

ISO/IEC 27033-6:2016-06 (E)

Information technology - Security techniques - Network security - Part 6: Securing wireless IP network access

Contents		Page
Foreword		v
Introduction		vi
1	Scope	1
2	Normative references	1
3	Terms and definitions	1
4	Abbreviated terms	3
5	Structure	5
6	Overview	5
7	Security threats	8
7.1	General	8
7.2	Unauthorized access	8
7.3	Packet sniffing	8
7.4	Rogue wireless access point	9
7.5	Denial of service attack	9
7.6	Bluejacking	10
7.7	Bluesnarfing	10
7.8	Adhoc networks	10
7.9	Other threats	10
8	Security requirements	10
8.1	General	10
8.2	Confidentiality	11
8.3	Integrity	11
8.4	Availability	11
8.5	Authentication	11
8.6	Authorization	12
8.7	Accountability (Non-repudiation)	12
9	Security controls	12
9.1	General	12
9.2	Encryption control and implementation	13
9.3	Integrity evaluation	14
9.4	Authentication	14
9.5	Access control	15
9.5.1	General	15
9.5.2	Permission control	16
9.5.3	Network-based control	16
9.6	Denial of service attack resilience	16
9.7	DMZ segregation via firewall protection	16
9.8	Vulnerability management through secure configurations and hardening of devices	16
9.9	Continuous monitoring of wireless networks	17
10	Security design techniques and considerations	17

10.1	General	17
10.2	Wi-Fi	18
10.2.1	General	18
10.2.2	User authentication	18
10.2.3	Confidentiality and integrity	19
10.2.4	Wireless Wi-Fi technologies	19
10.2.5	Other Wi-Fi Configurations	19
10.2.6	Access control -- User equipment	19
10.2.7	Access control -- Infrastructure access point	20
10.2.8	Availability	21
10.2.9	Accountability	21
10.3	Mobile communication security design	21
10.4	Bluetooth	22
10.5	Other wireless technologies	23
Annex A (informative) Technical description of threats and countermeasures		24
Bibliography		26