Universidade Federal de Pernambuco

Graduação em Ciência da Computação

Centro de Informática

2017.1

Uma Técnica de Identificação de Pontos de Acessos Falsos ou Maliciosos

Proposta para Trabalho de Graduação

Aluno: Caio César Leão Carneiro de Araújo (cclca@cin.ufpe.br)
Orientador: Paulo André da Silva Gonçalves (pasg@cin.ufpe.br)

Recife – Abril de 2017

1. Resumo

Na segunda metade da primeira década dos anos 2000, houve um grande boom na utilização da Internet. De 2007 para 2008, o número de usuários cresceu de 15 milhões para 22 milhões no Brasil, segundo um levantamento feito pelo Ibope/Netratings. O modo como a conexão sem fio é estabelecida atualmente é bastante vulnerável a ataques de pontos de acesso falso. Onde o atacante muda as configurações do roteador a ser usado no ataque para as mesmas da rede a ser atacada, copiando o Service Set Identifier (SSID) e o endereço MAC (Medium Access Control) para serem as mesmas configurações do ponto de acesso alvo. Como a escolha do ponto de acesso é baseada no SSID e na força de sinal, se o atacante possuir um sinal mais forte que o sua vítima, a mesma se conectará ao ponto de acesso falso sem saber que o mesmo é falso, pois ele responde todas as solicitações da mesma forma que o ponto original responderia e possui as mesmas configurações de identificação (SSID e endereço MAC). Um ataque simples e relativamente barato o qual pode ser feito tanto em residências quanto em ambientes executivos. Somando isso ao fato de que cada vez mais pessoas realizam operações envolvendo informações sensíveis pela Internet, desde de mensagem a familiares a operações envolvendo senhas de bancos e números de cartões, temos uma noção da escala do problema que uma vulnerabilidade como essa pode causar. Existem várias técnicas de identificação de pontos de acesso falsos. Dentro das várias técnicas que existem, este TG irá estudar e avaliar técnicas que identificam o ponto de acesso baseado no desvio de relógio dos APs, a qual é bastante promissora.

Palavras Chave: Ponto de Acesso, desvio de relógio, rede sem fio, detecção, segurança de redes.

1. Abstract

On the second half of the first decade of the year 2000's, there was a major increase in the number of internet users. From 2007 to 2008, the number of users in Brazil alone grew from 15 million to 22 million, according to data raised by Ibope/Netratings. The way wireless Internet connections are currently established are extremely vulnerable to Rogue AP (Access Point) attacks. In this attack, the attacker changes the configuration of his own Access Point in order to match the victim's, copying it's Service Set Identifier (SSID) and it's Medium Access Control (MAC). As the choice of Access Point is determined by the SSID, MAC and strength of signal, the victim's computer connects to the fake access point and because the fake access point responds normally as the original would, the victim's computer doesn't detect that the access point it's connected is a rogue one. A simple and relatively cheap attack that can be made to homes or corporations. Add that to the fact that users are realizing operations that involve more and more sensitive information, such as credit card numbers, business plans and meetings to even intimate and personal information. That being said we now have a more complete understanding of the problem's scale. There are various techniques that can be use as means of defense, and in this thesis we will analyze one that uses a digital fingerprint based on the access point's clock skew using different algorithms to estimate said skew through data that's acquired on Beacon and Probre Frames.

Keywords: Access Point, clock skew, wireless network, detection, network security.

2. Contexto

A Internet começou a se tornar acessível para o público geral por volta dos anos 90, deixando de ser um mercado de nicho onde apenas os entusiastas ou pesquisadores tinham acesso a mesma. Devido a facilidade de uso e de toda a comodidade que ela trazia, pessoas e empresas começaram a adotar a Internet e após algum tempo, começaram a fazer cada vez mais operações usando as mesmas. Inicialmente tendo apenas sites que serviam de banners e usados para expor seus trabalhos a salas de bate papo enquanto hoje temos empresas que tem seu modelo de negócio inteiramente baseado na Internet. Não houve apenas um grande aumento na quantidade de informação na rede, mas temos cada vez mais informações sensíveis. Conversas particulares, negociações, dados sensíveis, todos os tipos de dados são hoje guardados na Internet. Com esses tipos de dados agora na rede, era apenas uma questão de tempo até pessoas com más intenções começarem a usar brechas de segurança na mesma.

