

Contents

1	Introduction.....	5
1.1	The Main Expressions	5
1.2	Safety	5
1.3	Security and Reliability	6
1.4	Privacy	7
2	Architecture of the System	8
3	Data Collected and Data Released.....	10
3.1	What is Collected in Monitoring System.....	10
3.2	What Can Be Released	11
4	Security Models	13
5	Attack Scenarios and Analysis	15
5.1	Attacks by User.....	17
5.1.1	Attack on Sensors and Input Data.....	17
5.1.2	Attack on Sensor Unit Itself.....	17
5.1.3	Attack on Sensor Unit Data	18
5.1.4	Specific User's Attacks.....	18
5.1.5	Foiling the System	19
5.1.6	Protecting the User Own Privacy.....	19
5.2	Attacks by Service Provider	19
5.2.1	Attacks with Objective to Increase Revenue from Customer.....	20
5.2.2	Attacks on Customer Profile.....	20
5.2.3	Attacks with Objective to Resale of Data about Customers.....	20
5.2.4	Attacks with Objective to Reduction in Payments to Service Charger	21
5.3	Attacks by Service Charger	21
5.3.1	Attacks with Objective to Increase Revenue	22
5.3.2	Reselling the Data and Specific Information.....	22
5.4	Attacks by Hacker.....	23
5.4.1	Demonstration of System Vulnerability	23
5.4.2	Exhibitionism.....	23
5.4.3	Research Attacks.....	24
5.4.4	Attacks by Hacktivist or Terrorist	25
5.4.5	Societal Destabilization Through Manipulation of the Monitoring System.....	25

5.4.6	Raise in Profile of the Activists Cause.....	26
5.4.7	Direct Furthering of Activists Cause.....	26
5.4.8	Reduction in Credibility of the System.....	26
5.5	Communication Provider Attacks.....	26
5.5.1	Change in Network Utilization.....	26
5.5.2	Collecting the Travel Behavior.....	27
5.6	Attacks by Enterprise.....	27
5.6.1	Movement Tracking.....	27
5.6.2	Creation and Distribution of Cloned Equipment.....	28
5.6.3	Attack to Disable or to Compromise System Encryption.....	28
5.6.4	Stealing Equipment.....	28
5.6.5	Racketeering.....	28
5.6.6	Manipulation of Public Opinion.....	29
5.7	Attacks by Government and NGO.....	29
5.7.1	In Theatre Commercial Advantage.....	29
5.7.2	Political Targeting of Individuals and Organizations.....	30
5.7.3	Tracking of Individuals.....	30
5.7.4	NGO Activities.....	30
5.8	Attacks by Foreign Power.....	31
5.8.1	Societal Destabilization.....	31
5.8.2	Movement Tracking.....	31
5.8.3	Racketeering.....	31
5.8.4	International Prestige.....	32
6	Asset based threat analysis.....	33
6.1	Threatened Assets.....	33
6.2	Taxonomy of Threats.....	34
6.2.1	The Basic Threats.....	34
6.2.2	The Activation Threats.....	34
6.2.3	The Underlying Threats.....	35
6.3	Threats, Objects and Assets.....	37
7	Technology of Wireless Attacks.....	39
7.1	Eavesdropping.....	39
7.2	Security on Higher Layers of the System.....	40
7.3	Attack on Authentication.....	44
7.4	Passwords and Attack on Passwords.....	44

7.5	Challenge-Response Method	46
7.6	Skimming.....	47
7.7	Hiding and Jamming.....	47
7.8	Antijamming Techniques at Physical Layer.....	48
7.9	Anti-jamming Security Schemes	51
7.9.1	Proactive Countermeasures.....	51
7.9.2	Reactive Countermeasures.....	54
8	Privacy in Environmental Monitoring Network	56
8.1	Privacy Risk.....	56
8.2	Data Correlation, Evolution and Unusual Data	56
8.3	User Location.....	57
8.4	Publishing Environmental Macrodata and Microdata	57
8.5	How to Detect and Protect Sensitive Cell.....	58
8.6	Publishing Environmental Microdata.....	58
8.7	Protecting Privacy of Location Information in Environmental Data.....	60
9	Conclusion.....	61
10	References.....	63