UNIVERSITI PUTRA MALAYSIA

A NEW SECURITY FRAMEWORK TO PREVENT DENIAL OF SERVICE AND REPLAY ATTACKS FOR IEEE 802.11 WIRELESS NETWORKS

MINA MALEKZADEH

FSKTM 2011 25

A NEW SECURITY FRAMEWORK TO PREVENT DENIAL OF SERVICE AND REPLAY ATTACKS FOR IEEE 802.11 WIRELESS NETWORKS

By

MINA MALEKZADEH

Thesis Submitted to the School of Graduate Studies, Universiti Putra Malaysia, in Fulfilment of the Requirements for the Degree of Doctor of Philosophy

July 2011

Dedicated with endless love to

My beloved husband, Hadi
My little angels, Zahra and Reza
My dear mother and father

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirement for the degree of Doctor of Philosophy

A NEW SECURITY FRAMEWORK TO PREVENT DENIAL OF SERVICE AND REPLAY ATTACKS FOR IEEE 802.11 WIRELESS NETWORKS

By

MINA MALEKZADEH

July 2011

Chairman: Professor Abdul Azim Abdul Ghani, PhD

Faculty: Computer Science and Information Technology

The widespread use of IEEE 802.11 wireless networks demands enhancement in their security. One aspect of security is availability at which the network resources are accessible upon requests made from the authorized users. Persistent availability of the networks is essential particularly when it comes to critical areas such as healthcare centers, hospitals, police departments, military services, and airports. The main threats against availability of the networks are Denial of Service (DoS) and replay attacks. The attacks immediately shutdown the network and make it entirely unavailable for the authorized users.

Despite the presence of different security protocols in wireless networks, such as WEP, WPA, and WPA2, wireless networks are extremely vulnerable to DoS and replay attacks. This vulnerability has never been addressed by IEEE 802.11 standard even in the latest wireless security protocol (WPA2). Protection offered by the IEEE 802.11 security protocols does not cover control frames. The wireless control frames are transmitted in

clear-text form and there is no way for recipients to verify their validity. The unprotected control frames can be exploited by the attackers to carry out DoS attacks.

In order to prevent DoS attacks and guarantee wireless network availability, a new security framework is proposed which is called Authorized Control Frames (ACF). By considering the resource limitation in the wireless networks, the ACF is designed so that while it provides sufficient level of security and high efficiency, it avoids unnecessary overheads. The ACF framework comprises two distinct countermeasures called ACF-non-cryptographic and ACF-cryptographic. The ACF-non-cryptographic countermeasure proposes a lightweight security model without involving cryptographic algorithms. The ACF-cryptographic countermeasure proposes four distinct models; two models are based on SHA1 and SHA2, and another two models are based on modified SHA1 and SHA2. Furthermore, a new replay attack protection mechanism with secure time synchronization is proposed and embedded in the all five proposed models. The proposed models prevent DoS and replay attacks by detecting and discarding forgery control frames belong to the attackers and thereby guarantee availability of the IEEE 802.11 wireless networks.

In order to implement the models, two simulation environments were developed to represent the current model and the proposed models respectively. Seven distinct experiments were carried out to evaluate the proposed models. The experiments were used to determine reliability of the simulation tool, analyze behavior of the proposed models and determine their capabilities to prevent wireless DoS and replay attacks, determine detection accuracy of the proposed models, compare effectiveness of the proposed models, verify

lifetime overhead and security cost of the proposed models, and evaluate performance of the replay-preventing mechanism.

The results of the experiments show that the five proposed models successfully prevent DoS and replay attacks. The proposed models provide 100% performance improvement for the wireless networks under the attacks compared to the current model. Comparing the proposed models with each other shows that the best performance of the wireless networks is achieved when utilizing the ACF-non-cryptographic countermeasure. When comparing the four proposed models of the ACF-cryptographic countermeasure, the results show better performance for the models that are based on modified SHA1 and SHA2.

