

**POTENTIAL IDENTITY THEFT PERSONAL INFORMATION LEAKAGE
WITHIN X UNIVERSITY FREE PUBLIC HOTSPOT**

By

Meily
2-2013-101

A thesis submitted to the Faculty of

ENGINEERING & INFORMATION TECHNOLOGY

in partial fulfilment of the requirements
for the
MASTER'S DEGREE
in

INFORMATION TECHNOLOGY



SWISS GERMAN UNIVERSITY
EduTown BSD City
Tangerang 15339
Indonesia

September 2014
Revision after Thesis Defence on August 25, 2014

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Meily

Student

Date

Approved by:

Dr. Ir. Moh. A. Amin Soetomo, M.Sc.

Thesis Advisor

Date

Charles Lim, M.sc

Thesis Co-Advisor

Date

Dr. Ir. Gembong Baskoro, M.Sc.

Dean

Date

Meily

ABSTRACT

POTENTIAL IDENTITY THEFT PERSONAL INFORMATION LEAKS WITHIN UNIVERSITY X FREE PUBLIC HOTSPOT

By

Meily

Dr. Ir. Moh. A. Amin Soetomo, Advisor

Charles Lim, M.sc, Co-Advisor

SWISS GERMAN UNIVERSITY

The usage of Internet in Indonesia has grown rapidly. This was proved by the number of Internet users either wired or wireless. Internet has become the one thing that people need. With the growth in Internet technology, nowadays wireless Internet connection could be seen everywhere, made it easy for user to access to the Internet. However, there was risk that came with the wireless network connection. Due to its borderless nature, wireless network was vulnerable towards passive sniffing and attack. There was also concern on identity theft that could happen within the wireless network. This research aimed to find out whether there were information leaks that were potential an identity theft material within the wireless network. From the network forensic process done to the network trace data collected via passive sniffing in the university area, there were evidence of potential identity theft information leaks in the wireless network.

Keywords: Identity Theft, Information Leaks, Network Forensic, Passive Sniffing, Wireless Network.



DEDICATION

I dedicate this thesis to all of the Wi-Fi users whoever you are and for the University.
Hopefully this thesis would help open our eyes about the dangers and risks when using
the public free hotspot.



ACKNOWLEDGEMENTS

First of all, this thesis would not have been completed without the grace of the God, Lord and Saviour, Jesus Christ.

There are people who I would like to thank during the creation of this thesis.

I would like to thank the thesis defence panels for giving the University as the scope of this research.

I would like to thank the University's ISS Department's Head Pak Ipung, that gave me the permit to use the University's wireless network access to do the research and also to the staff Pak Budhi who was so helpful about it.

I would like to thank my thesis advisor, Pak Amin, and co-advisor, Pak Charles, for their valuable input during the writing and process of this thesis.

I would like to thank the university's laboratory staff, Mario, who has helped a lot during the data collection and data processing period with the setup.

I would also like to thank my classmates, Nicsen, Herry, Puguh for the input and idea during the formulation of the thesis problem, and also for your supports.

I would also like to thank my family and my co-workers for giving support when I decided to continue my study and when I was writing the thesis.

At last I would like to thanks those who are not mentioned here for your support and well wishes.

TABLE OF CONTENTS

	Pages
STATEMENT BY THE AUTHOR.....	2
ABSTRACT.....	3
DEDICATION.....	5
ACKNOWLEDGEMENTS.....	6
TABLE OF CONTENTS.....	7
LIST OF FIGURES.....	11
LIST OF TABLES.....	13
CHAPTER 1– INTRODUCTION.....	14
1.1 Background.....	14
1.2 General Statement of Problem Area.....	15
1.3 Research Problem.....	16
1.4 Research Question.....	17
1.5 Hypothesis.....	17
1.6 Research Objectives.....	18
1.7 Significance of Study.....	18
1.8 Research Limitation.....	18
1.9 Thesis Organisation.....	18
CHAPTER 2 – LITERATURE REVIEW.....	20
2.1 Theory of Information Leakage.....	20
2.1.1 Introduction.....	20
2.1.2 Source of Information Leakage.....	21
2.2 Theory of Identity Theft.....	22
2.2.1 Introduction.....	22

2.2.2	Type of Identity Theft	23
2.2.2.1	Personal Identity Theft	23
2.2.2.2	Business Identity Theft	25
2.2.3	Methods of Identity Theft	25
2.2.4	Information That Lead to Identity Theft	28
2.2.5	Statistic	37
2.3	Wi-Fi	37
2.3.1	Overview of Wi-Fi	37
2.3.2	Wi-Fi Protocol Architecture	38
2.3.3	Wireless Network Threats and Vulnerabilities	39
2.4	Relevant Previous Research	40
2.4.1	Analysis of a Local-Area Wireless Network	40
2.4.2	Analysis of a Campus wide Wireless Network	41
2.4.3	Large-scale Wireless Local-area Network Measurement and Privacy Analysis	42
2.4.4	Characterizing User Behaviour and Network Performance in a Public Wireless LAN	43
2.4.5	Signals from the Crowd: Uncovering Social Relationships through Smartphone Probes	44
2.4.6	Usage Analysis of a Large Public Wireless LAN	45
2.4.7	Analysis of a Metropolitan-Area Wireless Network	45
2.5	Methodology	46
2.5.1	Network Forensic Framework	46
2.6	Theoretical Framework	55
2.7	Discussion	57
CHAPTER 3 – METHODOLOGY		58

