Universidade Federal de Pernambuco

Graduação em Ciência da Computação

Centro de Informática

2016.1

Aplicação de desvio de relógio como fingerprint para a identificação de ponto de acesso falso

---

Proposta de Trabalho de Graduação

Aluno: Emanuel Felipe dos Santos (efs4@cin.ufpe.br)

Orientador: Paulo André da Silva Gonçalves (pasg@cin.ufpe.br)

Recife, 14 de Abril de 2016

Sumário

Contexto 3
Objetivos 4
Cronograma 5
Possíveis Avaliadores 5
Referências 6
Assinaturas 7

Contexto

Com o impressionante crescimento da internet, o que começou a ser experimentado a partir do final dos anos 80 e com a expansão da sua comercialização, o número de dispositivos que podem se conectar a internet chegou a um nível em que a atual infraestrutura de rede seus protocolos, à princípio, não foram desenvolvidos para funcionar.

A crescente necessidade de troca de informação de maneira rápida, móvel e eficiente, como também a grande demanda por serviços ubíquos[1], fez com que as redes Wi-Fi, que são as que seguem o protocolo IEE 802.11 [3], se tornassem uma necessidade na sociedade atualmente. Porém devido a sua importância em prover um serviço ubíquo de qualidade e também pela inerente vulnerabilidade de redes sem fio, devido ao sua natureza de difusão, as redes sem fio locais (WLAN) tem se tornado alvos de uma variedade de ataques [1].

Uma das formas em que as redes locais sem fio podem ser atacadas, é através da instalação de um ou mais pontos de acesso falsos. Esses pontos de acesso podem adotar as mesmas configurações, Service Set Identifier (SSID), Medium Access Control (MAC) e Basic Service Set Identifier (BSSID), do ponto de acesso (AP) original e evitar identificação utilizando diferentes características de canal físico. Assim, um usuário qualquer pode se conectar ao ponto de acesso falso sem perceber que ele não é autorizado, justamente pelo fato do ponto de acesso falso responder todas as solicitações que foram feitas da mesma forma que o ponto de acesso original responderia.

Dessa maneira, existem diversos algoritmos na literatura que utilizam diversos mecanismos para a detecção de pontos de acesso falsos [1] [2], como a Verificação de Identidade, Monitoramento de Tráfego, Tempo de Viagem de Pacotes, Intensidade de Sinal recebido e cálculo de desvo de relógios[1]. Além disso, existe a possibilidade da localização e desativação física do ponto de acesso falso

Objetivos

O objetivo geral deste Trabalho de Graduação é a especificação e a réplica da implementação de algoritmos já conhecidos, com possíveis melhorias, para a identificação de pontos de acesso falsos utilizando desvios de relógios como fingerprints.

Cronograma

	Prazo															
Entrega	***Abril***				***Maio***				***Junho***				***Julho***			
Proposta Inicial																
Revisão da Literatura																
Implementação dos Algoritmos																
Coleta, Separação, Analise e Comparação																
Elabroração do Relatório																
Apresentação																

Possíveis Avaliadores

Os possíveis avaliadores para o resultado a ser obtido ao final de todas as etapas da proposta descrita neste documento são:

- Carlos André Guimarães Ferraz (cagf@cin.ufpe.br)
- José Augusto Suruagy Monteiro (suruagy@cin.ufpe.br)

Referências

[1] Jana, S.; Kasera, S.K., "On Fast and Accurate Detection of Unauthorized Wireless Access Points Using Clock Skews," Mobile Computing, IEEE Transactions on, vol.9, no.3, pp.449,462, March 2010.

[2] Arackaparambil, Chrisil; Bratus, Sergey; Shubina, Anna; and Kotz, David. 2010. On the reliability of wireless fingerprinting using clock skews. In Proceedings of the third ACM conference on Wireless network security (WiSec '10). ACM, New York, NY, USA, 169-174.

[3] Kurose, James F; Ross, Keith W., Redes de computadores e a Internet: uma abordagem top-down, 5. ed., São Paulo : Addison Wesley, 2010.

Assinaturas

_____

Paulo André da Silva Gonçalves
Orientador

_____

Emanuel Felipe dos Santos
Orientando