UM ESTUDO SOBRE TÉCNICAS DE DETECÇÃO DE PONTOS DE ACESSO FALSO

ALUNO: ANTONIO NÓBREGA
ORIENTADOR: PAULO GONÇALVES

02 DE OUTUBRO DE 2015

CONTEÚDO

1. CONTEXTO

Com o avanço de micro-tecnologias e redes sem fio, cada vez mais sistemas móveis estão sendo conectados à internet [5]. Juntando esse fato a grande demanda por sistemas ubíquos, o número de dispositivos do nosso dia a dia que estão utilizando de redes sem fio, incluindo as redes que seguem o protocolo IEEE 802.11, cresceu muito nos últimos anos. Esse crescimento faz com que cada vez mais, atacantes aproveitem-se do fato de essas redes sem fio utilizarem o ar como meio de propagação. Esse evento possibilita que qualquer usuário que esteja nas proximidades de uma rede sem fio, possa tornar-se um potencial atacante. Aliado à isso, há um crescimento na quantidade de tráfego de informações sensíveis nas redes locais sem fio (*wireless local area networks, WLANs*), e tudo isso gerou um aumento do número de ataques a redes sem fio nos últimos anos.

Um dos possíveis ataques a uma WLAN é a instalação de um Ponto de Acesso (*Access Point, AP*) falso. Um AP falso pode ser facilmente instalado apenas com o atacante clonando o SSID(Service Set Identifier), o BSSID (Base Set Service Identifier) e o endereço MAC (medium access control) do AP original. Há também uma grande quantidade de ferramentas que tornam a criação de um AP falso uma tarefa trivial, bastando que o atacante selecione a rede que o mesmo deseja invadir para que o objetivo seja praticamente alcançado. O invasor tem o objetivo de instalar um AP falso pois os usuários se conectarão à ele, acreditando que estão conectando-se ao AP original. Caso o usuário se conecte ao AP falso, uma variedade de ataques pode ser feitas contra o usuário, comprometendo assim a segurança da comunicação sem fio.

Existe um aprimoramento do protocolo IEEE 802.11, o 802.11i RSNA (*Robust Security Network)* que utiliza métodos tradicionais de criptografia para prover uma autenticação mútua e segura entre os clientes e os APs, mas essa solução ainda possui falhas que fazem com que a criação de um AP falso ainda seja possível. Há diversos algoritmos na literatura que utilizam outros mecanismos para a detecção de APs falsos [1,6,7,8,9,10]. Dentre esses algoritmos, o método utilizado por [1] mostrou-se uma técnica interessante e atual que utiliza um procedimento para calcular o desvio do relógio *(clock skew)* a partir da captura de *beacons* do AP, para fazer um fingerprinting do ap, o objetivo deste trabalho é implementar essa técnica.

2. OBJETIVOS

O objetivo principal deste trabalho é o de avaliar soluções propostas na literatura para detecção de Pontos de Acesso falso e implementar a solução proposta por [1]. Para atingir esse objetivo o driver da placa wireless terá que ser modificado para capturar desvio do relógio. Para fazer essa modificação, o driver *Backports* [2] para o linux será utilizado. O sistema operacional usado foi o Kubuntu 14.04.

Com o driver modificado, a solução proposta possui quatro fases distintas a serem executadas. A primeira fase, a fase de coleta de dados será feita usando o pacote *aircrack* [3] que contém o programa *airmon-ng* [4] e a ferramenta *tshark* para capturar os pacotes enviados pelo AP.

As fases de separação, análise e comparação dos dados serão executadas com o auxílio de um software escrito em C++.

3. CRONOGRAMA

ATIVIDADES	OUTUBRO		NOVEMBRO		DEZEMBRO	
Estudo da bibliografia						
Estudo dos conceitos e metodologia usado na solução						
Documentação e Modificação do Hardware necessário						
Implementação da solução						
Elaboração do Relatório e da Apresentação						

4. REFERÊNCIAS

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

[2] Backports.wiki.kernel.org, 'Driver Backports Wiki', 2015. [Online]. Available: https://backports.wiki.kernel.org/index.php/Main_Page. [Accessed: 29- Dec- 2015].

[3] Aircrack-ng.org, 'Aircrack-ng', 2015. [Online]. Available: http://www.aircrack-ng.org/. [Accessed: 29- Sep- 2015].

[4] Aircrack-ng.org, 'airmon-ng [Aircrack-ng]', 2015. [Online]. Available: http://www.aircrack-ng.org/doku.php?id=airmon-ng. [Accessed: 29- Sep- 2015].

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

[6] L. Ma, A. Teymorian, X. Cheng, and M. Song, “RAP: Protecting Commodity Wi-Fi Networks from Rogue Access Points,” Anais da Fourth International Conference on Heterogeneous Networking for Quality, Reliability, Security and Robustness & Workshops. ACM, 2007, pp. 1–7.

[7] W. Wei, K. Suh, B. Wang, Y. Gu, J. Kurose, and D. Towsley, “Passive online rogue access point detection using sequential hypothesis testing with TCP ACK-pairs,” in IMC 2007.

[8] Taebeom Kim; Haemin Park; Hyunchul Jung; Heejo Lee, "Online Detection of Fake Access Points Using Received Signal Strengths," Vehicular Technology Conference (VTC Spring), 2012 IEEE 75th , pp.1,5, 6-9 May 2012

[9] 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.

[10] Hao Han; Bo Sheng; Tan, C.C.; Qun Li; Sanglu Lu, "A Measurement Based Rogue AP Detection Scheme," INFOCOM 2009, IEEE , pp.1593,1601, 19-25 Abril 2009.

5. Possíveis Avaliadores

Carlos Ferraz – cagf@cin.ufpe.br

José Augusto Suruagy – suruagy@cin.ufpe.br

Ruy de Queiroz – ruy@cin.ufpe.br

6. ASSINATURAS

Antonio Marino da Nóbrega Gomes

Aluno

Paulo André da Silva Gonçalves

Orientador