Com o passar do tempo, a segurança da rede foi evoluindo e se tornando cada vez mais sofisticada, e os ataques também. O estabelecimento de padrões como o protocolo IEEE 802.11 [2] foi uma faca de dois gumes, fazendo com que o funcionamento e a comunicação melhorasse, mas criando um ponto único de falha, pois uma brecha na segurança do protocolo significa que todos que o utilizam estão em risco de abuso da mesma brecha. E atacantes não perderam essa chance, criando o ataque conhecido como Ataques de Ponto Acesso Falso. Métodos para contra-atacar essa abordagem de ataque estão sendo pesquisados e desenvolvidos, entre eles temos a Verificação de Identidade, Monitoramento de Tráfego, Tempo de Viagem de Pacotes, Intensidade de Sinal Recebido até o cálculo de desvio de relógios[1]. O intuito desse projeto é analisar o método de desvio de relógio e verificar a quantidade de recursos (pacotes) que são necessários para a identificação do ponto falso ou a confirmação do ponto real, assim como a acurácia no cálculo de estimativa do desvio de relógio.

3. Objetivos

Este trabalho tem como objetivo replicar métodos de cálculo de desvio de relógio baseado em informações adquiridas através de pacotes obtidos em uma rede, utilizando o adaptador wireless TP-Link TL-WN722N e uma versão modificada do driver do mesmo para aumentar a granularidade do timestamp dos quadros probes e beacon a serem obtidos, consequentemente aumentando a precisão dos métodos mencionados.

O Projeto é dividido em quatro etapas, a fase de coleta, onde os pacotes serão coletados usando o adaptador wireless com o driver modificado, a separação onde os dados são separados por ponto de acessos real e falso para um ambiente de testes controlado, a análise onde o resultado dos métodos implementados para a identificação do ponto de acesso falso será inspecionado e a quarta e última é a comparação, onde será feita a comparação entre resultado dos diferentes métodos implementados. Melhorias e diferente versões desses métodos serão implementadas e comparadas ao original, usando os mesmos dados para verificar a viabilidade de tais melhorias e se elas de fato são uma melhoria. Também será discutido se, caso haja melhorias, elas são viáveis pois as mesmas podem exigir um número maior de pacotes até a convergência na previsão do desvio de relógio e mais tempo de processamento.

4. Cronograma

Atividade	Abril				Maio				Junho			
	1ª sem.	2ª sem.	3ª sem.	4ª sem.	1ª sem.	2ª sem.	3ª sem.	4ª sem.	1ª sem.	2ª sem.	3ª sem.	4ª sem.
Revisão Bibliográfica	X											
Projetar Ferramenta		X										
Implementação da Ferramenta			X	X	X	X						
Planejar e Realizar Experimentos							X	X	X	X		
Avaliar Resultados											X	
Escrever TG						X	X	X	X	X	X	
Revisão e Correção do TG											X	X

5. Bibliografia

[1] Emanuel Felipe dos Santos. Aplicação de desvio de relógio como fingerprint para a identificação de ponto de acesso falso. Centro de Informática, Universidade Federal de Pernambuco.
[2] IEEE 802.11 Working Group. < http://www.ieee802.org/11/ >. Acessado em 04 de Abril de 2017

5. Possíveis Avaliadores

São possíveis avaliadores do trabalho a ser produzido conforme especificado nesta proposta:

- Prof.º Sérgio Soares, Centro de Informática - UFPE, Recife
- Prof.º Silvio de Barros Melo, Centro de Informática - UFPE, Recife
- Prof.º Carlos André Guimarães Ferraz, Centro de Informática - UFPE, Recife

6. Assinaturas

DADOS DO ALUNO

NOME: Caio César Leão Carneiro de Araújo
MATRÍCULA: 09719355484
e-mail: cclca@cin.ufpe.br
Telefone(s) p/ contato: (81) 9 9858 0021

CIENTE DO ORIENTADOR

NOME: Paulo André da Silva Gonçalves