

Sicherheit in Android und iOS

David Artmann¹ Kristoffer Schneider¹

¹Hochschule für angewandte Wissenschaften
Würzburg-Schweinfurt

30. Juni 2015

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Trusted Execution Environment / Secure Enclave

Secure boot chain

Userland (Sandboxing / Rechte)

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- **Applikationssicherheit**

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler

App-Berechtigungen

iOS bis Android M granularer

Zeitweise Abhilfe durch AppOps

Mit iOS 9 und Android M gleichauf

App-Berechtigungen

iOS bis Android M granularer

Zeitweise Abhilfe durch AppOps

Mit iOS 9 und Android M gleichauf

App-Berechtigungen

iOS bis Android M granularer

Zeitweise Abhilfe durch AppOps

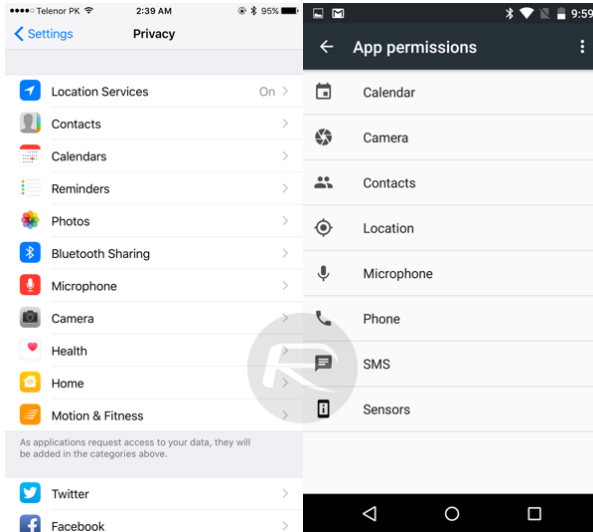
Mit iOS 9 und Android M gleichauf

App-Berechtigungen

iOS bis Android M granularer

Zeitweise Abhilfe durch AppOps

Mit iOS 9 und Android M gleichauf



Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext



freie Modifikation

dezentrale Updatepolitik

offener Quelltext



einheitliche Konfiguration

zentrale Updateregulung

geschlossener Quelltext

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- **Opensource von Android**
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	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	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523</
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-------



	0	1	...



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	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	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523</
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-------



	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	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	160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191	192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255	256	257	258	259	260	261	262	263	264	265	266	267	268	269	270	271	272	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	291	292	293	294	295	296	297	298	299	300	301	302	303	304	305	306	307	308	309	310	311	312	313	314	315	316	317	318	319	320	321	322	323	324	325	326	327	328	329	330	331	332	333	334	335	336	337	338	339	340	341	342	343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362	363	364	365	366	367	368	369	370	371	372	373	374	375	376	377	378	379	380	381	382	383	384	385	386	387	388	389	390	391	392	393	394	395	396	397	398	399	400	401	402	403	404	405	406	407	408	409	410	411	412	413	414	415	416	417	418	419	420	421	422	423	424	425	426	427	428	429	430	431	432	433	434	435	436	437	438	439	440	441	442	443	444	445	446	447	448	449	450	451	452	453	454	455	456	457	458	459	460	461	462	463	464	465	466	467	468	469	470	471	472	473	474	475	476	477	478	479	480	481	482	483	484	485	486	487	488	489	490	491	492	493	494	495	496	497	498	499	500	501	502	503	504	505	506	507	508	509	510	511	512	513	514	515	516	517	518	519	520	521	522	523</
--	---	---	---	---	---	---	---	---	---	---	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-----	-------

Rooting von Androidsystemen

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Rooting von Androidsystemen

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Rooting von Androidsystemen

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke

Möglich durch Exploits oder spezielle Builds

Gefährdung des Sicherheitssystems

Schwer zu kontrollieren für Nutzer und Entwickler

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Beispiel: Rooting von Samsung Geräten durch einen Sicherheitslücke Der Exploit

Wurde von alephzain, des XDA-Forums entdeckt

Betroffen sind waren bzw. sind mehrere Geräte von Samsung (S2, S3)

Zugriff auf den **gesamten** physischen Arbeitsspeicher möglich

Fahrlässige Berechtigungsvergabe für /dev/exynos-mem

Veränderungen am Kernel durch **jeden** Nutzer möglich

Hersteller und proprietäre Apps

Nur schwer zu kontrollieren

Erweiterte Rechte durch Herstellerzertifikate

Beispiel: Google Settings

Hersteller und proprietäre Apps

Nur schwer zu kontrollieren

Erweiterte Rechte durch Herstellerzertifikate

Beispiel: Google Settings

Hersteller und proprietäre Apps

Nur schwer zu kontrollieren

Erweiterte Rechte durch Herstellerzertifikate

Beispiel: Google Settings

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Beispiel: *Google Einstellungen*

Auf den meisten Geräten
vorinstalliert

Dient zur Synchronisation mit
dem Google-Account

Installation durch Google
möglich

Weitere versteckte Funktionen?

