Force

17

Gerade im Umfeld von klassischen *Binaries* für Windows, Mac und Linux erhöhen Compiler Optimierungen, z.B. von C/C++ und Rust Compilern (`-O2` / `-O3`), bereits den Aufwand, der notwendig ist den Code zu verstehen, erheblich.

Hinweis

Einen ambitionierten und entsprechend ausgestatteten Angreifer wird **Code Obfuscation** bremsen, aber sicher nicht vollständig ausbremsen und das Vorhaben verteilen.

Obfuscation - Techniken (Auszug)

- entfernen aller Debug-Informationen
- das Kürzen aller möglichen Namen (insbesondere Methoden und Klassennamen)
- das Verschleiern von Konstanten durch den Einsatz vermeintlich komplexer Berechnungen zu deren Initialisierung.

```
~(((int)Math.PI) ^ Integer.MAX_VALUE >> 16)+Short.MAX_VALUE  
= 2
```

Obfuscation - Techniken (Auszug)

- die Verwendung von Unicode Codepoints für Strings oder die Verschleierung von Strings mittels rot13 Verschlüsselung.

```
/* ??? */ printf("\x48""e\x154l\x6F"" \x127o\x72""l\x144!");  
/* = */ printf("Hello World!");
```

- das Umstellen von Instruktionen, um das Dekompilieren zu erschweren
- das Hinzufügen von totem Code
- den relevanten Teil der Anwendung komprimieren und verschlüsseln und erst bei Verwendung entpacken und entschlüsseln.
- ...

Umstellen von Instruktionen

Das Umstellen von Instruktionen erschwert die Analyse, da viele Werkzeuge zum Dekompilieren auf die Erkennung von bestimmten Mustern im Code angewiesen sind und ansonsten nur sehr generischen (Spaghetti Code) oder gar unsinnigen Code zurückgeben.

Verschleierung von Strings

Das Verschleiern von Strings kann insbesondere das Reversen von Binärkode erschweren, da ein Angreifer häufig „nur“ an einer ganz bestimmten Funktionalität interessiert ist und dann Strings ggf. einen sehr guten Einstiegspunkt für die weitergehende Analyse bieten.

Stellen Sie sich eine komplexe Java Anwendung vor, in der alle Namen von Klassen, Methoden und Attributen durch einzelne oder kurze Sequenzen von Buchstaben ersetzt wurden und sie suchen danach wie von der Anwendung Passworte verarbeitet werden. Handelt es sich um eine GUI Anwendung, dann wäre zum Beispiel die Suche nach Text, der in den Dialogen vorkommt (z.B. **"Password"**) z.B. ein sehr guter Einstiegspunkt.

3. EINE SEHR KURZ EINFÜHRUNG IN JAVA

BYTECODE

Prof. Dr. Michael Eichberg

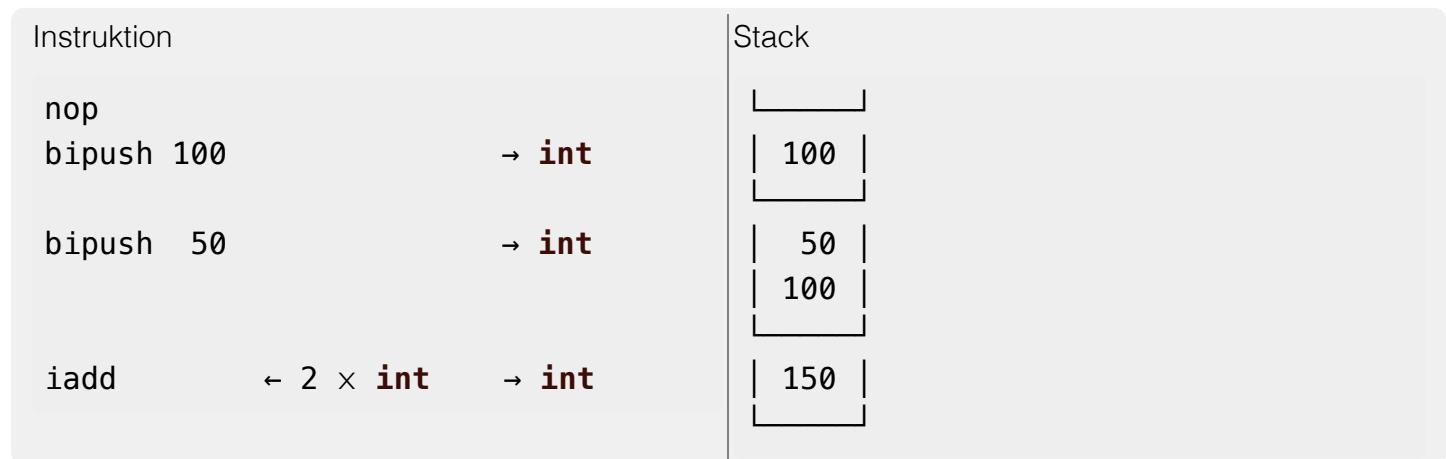
Die Java Virtual Machine

- **Java Bytecode** ist die Sprache, in der Java (oder Scala, Kotlin, Groovy, ...) Programme auf der Java Virtual Machine (JVM) [1] ausgeführt werden.
- In den meisten Fällen arbeiten Java Decompiler so gut, dass ein tiefgehendes Verständnis von Java Bytecode selten notwendig ist.
- Java Bytecode kann, muss aber nicht interpretiert werden. (z.B. können virtuelle Methodenaufrufe in Java schneller sein als in C++)

[1] Java Bytecode Spezifikation

Java Bytecode - stackbasierte virtuelle Maschine

Die JVM ist eine stackbasierte virtuelle Maschine; die getypten Operanden eines Befehls werden auf einem Stack abgelegt und die Operationen arbeiten auf den obersten Elementen des Stacks. Jeder Thread hat seinen eigenen Stack.