Abstrak tesis yang dibentangkan kepada Senat Universiti Putra Malaysia bagi memenuhi keperluan untuk ijazah Doktor Falsafah

KERANGKA KERJA KESELAMATAN BAHARU UNTUK MENCEGAH SERANGAN PENAFIAN PERKHIDMATAN DAN ULANGAN UNTUK RANGKAIAN WAYERLES IEEE 802.11

Oleh

MINA MALEKZADEH

Julai 2011

Pengerusi: Profesor Abdul Azim Abd. Ghani, PhD

Fakulti: Sains Komputer Dan Teknologi Maklumat

Penggunaan rangkaian wayerles IEEE 802.11 yang meluas menuntut peningkatan dalam keselamatan mereka. Satu aspek keselamatan ialah ketersediaan sumber rangkaian yang dipohon oleh pengguna yang berizin. Ketersediaan rangkaian yang berterusan adalah penting terutamanya dalam kawasan kritikal seperti pusat kesihatan, hospital, jabatan polis, dan lapangan terbang. Serangan penafian perkhidmatan (DoS) dan ulangan adalah ancaman utama terhadap ketersediaan rangkain. Serangan ini akan dengan segera menutup rangkaian dan menjadikannya secara keseluruhan tidak tersedia untuk penguna.

Walaupun terdapat protokol keselamatan yang berbeza dalam rangkaian wayerles seperti WEP, WPA, dan WPA2, rangkaian wayarles sangat rentan terhadap serangan penafian perkhidmatan. Kerentanan ini tidak pernah di beri tumpuan oleh piawai IEEE 802.11 walaupun dalam protokol terkini, WPA2. Perlindungan yang ditawarkan oleh protokol keselamatan IEEE 802.11 hanya ke atas bingkai data. Namun begitu, bingkai kawalan wayerles dibiarkan tanpa sebarang perlindungan dan tiada cara bagi penerima untuk

mengesahkan kesahihan bingkai kawalan yang diterima. Bingkai kawalan yang tiada perlindungan dapat dieksploit oleh penyerang untuk melakukan serangan penafian perkhidmatan.

Untuk mencegah serangan DoS wayarles dan memastikan ketersediaan rangkaian, kerangka kerja keselamatan baharu dicadangkan yang dipanggil *Authorized Control Frames (ACF).* Dengan mengambil kira keterbatasan sumber dalam rangkaian wayarles, *ACF* direka untuk menyediakan tahap keselamatan yang mencukupi dan kecekapan tinggi sambil mengelak overhed yang tidak perlu. Kerangka kerja *ACF* terdiri daripada dua tindakan pencegahan yang berbeza dipanggil *ACF-non-cryptograhic* dan *ACF-cryptographic*. Tindakan pencegahan *ACF-non-cryptographic* mencadangkan satu model keselamatan ringan. Tindakan pencegahan *ACF-cryptographic* mencadangkan empat model yang berbeza; dua model berasaskan algoritma cincang, SHA1 dan SHA2, dan dua model berasaskan SHA! dan SHA2 yang diubahsuai. Selain itu, mekanisme perlindungan serangan ulangan baharu dicadangkan dan dibenamkan dalam semua lima model yang dicadangkan. Model yang dicadangkan mencegah serangan DoS dan ulangan dengan mengesan dan membuang pemalsuan atau rangka kawalan ulangan milik penyerang dan dengan demikian menjamin ketersediaan rangkaian IEEE 802.11 wayarles.

Enam eksperimen berbeza telah dijalankan untuk menilai model yang dicadangkan. Dua persekitaran simulasi telah dibangunkan masing-masing mewakili model semasa dan model yang dicadangkan. Eksperimen tersebut digunakan untuk menentukan kebolehpercayaan alat simulasi, menentukan kemampuan model yang dicadangkan dalam mencegah serangan DoS dan ulangan wayarles, menganalisis perilaku model yang dicadangkan, menentukan

ketepatan pengesanan model yang dicadangkan, membandingkan keberkesanan model yang dicadangkan, dan mengesahkan overhed masa hayat dan kos keselamatan model yang dicadangkan.