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- **Proprietät unter iOS**

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler



Produktion HW/SW im eigenen Haus

Ungewissheit durch Proprietät





Produktion HW/SW im eigenen Haus

Ungewissheit durch Proprietät

Umgehen dieser Politik durch Jailbreaking

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

Publizieren von undokumentierten Diensten im Juni 2013

Nach Zdziarski's Paper

lockdownd

com.apple.mobile.pcapd

com.apple.mobile.file_relay

com.apple.mobile.house_arrest

lockdown

Ermöglicht Zugriff über TCP Port 62078

Abarbeitung über eigenes Protokoll *usbmux*

Übergebene Portnummer auf localhost

lockdown

Ermöglicht Zugriff über TCP Port 62078

Abarbeitung über eigenes Protokoll *usbmux*

Übergebene Portnummer auf localhost

lockdown

Ermöglicht Zugriff über TCP Port 62078

Abarbeitung über eigenes Protokoll *usbmux*

Übergebene Portnummer auf localhost

com.apple.mobile.**pcapd**

Sniffingsoftware auf Basis von *pcap*

Implementierung durch Bibliothek *libcap*

Kein visueller Hinweis auf Aktivität des Dienstes

Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

Sniffingsoftware auf Basis von *pcap*

Implementierung durch Bibliothek *libcap*

Kein visueller Hinweis auf Aktivität des Dienstes

Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

Sniffingsoftware auf Basis von *pcap*

Implementierung durch Bibliothek *libcap*

Kein visueller Hinweis auf Aktivität des Dienstes

Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.**pcapd**

Sniffingsoftware auf Basis von *pcap*

Implementierung durch Bibliothek *libcap*

Kein visueller Hinweis auf Aktivität des Dienstes

Seit iOS 8 nicht mehr über WLAN ansprechbar

com.apple.mobile.file_relay

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.file_relay

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.file_relay

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.**file_relay**

Zugriff auf Adressbuch, GPS Daten, Fotos

Metadaten Abbild des Dateisystems

Apple:

In iOS 8 and later, this capability requires additional configuration before use.

com.apple.mobile.house_arrest

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

`com.apple.mobile.house_arrest`

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

com.apple.mobile.**house_arrest**

Offiziell für Datentransfer von iTunes und Testdaten für Xcode

Zdziarski: Zugriff auf Library, Cache, Cookies, bevorzugte Ordner

Obwohl die iTunes GUI dies nicht erlaubt

Historische Exploits

libTiff Exploit

Ikee Virus

No iOS Zone

Historische Exploits

libTiff Exploit

Ikee Virus

No iOS Zone

Historische Exploits

libTiff Exploit

Ikee Virus

No iOS Zone

Historische Exploits

libTiff Exploit

Ikee Virus

No iOS Zone

libTiff Exploit (2007)

Pufferüberlauf der libtiff Bibliothek

Wurde für Jailbreak genutzt

iOS Prozesse liefen noch mit root (iOS 1)

libTiff Exploit (2007)

Pufferüberlauf der libtiff Bibliothek

Wurde für Jailbreak genutzt

iOS Prozesse liefen noch mit root (iOS 1)

libTiff Exploit (2007)

Pufferüberlauf der libtiff Bibliothek

Wurde für Jailbreak genutzt

iOS Prozesse liefen noch mit root (iOS 1)

Ikee Virus (2009)

Einer der ersten Würmer unter iOS

Standardpasswort der Jailbreak SSH Zugänge ausgenutzt

Bösartige Variante *Ikee.B* stahl Daten

Ikee Virus (2009)

Einer der ersten Würmer unter iOS

Standardpasswort der Jailbreak SSH Zugänge ausgenutzt

Bösartige Variante *Ikee.B* stahl Daten

Ikee Virus (2009)

Einer der ersten Würmer unter iOS

Standardpasswort der Jailbreak SSH Zugänge ausgenutzt

Bösartige Variante *Ikee.B* stahl Daten

No iOS Zone (2014)

<https://www.youtube.com/watch?v=i2tYdmOQisA>

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

No iOS Zone (2014)

<https://www.youtube.com/watch?v=i2tYdmOQisA>

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

No iOS Zone (2014)

<https://www.youtube.com/watch?v=i2tYdmOQisA>

Fehler im Parser für SSL-Zertifikate

Verbinden zu WLAN-AP führt zu DoS und Bootloop

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler

Gliederung

1 Gemeinsamkeiten und Unterschiede

- Systemsicherheit
- Applikationssicherheit

2 Systemkultur

- Android vs. iOS
- Opensource von Android
- Proprietät unter iOS

3 Härten

- Tips für Endnutzer
- Ratschläge für Entwickler