# Abstracts

4th ICIBA

## 4th International Conference on Information Technology and Engineering Application

**February 20 - 21, 2015**

## IT & Engineering For a Better Life

**PALEMBANG - INDONESIA**

Hosted by

Universitas Bina Darma

In Cooperation with

UTM

Program Pascasarjana

epon : 0711-515679, 515582
: 0711-515582
osite : http://iciba.binadarma.ac.id
ail : iciba@binadarma.ac.id

# DISTRIBUTED PENETRATION OF WIRELESS PASSWORDS FOR WIRED PROTECTED ACCESS TYPE SECURITY

Taqrim Ibadi, Muhammad Izman Herdiansyah, Yesi Novaria Kunang

Universitas Bina Darma
taqrimibadi91@yahoo.com
m.izmanherdiansyah@mail.binadarma.ac.id
yesi_kunang@mail.binadarma.ac.id

Abstract

This research is a testing of the wireless password which types tested Security are WPA (Wired Protected Access). The issues raised are how influential the time of the many clients that perform password cracking from 2 clients to 10 clients and a password from 8 characters in length to 12 characters. This research uses experimental research methods that perform an experiment to see a result. That results would confirm how the position of the causal relationship between the variables researched, and using White Box as a test method. The results from this research would confirm that the increasing number of clients who make the process of the cracking password will be produced faster time to get the password from wireless devices that serve as target research.

Keywords: Cracking Password, Crunch, WPA



The 4th ICIBA 2015, International Conference on
Information Technology and Business Applications
Palembang-Indonesia, 20-21 February 2015

# DESIGN OF PORTABLE DIGESTER FOR DOMESTIC AND RESTAURANT ORGANIC SOLID WASTE PROCESSING AS CLEAN BIOGAS IN REPLACING LPG AS ALTERNATIVE ENERGY SOURCE

Agus Mansur[1], Agus Taufik[2], Dian Janari[3]

[1,2,3]Industrial Engineering Department,

Faculty of Industrial Technology,

Universitas Islam Indonesia

gus_mansur@uii.ac.id,ker_adian@gmail.com

Abstract

Fuel consumption that reaches 1,3 millions/barrel is unbalance with production that only reaches 1 million/barrel. Its shortage, hence, has to be fulfilled by importing. This research is designated to apply biogas technology in the form of applicative Portable Digester, suitable for public under good quality, reasonable price and applicable in limited area. Based on the research, the selected designs for Portable Digester to be assessed using Scoring concept are (a) design concept 2 that will later be applied as design A; (b) design concept 3 that will later be applied as design B; (c) design concept 5 that will later be applied as design C. The selected design concept is the concept E with score of 1,98.

Keyword: biogas, digester, portable digester

The 4th ICIBA 2015, International Conference on
Information Technology and Business Applications
Palembang-Indonesia, 21-22 February 2015

# DISTRIBUTED PENETRATION OF WIRELESS PASSWORDS FOR WIRED PROTECTED ACCESS TYPE SECURITY

Taqrim Ibadi, Muhammad Izman Herdiansyah,
Yesi Novaria Kunang

Universitas Bina Darma
Email: taqrimibadi91@yahoo.com
Email: m.izmanherdiansyah@mail.binadarma.ac.id
Email: yesi_kunang@mail.binadarma.ac.id

Abstract

This research is a testing of the wireless password which types tested Security are WPA (Wired Protected Access). The issues raised are how influential the time of the many clients that perform password cracking from 2 clients to 10 clients and a password from 8 characters in length to 12 characters. This research uses experimental research methods that perform an experiment to see a result. That results would confirm how the position of the causal relationship between the variables researched, and using White Box as a test method. The results from this research would confirm that the increasing number of clients who make the process of the cracking password will be produced faster time to get the password from wireless devices that serve as target research.