3.1	Research Flow	58
3.2	Data Collection.....	59
3.2.1	Data Sampling.....	60
3.2.2	Primary Data Collection.....	61
3.2.3	Secondary Data Collection.....	61
3.3	Data Analysis	61
3.3.1	Data Collection	62
3.3.2	Data processing	63
3.3.3	Data analysis	63
3.4	Data Validation.....	63
CHAPTER 4 – DATA PROCESSING AND ANALYSIS		64
4.1	Data Collection.....	64
4.1.1	Data Collection Timeframe.....	64
4.1.2	Tools.....	64
4.1.3	Process	64
4.1.3.1	Sniffing in WLAN via Ethernet Bridging	65
4.1.3.2	Sniffing in WLAN using USB Wireless Adapter.....	66
4.1.3	Result	67
4.2	Data Processing	68
4.2.1	Tools.....	68
4.2.2	Data Processing Steps	69
4.2.2.1	Processing data with Network Miner, NetSleuth, Tshark, and CapLoader 69	
4.2.2.1.1	Network Miner.....	69
4.2.2.1.2	NetSleuth	73
4.2.2.1.3	CapLoader 1.2.....	74

4.2.2.1.4 Tshark	76
4.2.2.2 Processing Carved Data	76
4.2.3 Result and Analyses	76
4.2.3.1 Information Recovered	76
4.2.3.2 Information on Device Connected	80
4.2.3.2.1 By Total	80
4.2.3.2.2 Unique Device	81
4.2.3.3 Services Used	81
4.2.4 Observation	82
4.2.4.1 Finding and Evidences	82
4.2.4.2 Challenges	95
4.2.4.2.1 Data Collection	95
4.2.4.2.2 Data Processing	95
4.3 Discussion	98
CHAPTER 5 – CONCLUSION AND RECOMMENDATION	101
5.1 Conclusion	101
5.2 Recommendation	102
5.2.1 People	102
5.2.2 Process	103
5.2.3 Technology	105
5.3 Future Works	106
GLOSSARY	107
REFERENCE	110
APPENDIX	119
CURRICULUM VITAE	128

LIST OF FIGURES

Figures	Page
Figure 1.1 Indonesia Internet User Statistics by APJII.....	14
Figure 1.2 Fishbone Analysis.....	17
Figure 2.1 Architecture of Wi-Fi (Wang, 2009)	39
Figure 3.1 Research Flow	58
Figure 3.2 Data Analysis Flow	62
Figure 4.1 General Diagram of University Wireless Area Network.....	65
Figure 4.2 Setup in Ethernet	66
Figure 4.3 Processed Caps and Keyword search result	73
Figure 4.4 NetSleuth Processed Data.....	74
Figure 4.5 Sample Loaded <i>Pcap</i> Files in <i>CapLoader</i>	75
Figure 4.6 Keyword Search Process	75
Figure 4.7 Total Device Connected	80
Figure 4.8 Total Unique Devices Connected	81
Figure 4.9 Services Used	82
Figure 4.10 Clear text user name and password finding.....	84
Figure 4.11 Slides of School's Financial Document.....	85
Figure 4.12 Student Grading Score.....	85
Figure 4.13 Email Addresses of 2013 Graduates.....	86
Figure 4.14 Alumni Survey Result	86
Figure 4.15 Email content.....	87
Figure 4.16 Clients Summary Page.....	88
Figure 4.17 Client's Invoice Payment Page.....	88
Figure 4.18 Logged In Jobstreet Page of Someone	89

Figure 4.19 Gaming Market Page	89
Figure 4.20 User Google Search Page	90
Figure 4.21 HTTPS Warning	91
Figure 4.22 Instagram Timeline	92
Figure 4.23 Tumblr Timeline	92
Figure 4.24 Captive Portal Status	93
Figure 4.25 Logged Out Email	93
Figure 4.26 Logged In Wordpress Cookie	94
Figure 4.27 Group Photo	94
Figure 4.28 Private Photo	95
Figure 4.29 Manual Keyword Search	97
Figure 4.30 JSON File	97
Figure 4.31 Type of Information Exposed In Deliberate Breaches (Norton Cybercrime Index 2011)	99

SWISS GERMAN UNIVERSITY

LIST OF TABLES

Tables	Page
Table 2.1 Scholarly Articles on Information Leads to Identity Theft.....	29
Table 4.1 Summary of Data Collection Result	67
Table 4.2 Keywords	70
Table 4.2 Information Type Recovered	76