Keputusan eksperimen menunjukkan lima model yang dicadangkan berjaya mencegah serangan DoS dan ulangan wayerles. Model yang dicadangkan memberikan peningkatan prestasi 100% untuk rangkaian wayarles dalam keadaan serangan berbanding dengan model semasa. Membandingkan model cadangan dengan satu sama lain menunjukkan bahawa prestasi terbaik rangkaian wayarles dicapai apabila menggunakan model *ACF-non-cryptograhic*. Apabila membandingkan empat model cadangan *ACF-cryptographic*, keputusan menunjukkan prestasi yang lebih baik bagi model yang berasaskan SHA1 dan SHA2 yang diubahsuai.

ACKNOWLEDGEMENTS

I am thankful to the one above all of us to give the strength that keeps me standing and for the hope and kindness that keep me believing he is always there for me.

I am heartily thankful to my beloved husband and children, my supportive father and mother who with their unconditional love have always stood by me and accept all my absence from many family occasions with a smile.

I am truly thankful to my supervisor Professor Abdul Azim Abdul Ghani, dean of Faculty of Computer Science and Information Technology, whose sincerity, patience, understanding, and encouragement I will never forget. Professor Azim has been my inspiration through all the obstacles from the initial to the final level in completion of this work and other technical papers.

I owe my deep gratitude to my co-supervisor, Dr.Shamala, for her valuable advices and comments which guide me through the proper direction.

APPROVAL

I certify that an Examination Committee has met on date of viva to conduct the final examination of **Mina Malekzadeh** on her **Doctor of Philosophy** thesis entitled ñ**A NEW SECURITY FRAMEWORK TO PREVENT DENIAL OF SERVICE AND REPLAY ATTACKS FOR IEEE 802.11b WIRELESS NETWORKS**" in accordance with Universiti Pertanian Malaysia (Higher Degree) Act 1980 and Universiti Pertanian Malaysia (Higher Degree) Regulations 1981. The Committee recommends that the candidate be awarded the relevant degree. Members of the Examination Committee are as follows:

Ramlan Mahmod, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Mohamed Othman, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Nur Izura Udzir, PhD
Lecturer
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Internal Examiner)

Abderrahim Benslimane, PhD
Professor
Laboratoire Dyinformatique Dyavignon
University Dyavignon
(External Examiner)

HASANAH MOHD GHAZALI, PhD
Professor/Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

This thesis was submitted to the Senate of Universiti Putra Malaysia and has been accepted as fulfilment of the requirements for the degree of Doctor of Philosophy. Members of the Supervisory Committee were as follows:

Abdul Azim Abdul Ghani, PhD
Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Chairman)

Shamala Subramaniam, PhD
Associate Professor
Faculty of Computer Science and Information Technology
Universiti Putra Malaysia
(Member)

Jalil Desa, PhD
Telekom Research & Development
UPM-MTDC technology incubation centre
(Member)

Bujang Kim Huat, PhD
Professor/Deputy Dean
School of Graduate Studies
Universiti Putra Malaysia

Date:

DECLARATION

I declare that the thesis is my original work except for quotations and citations which have been duly acknowledged. I also declare that it has not been previously and is not concurrently, submitted for any other degree at Universiti Putra Malaysia or other institutions.

Mina Malekzadeh

Date: 4 July 2011

TABLE OF CONTENTS

			Page
DEDICATION			ii
ABSTRACT			iii
ABSTRAK			vi
ACKNOWLEDGEMENTS			ix
APPROVAL			x
DECLRATION			xii
LIST OF TABLES			xviii
LIST OF FIGURES			xix
CHAPTERS			
1	**INTRODUCTION**		1
	1.1	Background	1
	1.2	Problem statement	2
	1.3	Research motivation	3
	1.4	Research objectives	4
	1.5	Scope of thesis	6
	1.6	Contribution of thesis	9
	1.7	Thesis outline	11
2	**LITERATURE REVIEW**		13
	2.1	Introduction	13
	2.2	IEEE 802.11 wireless networks	13
		2.2.1 DCF in basic access mode	14
		2.2.2 DCF in RTS/CTS handshake mode	15
	2.3	IEEE 802.11 control frames structure	17
	2.4	Attacks against availability of the wireless networks	20
		2.4.1 Replay attacks	21
		2.4.2 Denial of service attacks	22
	2.5	Summary	34
3	**RESEARCH METHODOLOGY**		35
	3.1	Introduction	35
	3.2	Steps of methodology	35
	3.3	Literature review	37
	3.4	Testbed set up to conduct wireless DoS attacks	38
	3.5	Hash functions analysis	39
	3.6	Proposed ACF security framework	40
	3.7	Countermeasure 1: Proposed ACF-non-cryptographic	41
		3.7.1 Creating TS security field	41
		3.7.2 Development replay-preventing mechanism	41
	3.8	Countermeasure 2: Proposed ACF-cryptographic	42
		3.8.1 Development key derivation algorithm	43
		3.8.2 Creating TS and AF security fields	44
		3.8.3 Development replay-preventing mechanism	45

