

Contents

1	Introduction	1
2	Overview of Bluetooth Security	3
3	Reasons for Bluetooth Network Vulnerabilities	15
3.1	Vulnerability to Eavesdropping	15
3.2	Weaknesses in Encryption Mechanisms	19
3.3	Weaknesses in PIN Code Selection	20
3.4	Weaknesses in Association Models of SSP	21
3.5	Weaknesses in Device Configuration	22
4	Comparative Analysis of Bluetooth Security Attacks	23
4.1	Disclosure Threats	24
4.2	Integrity Threats	34
4.3	DoS Threats	36
4.4	Multithreats	42
5	MITM Attacks on Bluetooth	61
5.1	MITM Attacks on SSP	61
5.2	Comparative Analysis of Bluetooth MITM Attacks	67
6	Countermeasures	71
6.1	Intrusion Detection and Prevention System	71
6.2	RF Fingerprint-Based Security Solution for SSP	74
6.3	Countermeasures for Bluetooth Devices up to 2.0 + EDR	77
6.4	Countermeasures for SSP-Enabled Bluetooth Devices	80
7	New Practical Attack	83
8	Conclusion and Future Work	85
	References	89

Bluetooth Security Attacks

Comparative Analysis, Attacks, and Countermeasures

Haataja, K.; Hyppönen, K.; Pasanen, S.; Toivanen, P.

2013, VII, 93 p. 31 illus., Softcover

ISBN: 978-3-642-40645-4