Keywords: Cracking Password, Crunch, WPA

## 1. INTRODUCTION

Wireless network technology is becoming very popular even though on the other side of this technology still has some problems with the security system. Based on the OSI reference architecture layer, wireless technology works at layer 2 and using the 802.11 protocol to the date data communication standard that is used generally is a family of IEEE 802.11a, 802.11b, 802.11g and 802.11n. Wireless technology can be seen in every aspect of human life starts from education, business, transportation, communication, and so forth. Computer, notebook, mobile phone (mobile phone) and PDA dominate usage of wireless technology. The wireless network is a wireless computer network technology that uses high frequency waves so that the computers can connect to each other without the use of wires and allow for users to perform data and voice communications with ease.

According by Efvy (2014) that, WEP (Wired Equivalent Privacy) is the first safety standard of wireless network created by using the RC4 encryption algorithm. This algorithm is simple and easy to implement because it does not require heavy computation, so it does not require sophisticated hardware. Although the WEP security method still has a lot of security holes, there are still many people who still use it. WPA (Wi-Fi Protected Access) or also known as WEP WEPv2 aka version 2, which was introduced in April 2003. The WPA is an improvement over WEP, so it is not a new security method, so that the weaknesses found in WEP still exist in where

the WPA encryption system used still apply RC4.

The latest generation of wireless security in this time that WPA / WPA2 PSK was still too vulnerable to dictionary attacks. The input required for this attack, with over four directions including WPA handshake between the client and the access point, and wordlist containing general passphrase. Then, using tools such as Aircrack-ng, can also solve the WPA / WPA2 PSK passphrase. The workings of WPA / WPA2 PSK is, came from each session key Pairwise Transient Key called (PTK), using Pre-Shared Key and five other Network SSID parameter, Authenticator Nounce (anounce), Supplicant Nounce (SNounce), MAC Authenticator (Access Point MAC), and the MAC address of the applicant (Wi-Fi MAC Client). This key is then used to encrypt all the data between the access point and the client. An attacker who hearing the whole conversation is that by monitoring the data packets through the air and can get all the five parameters mentioned in the previous statement.

Another opinion from the official site a password cracking software that is www.aircrack-ng.org stated limitations to perform brute-force techniques with a computer can only test 50-300 possible keys per second depending on the computer's CPU. Meanwhile, to make a large dictionary will be greatly needed a long time if it uses all the characters. Based on the previously mentioned some things about security, WPA can be attacked using brute-force techniques that 100% success rate, but it takes time and the device is not small, we conducted research in distributed wireless password cracking in the hope it would be to shorten the time in an attack. This technique is the review of the large number of the client as well as how long the password characters are used. Is said to be distributed as a union of elements systems communicate with each other will act wireless password cracking attack is jointly for one purpose to get a wireless password with WPA security type using a brute force attack.

Follow up the matter contained in the above background, the identification of issues to be raised in this research is focused on the type of WPA security passwords that can be attacked using brute-force techniques but it takes a long time if only using one device to attack with this technique.

In order to research more focused and not deviate from the existing problems, it is necessary to limit the problem. Boundary problem in this study is only a comparison of how much time we need to get the wireless security type WPA password using brute-force techniques in terms of how many clients are distributed and how long the characters for passwords used.

Based on the above, the authors formulate the problem in this study is how the influence of the number of clients who are used to the speed of cracking passwords in a distributed system.

The purpose of this research is to analyze the influence of the number of clients who used the speed of cracking passwords in a distributed system, so that produce the WPA password security profile.