3.8.4 Development Mhmac1 and Mhmac2 46
3.9 Security analysis of the ACF countermeasures 46
3.10 Experiments 47
3.10.1 Behavior analysis of the current model 49
3.10.2 Simulation reliability: Testbed results vs. Simulation results 50
3.10.3 Behavior analysis of the proposed models 50
3.10.4 Detection accuracy of the proposed models 51
3.10.5 Performance comparison of the models under DoS attacks 51
3.10.6 Performance comparison of the models in baseline mode 52
3.10.7 Performance evaluation of the replay-preventing mechanism 53
3.11 Results and discussion 53
3.12 Conclusion 53
3.13 Summary 54

4 **TESTBED SET UP TO CONDUCT WIRELESS DOS ATTACKS** 55
4.1 Introduction 55
4.2 Testbed environment 55
4.2.1 Hardware details 57
4.2.2 Software details 58
4.2.3 Generating forgery control frames 59
4.2.4 Performance metrics 63
4.2.5 Wireless DoS attacks scenarios 64
4.3 Measurement results and discussion 65
4.3.1 Scenario 1: ACK-DoS-AP attack 66
4.3.2 Scenario 2: ACK-DoS-C attack 67
4.3.3 Scenario 3: CTS-DoS-AP attack 69
4.3.4 Scenario 4: CTS-DoS-C attack 70
4.3.5 Scenario 5: RTS-DoS-AP attack 71
4.3.6 Scenario 6: RTS-DoS-C attack 72
4.3.7 Scenario 7: Contention-Free DoS attacks 75
4.4 Summary 80

5 **CRYPTOGRAPHIC HASH FUNCTIONS** 81
5.1 Introduction 81
5.2 Overview of hash functions 81
5.3 General structure of hash functions 83
5.4 Hash functions security 86
5.5 Hash function applications 89
5.5.1 Key derivation functions 89
5.5.2 Data integrity 90
5.5.3 Message authentication codes 90
5.6 Security analysis of MAC algorithms 93
5.6.1 MAC guessing attack 94
5.6.2 Key recovery attack 95
5.6.3 Forgery attack 96
5.6.4 Distinguishing attack 96
5.6.5 Attacks against compression function 97
5.7 Performance comparison of the hash functions 98

5.7.1 Processing time comparison of the hash functions 99
5.7.2 Throughput comparison of the hash functions 100
5.8 Summary 102

6 **ACF: AUTHORIZED CONTROL FRAMES SECURITY FRAMEWORK** 103
6.1 Introduction 103
6.2 Proposed ACF security framework 103
6.3 Countermeasure 1: Proposed ACF-non-cryptographic 105
6.3.1 Creating TS security field 105
6.3.2 Development replay-preventing mechanism 105
6.3.3 Procedure of the ACF-non-cryptographic countermeasure 119
6.4 Countermeasure 2: Proposed ACF-cryptographic 120
6.4.1 Development key derivation algorithm 121
6.4.2 Creating AF and TS security fields 124
6.4.3 Development replay-preventing mechanism 125
6.4.4 Development Mhmac1 and Mhmac2 127
6.4.5 Procedure of the ACF-cryptographic countermeasure 137
6.5 Security analysis of the ACF-non-cryptographic countermeasure 142
6.6 Security analysis of the ACF-cryptographic countermeasure 143
6.6.1 MAC guessing attack 143
6.6.2 Key recovery attack 144
6.6.3 Forgery attack 145
6.6.4 Attacks against compression function 147
6.7 Summary 150

