

Contents

1	Digital Television and Smart TVs	1
1.1	Introduction	1
1.1.1	Smart TV	2
1.1.2	HbbTV	2
1.1.3	Security and Privacy	3
1.1.4	Threats	3
1.2	Architecture	4
1.2.1	Hardware	4
1.2.2	Software	5
1.3	Successful Attack Vectors	5
1.3.1	TOCTTOU	6
1.3.2	App Installation	9
1.3.3	Media Player	9
1.3.4	UPNP	10
1.3.5	Countermeasures	11
	References	12
2	Media Playback System	15
2.1	Introduction	15
2.2	Integration	16
2.2.1	Media Player	17
2.2.2	Applications	17
2.3	Implementation	18
2.3.1	Proprietary Player	18
2.3.2	File Format Identification	18
2.3.3	Playback	19
2.4	Attack Scenarios	19
2.5	Exploitation	20
2.5.1	4xm	21
2.5.2	Buffer Overflow	25
2.5.3	Summary	28

- 2.6 Discussion 29
 - 2.6.1 Mitigation 29
 - 2.6.2 Disclosure 29
 - 2.6.3 Affected Devices 30
 - 2.6.4 Vendor Comparison 31
- Appendix 32
- References 32
- 3 Broadcast 35**
 - 3.1 Introduction 35
 - 3.2 DVB 37
 - 3.2.1 PSI and SI Tables 37
 - 3.2.2 Transmission 38
 - 3.3 HbbTV 40
 - 3.4 Previous Attacks 41
 - 3.4.1 Privacy 42
 - 3.4.2 Request Forgery 43
 - 3.4.3 Various 43
 - 3.5 Compromising Smart TV Security via HbbTV 44
 - 3.5.1 Smart TV Attack Surface 44
 - 3.5.2 Replacing the Regular Broadcast Signal 46
 - 3.6 PoC Attack 51
 - 3.6.1 Scenario 51
 - 3.6.2 Regular Signal Acquisition 52
 - 3.6.3 Transport Stream Modification 52
 - 3.6.4 Retransmission 53
 - 3.6.5 Exploitation 55
 - 3.6.6 Malicious App 55
 - 3.6.7 Disclosure and Reaction 56
 - 3.7 Co-channel Protection Ratio 56
 - 3.7.1 Measurements 57
 - 3.7.2 Attack Range and Controlled Area 60
 - 3.7.3 Comparison to Previous Work 62
 - 3.7.4 Mush Zone 63
 - 3.7.5 Variations 65
 - 3.8 Cookie Jar Isolation 66
 - 3.8.1 Authenticated Request Forgery 68
 - 3.8.2 Analysis 69
 - 3.8.3 Results 69
 - 3.8.4 Side Effects 71

- 3.9 A Novel Protection Scheme. 72
 - 3.9.1 Attack Properties 72
 - 3.9.2 Lock-Based Protection 73
 - 3.9.3 Long-Term Solution. 75
 - 3.9.4 Discussion 76
- 3.10 Conclusions. 77
- References 78
- 4 Security & Privacy Implications 81**
 - 4.1 Consumers 81
 - 4.1.1 Threats 81
 - 4.1.2 Mitigation. 84
 - 4.2 Content Providers. 85
 - 4.3 Vendors 86
 - 4.3.1 Firmware Updates 86
 - 4.3.2 Exploit Mitigation 90
 - 4.3.3 Opportunities. 90
 - 4.4 Broadcasters 91
 - References 91



<http://www.springer.com/978-3-319-20993-7>

Smart TV Security

Media Playback and Digital Video Broadcast

Michéle, B.

2015, XV, 92 p. 19 illus., 9 illus. in color., Softcover

ISBN: 978-3-319-20993-7