**Final Paper Proposal Lloyd Jones**

**ITEC-451 4.10.2014**

INTRODUCTION

In an attempt to cater to non-technical users, most consumer and small business wireless routers include a feature known as Wi-Fi Protected Setup, or WPS. Developed by the Wi-Fi Alliance, this feature enables users to connect a wireless device to an access point by pushing a button or entering a PIN number, as opposed to remembering a typically long or difficult to memorize passphrase. The weak security of the WPS protocol is already well-known and has been documented by multiple individuals. Additionally, tools have been developed to automate the exploitation of this technology. The goal of this paper is to examine the timeout and lockout mechanisms that some routers employ and determine their overall effectiveness in delaying brute-force attacks on the WPS protocol. Using Markov chains, we can model the probability of a successful attack at different stages of the WPS authentication process. We can then make a decision as to which method produces the best results. This topic is interesting because of the fact that WPS is so widely deployed despite its inherent security weaknesses. Also, I have not found any studies concerning brute-force mitigations mechanisms in wireless routers.

PROBLEM STATEMENT

Each stage of the WPS authentication process presents a fixed probability of a host guessing the information needed to proceed to the next stage. Modeling these probabilities with Markov chains, we can visually understand how this works. Afterwards, we can choose different delay values and calculate the probability of a successful attack given a certain amount of time. For example, we can show the probability of a successful attack taking place within five hours given an access point lockout of 60 seconds, a PIN verification time of 4 seconds per PIN, and a lockout of 60 seconds per 3 failed PIN attempts.

LITERATURE SURVEY

The WPS standard was originally published in December of 2006 [1] and has been implemented in wireless routers sold by a wide array of manufacturers. Securing devices such as these can seem intimidating to end users, so the WPS protocol was established to meet this need. In December of 2011, Stefan Viehboch came across a vulnerability in the implementation of WPS which allowed the brute-forcing of the WPS PIN, a required feature of this specification. WPS is usually enabled by default on routers that support it. Even worse, some devices do not offer the options to disable it. Others allow the user to disable WPS but don’t actually turn it off at all.

The aforementioned attack is made possible by a weakness in PIN validation between the enrollee, or client device requesting access, and the registrar, or the device providing wireless settings to the enrollee. The format of the PIN is shown below [3]:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | Checksum |
| First half of PIN | | | | Second half of PIN | | | |

Figure 1. <Please give a title of this figure>

Ideally, this numeric implementation should allow for 107 PINs, but instead the PIN is split into two halves and each one is verified separately. This behavior is shown in the M4-M7 messages included in the WPS specification document [2].

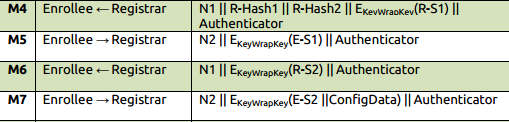


Figure 2. <Figure Title>

This detail drastically reduces the amount of possible PINs from 107 (10,000,000) to 104 + 103 (11,000). If the correct PIN is found, the registrar will provide the enrollee with the WPA/WPA2 encryption key.

As stated above, some of these devices include a timing delay or lockout after a PIN has been incorrectly entered a certain number of times. This functionality is not documented or required by the WPS specification. Additionally, router manufacturers do not include information about these mechanisms online or elsewhere. Devices can have no delay, a static delay, an incremental delay, or total lockout. Brute-force attempts may also be influenced by other factors as well, including signal strength, interference, access point load, and client wireless interface limitations. We will examine multiple scenarios and attempt to model reasonable values for each of these variables.

PROBLEM-SOLVING APPROACH

The approach used to solve this problem will be to first model the probabilities of each PIN half being successfully guessed. Afterwards, we will examine and document commonly observed lockout mechanisms in consumer wireless routers. We will then compute and graph the success percentages of brute-force attacks against WPS in each system. We can then compare and contrast the various approaches.

TIMELINE

* April 11 – Submit proposal.
* April 11-13 – Research common router lockout and delay periods. Model Markov chains.
* April 13-17 – Perform experiments and computations. Analyze and graph results.
* April 17-20 – Write paper detailing work in IEEE transaction format.
* April 20-25 – Create presentation slides of work done.
* April 26 – Submit final paper and presentation.
* April 30- May 2 – Give presentation to class.

REFERENCES

1. Wi-Fi Alliance, “Wi-Fi Protected Setup Specification,” pp.34, December 2006.
2. S. Viehbock, “Brute forcing Wi-Fi Protected Setup,” pp.2-9, Dec. 2011.
3. D. Sora, “Wi-Fi Protected Setup – Security Enhancement or Threat?,” pp.1-5, Nov. 2013.