7 **EXPERIMENTS** 151
7.1 Introduction 151
7.2 Experimental design 151
7.3 Performance measures 152
7.4 Traffic types 153
7.4.1 Connection-oriented traffics 154
7.4.2 Connectionless traffics 155
7.5 Design of scenarios 158
7.5.1 Handshake status 158
7.5.2 Network conditions 159
7.6 Model simulation 162
7.6.1 Simulation of the current model: Simulation environment A 162
7.6.2 Simulation of the proposed models: Simulation environment B 166
7.7 Behavior analysis of the current model 171
7.7.1 Dependent and independent variables 171
7.7.2 Materials and methods 172
7.8 Simulation reliability: Testbed s. Simulation 173
7.8.1 Dependent and independent variables 173
7.8.2 Materials and methods 174
7.9 Behavior analysis of the proposed models 175
7.9.1 Dependent and independent variables 175
7.9.2 Materials and methods 176
7.10 Detection accuracy of the proposed models 177

7.10.1 Dependent and independent variables 177
7.10.2 Materials and methods 178
7.11 Performance comparison of the models under DoS attacks 179
7.11.1 Dependent and independent variables 179
7.11.2 Materials and methods 180
7.12 Performance comparison of the models in baseline mode 180
7.12.1 Dependent and independent variables 180
7.12.2 Materials and methods 181
7.13 Performance evaluation of the replay-preventing mechanism 182
7.13.1 Dependent and independent variables 182
7.13.2 Materials and methods 183
7.14 Summary 183

8 **RESULTS AND DISCUSSION** 184
8.1 Introduction 184
8.2 Behavior analysis of the current model 184
8.2.1 TCP delay analysis in the current model 184
8.2.2 Video streams delay analysis in the current model 186
8.2.3 RTT and PLR analysis in the current model 188
8.2.4 Throughput analysis in the current model 189
8.3 Simulation reliability: Testbed results vs. Simulation results 190
8.4 Behavior analysis of the proposed models 193
8.4.1 TCP delay and throughput analysis in the ACFM1 model 193
8.4.2 TCP delay and throughput analysis in the ACFM2 model 194
8.4.3 TCP delay and throughput analysis in the ACFO1 model 196
8.4.4 TCP delay and throughput analysis in the ACFO2 model 197
8.4.5 TCP delay and throughput analysis in the ACFNC model 198
8.4.6 Video streams delay and throughput analysis in the ACFM1 model 199
8.4.7 Video streams delay and throughput analysis in the ACFM2 model 201
8.4.8 Video streams delay and throughput analysis in the ACFO1 model 202
8.4.9 Video streams delay and throughput analysis in the ACFO2 model 203
8.4.10 Video streams delay and throughput analysis in the ACFNC model 204
8.4.11 RTT analysis in the proposed models 205
8.5 Detection accuracy of the proposed models 207
8.5.1 Accuracy of the ACF-non-cryptographic countermeasure 207
8.5.2 Accuracy of the ACF-cryptographic countermeasure 212
8.6 Performance comparison of the proposed models under DoS attacks 216
8.6.1 TCP and video streams delay comparison under DoS attacks 217
8.6.2 TCP and video streams throughput comparison under DoS attacks 220
8.6.3 RTT and PLR comparison under DoS attacks 224
8.7 Performance comparison of the proposed models in baseline mode 227
8.7.1 TCP and video streams delay comparison in baseline mode 227

8.7.2 TCP and video streams throughput comparison in baseline mode 229
8.7.3 RTT comparison in baseline mode 233
8.8 Performance evaluation of the replay-preventing mechanism 234
8.8.1 Delay comparison: STSF vs. TSF 234
8.8.2 MAC loss rate comparison: STSF vs. TSF 235
8.9 Summary 236

9 **CONCLUSION AND FUTURE WORK** 238
9.1 Conclusion 238
9.2 Future works 244

REFERENCES 245
BIODATA 260
LIST OF PUBLICATIONS 261