## 2. RESEARCH METHODOLOGY

### 2.1. Research Methods Used

In this research, using experimental research methods of conducting an experiment to see some results. The results will confirm how the position of the causal relationship between the variables investigated / researched. According www.ut.ac.id, laboratory experiments in more "easily" done by because of the special facilities and the existence of a separate situation from outside interference, so that each variable can be manipulated based planning. Experimental research can be interpreted as the research methods used to search for a specific treatment effect against the other in uncontrolled conditions according Sugiyono (2012). Based on direct quotes from Zuriah (2006) that, the purpose of the research experiment is:

1. Test the hypothesis proposed in the research
2. Predicting event or occurrence in the experimental setting
3. Generalize the relationship between variables

2.2. Method Of Collecting Data

The data used in this study were divided into primary data and secondary data. To obtain the data used is done by:

1. Primery Data
   a. Observation and studied condition of the object of research. Data needed physical and non-physical form of data relating to the condition of the object of research networks.
   b. Experiment with scanning and network penetration experiments so get data for materials analysis.
2. Secondary Data
   The required data in the form of documents relating to the theme of the study by filing a petition to the authorities officially in the object of study.

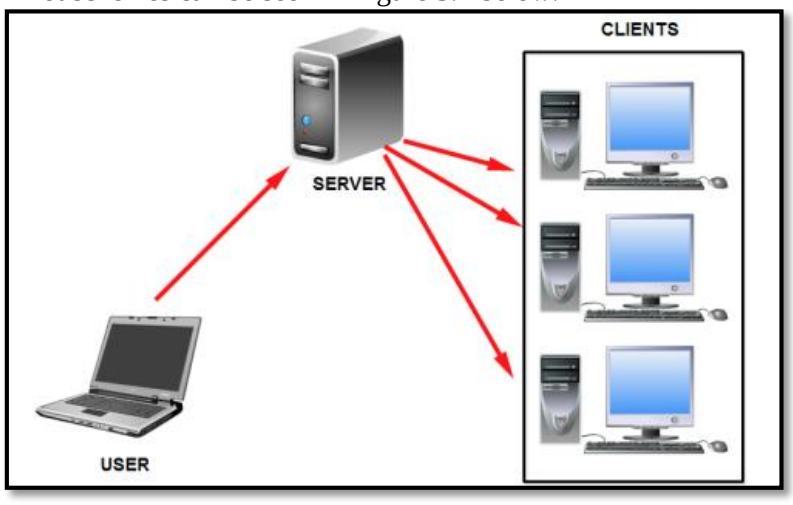
2.3. Data Analysis Methods

Methods in analyzing the data using methods Mile and Huberman include data reduction, data presentation and conclusion, A. Salim (2006):

1. Data reduction
   The data has been obtained from various sources are grouped according to categories of data preparation, assessment of data and data reporting.
2. Presentation of data
   Data that has been prepared in accordance with its type is then presented in the form of narrative text so as easy to make a conclusion.
3. Withdrawal Conclusion
   Making the conclusion of each category to draw overall conclusions of the research.

## 3. RESULTS AND DISCUSSION

To get maximum results and a structured and easy to understand, is needed a testing process scheme which aims to illustrate how the testing process takes place that facilitate research in action and analyze the results and for those who see the scheme without having to look directly at the time of their study can already imagine what it will be like that and the process rather than testing it like it is. Pilot schemes can be seen in Figure 3.1 below:




**Picture 3.1** Scheme Testing Process

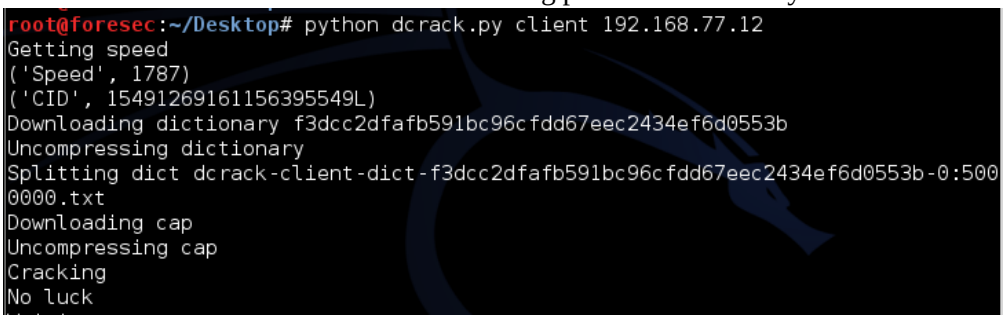
In accordance with the purpose of experimental the research of conducting an experiment to see some results, which confirms how the results will be a causal relationship between the variables investigated or researched as well as the conduct in accordance with the purpose of experimental research.