- Die benötigte Höhe des Stacks wird vom Compiler berechnet und von der JVM überprüft.

Java Bytecode - Methodenaufrufe und lokale Variablen

- Die Java Virtual Machine verwendet lokale Variablen zur Übergabe von Parametern beim Methodenaufruf.
- Beim Aufruf von *Klassenmethoden* (**static**) werden alle Parameter in aufeinanderfolgenden lokalen Variablen übergeben, beginnend mit der lokalen Variable 0. d.h. in der aufrufenden Methode werden die Parameter vom Stack geholt und in lokalen Variablen gespeichert.
- Beim Aufruf von *Instanzmethoden* wird die lokale Variable 0 dazu verwendet, um die Referenz (**this**) auf das Objekt zu übergeben, auf dem die Instanzmethode aufgerufen wird. Anschließend werden alle Parameter in aufeinanderfolgenden lokalen Variablen übergeben, beginnend mit der lokalen Variable 1.
- Die Anzahl der benötigten lokalen Variablen wird vom Compiler berechnet und von der JVM überprüft.

Beispiel: *Default Constructor In Java Bytecode*

Ein *Constructor* welcher keine expliziten Parameter hat und nur den super Konstruktor aufruft.

```
// Method descriptor #8 ()V
// Stack: 1, Locals: 1
public Main();
  0  aload_0 [this]
  1  invokespecial java.lang.Object() [31]
  4  return
```

Die Zeilennummern und die Informationen über die lokalen Variablen ist optional und wird nur für Debugging Zwecke benötigt.

```
Line numbers:          [pc: 0, line: 9]
Local variable table: [pc: 0, pc: 5]  local: this
                           index: 0
                           type: de.dhbw.simplesecurepp.Main
```

Es gibt weitere Metainformationen, die „nur“ für Debugging-Zwecke benötigt werden, z.B. Informationen über die ursprünglich Quelle des Codes oder die sogenannte "Local Variable Type Table" in Hinblick auf generische Typinformationen. Solche Informationen werden häufig vor Auslieferung entfernt bzw. nicht hineinkompiliert.

Beispiel: Aufruf einer komplexeren Methode

```
// Method descriptor #36 ([Ljava/lang/String;)V
// Stack: 5, Locals: 8
public static void main(java.lang.String[] args) throws ...;
  0  aload_0 [args]
  1  arraylength
  2  iconst_2
  3  if_icmpneq 74           // integer comparison for equality
  6  getstatic java.lang.System.err : java.io.PrintStream
  9  ldc <String "SimpleSecure++">
11  invokevirtual java.io.PrintStream.println(java.lang.String) : void
...
...
```

4. VERSCHLÜSSELUNG VON DATEN

Prof. Dr. Michael Eichberg

Alternativen zur Speicherung von Passwörtern

In einigen Anwendungsgebieten ist es möglich auf das explizite Speichern von Passwörtern ganz zu verzichten [*].

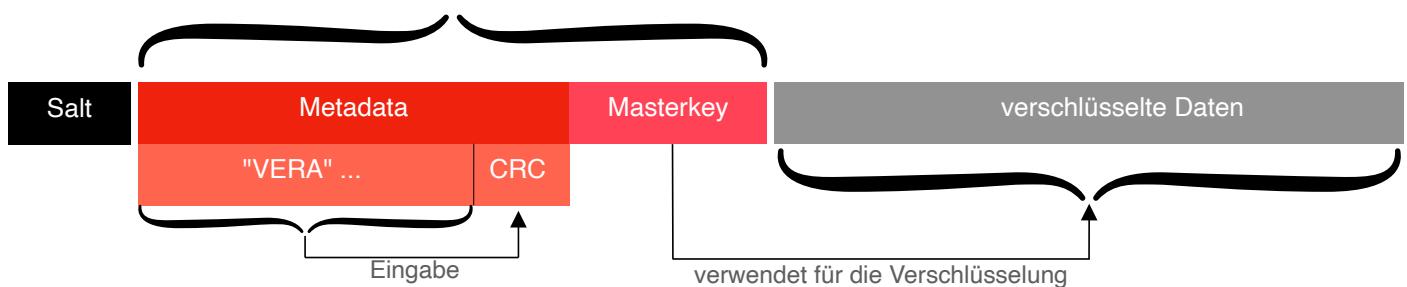
Stattdessen wird z.B. einfach versucht das Ziel zu entschlüsseln und danach evaluiert ob das Passwort (vermutlich) das Richtige war.

Kann darauf verzichtet werden zu überprüfen ob das Passwort korrekt war, dann sind keine Metainformationen notwendig und die verschlüsselte Datei kann genau so groß sein wie die unverschlüsselte Datei.

[*] Bei einer Verschlüsselung mit OpenSSL wird das Passwort nicht gespeichert.

schematische Darstellung der Verschlüsselung von Containern (z. B., Veracrypt)

Der Schlüssel wird mit Hilfe bekannter Schlüsselableitungsfunktionen aus dem Nutzerpasswort berechnet.



Generische Dateiverschlüsselung ohne explizite Speicherung des Passworts

verschlüsselt mit einem vom Passwort des Nutzers abgeleiteten Schlüssel



Alt 1



Alt 2

Die Prüfsumme (CRC) oder der wohldefinierte Header werden zur Validieren des Passworts verwendet.

Bleibe fokussiert!

Analysiere nur was notwendig ist.