In a brute-force techniques needed a file that stores the possibility of passwords used by the owner of the access point device. to facilitate the the research then be made using the software

crunch that is already present on the operating system or Kali BackTrack Linux.

When the process of cracking the password on the client have been run there will be a notification on the client terminal window if successfully found the password of the target device or not. If the password cracking process is successful then the password of the device will be listed in the terminal window, and if it fails then there is a client terminal window will be writing no luck as seen in the picture 3.2 and 3.3 below.


Picture 3.2 Password cracking process successfully




Picture 3.3 Password cracking process fails

Test data to cracking passwords is presented in tabular form as a visual to show that the time required to perform this action more and more clients in a distributed password cracking the time produced fewer and faster in the process of getting the password of the target wireless device such that seemingly on the table 3.1.

Tabel 3.1 Testing Results

| Type Password | Total Clients | Capture File Size | Password File Size | Time Testing |
|---|---|---|---|---|
| Numbers | 2 | 70.9 MB | 858 MB | 7h 46m |
| | 4 | 70.9 MB | 858 MB | 3h 53m |
| | 8 | 70.9 MB | 858 MB | 1h 56m |
| | 10 | 70.9 MB | 858 MB | 1h 33m |

Tests conducted on the type of passwords starting from numbers, letters of the alphabet, alphabet uppercase and lowercase letters, uppercase letters lowercase letters of the alphabet and numbers, and the alphabet uppercase lowercase letters plus numbers and symbols. After testing the results obtained only limited types of passwords numbers only with a password length of 8 characters not to test 12 characters. It is based due to the limitations of software testing and the research tools used so that the time needed for this study does not allow resolved in a little time. Given the limitations of the device and knowledge in the research, then the research has not been able to continue in the near future.

Limitations than dcrack.py script capability is becoming one of the factors inhibiting the research should be discontinued as seen in the picture 3.4 which shows that the terminal window there is a notification server error occurred on several lines of program syntax and too long delivery process dictionary password from the user to the server cause over flow error in the shipping process.


Picture 3.4 The process of sending the password dictionary server error

This occurs because the file is sent exceeds the capacity contained in scrypt python and delivery time exceeds the maximum limit as well as the limitations of server memory is not sufficient as a first capacity in the delivery process.

## 4. CONCLUSION

From the results of wireless penetration password conducted in this study, obtained some conclusions as follows:

1. After the test is done to see the comparison between time, the number of clients and the length of passwords used the results as the initial hypothesis that the increasing number of clients and the shorter the length of passwords used in the process of cracking the passwordthen time required will be less too, so the opportunity to obtain a password more quickly and accurately, it is clarified on the tables 3.1 test results.
2. Character password and the password length affects the size of the dictionary file password. So much attention to the category and length of the password that will be used in the manufacture of dictionary words.

## References

Salim, A. (2006). Teori dan Paradigma Penelitian Sosial. Yogyakarta: Tiara Wacana.

Sugiyono. 2012. Metode Penelitian Kombinasi (Mixed Methods). Bandung: Alfabeta , hal. 109.

Zam, Efvy Zamidra. 2014. Cara Mudah Membuat Jaringan Wireless. Jakarta: PT.Elek Media Komputindo.

Zuriah, Nurul. 2006. Metodologi Penelitian Sosial dan Pendidikan. Jakarta: Bumi Aksara, hal. 58.

Software aircrack (http://www.aircrack-ng.org/doku.php?id=cracking_wpa, accessed on Januari, 5th, 2015)

Teori Eksperimental (http://www.ut.ac.id/html/suplemen/espa4315/Penelitian%20Eksperimental.htm, accessed on November 5th, 2014)