Fênix Firewall System
Um Firewall Pessoal Sensível ao Contexto para Dispositivos Móveis

Marcos Alves Trindade de Azevedo, Vagner José do Sacramento Rodrigues

[1] Instituto de Informática – Universidade Federal de Goiás
Caixa Postal 131 - CEP 74001-970 - Goiânia - GO

marcos@digitalsec.com.br, vagner@inf.ufg.br

Resumo. *A segurança de dispositivos móveis está se tornando rapidamente parte integrante de uma estratégia completa de segurança. O uso de um firewall pessoal que ofereça mecanismos de defesa em tempo real contra ameaças emergentes que atingem smartphones e outros dispositivos móveis imprescindível contra invasões, vazamento de dados e perda de produtividade. Este artigo descreve a arquitetura de de um firewall sensível ao contexto para dispositivos móveis, codinome Fênix Firewall, que vai além dos sistemas tradicionais de firewall, por se utilizar da localização do usuário para carregar as políticas de segurança de acordo com suas preferências. Para isso, o Fênix Firewall toma medidas de segurança baseado em políticas predefinidas, gerenciando as preferências do usuário segundo a sua localização corrente e o alertando quanto a potenciais perigos.*

1. Introdução

Os últimos anos têm presenciado um movimento de mudança do paradigma de computação *desktop*, tradicionalmente estático, para um novo paradigma, altamente dinâmico, caracterizado pelo emprego de novos dispositivos portáteis multifuncionais – que substituem as agendas, telefones, pagers ou um computador pessoal – e pela constante mudança no ambiente, como conseqüência da mobilidade do usuário. Esse novo paradigma, o da **Computação Ubíqua** (*Ubiquitous Computing*), traz consigo a possibilidade de se explorar uma nova geração de aplicações, sensíveis ao contexto (*Context-Aware Applications*), em que a interação usuário-aplicação é enriquecida pela percepção e uso de informações contextuais. Essas aplicações levam em consideração na sua tomada de decisão e em seus processamentos não apenas as entradas explícitas, mas também entradas implícitas, provenientes do contexto físico e computacional do ambiente e de seus usuários. O termo *Computação Ubíqua* foi introduzido por Mark Weiser [Weiser 1993], quando vislumbrou ambientes acrescidos de recursos computacionais capazes de prover serviços e informações quando e onde sejam desejadas. De acordo com Weiser, deve haver integração contínua entre tecnologia e ambiente de modo a auxiliar os usuários em atividades cotidianas; portanto, computadores devem ser embutidos de forma implícita ao ambiente do usuário.

Contudo, a facilidade de mobilidade proporcionada pelos dispositivos móveis os tornam cada vez mais vulneráveis a ataques, pois não há uma fronteira bem definida do perímetro que representa uma ameaça para o usuário final. O dispositivo móvel de um usuário pode ser alvo de ataques em diferentes ambientes e circunstâncias, por exemplo, no seu trabalho, no shopping, em uma festa, etc. Isto ocorre, principalmente, porque muitos dos dispositivos móveis tais como Smartphones tem suas interfaces de rede sem fio (*e.g., Bluetooth, WiFi*) habilitadas por padrão, e nem sempre os usuários sabem desabilitar

tais interfaces ou restringir o acesso a um serviço executando em seu dispositivo. Tudo isto representa ameaças a privacidade dos usuários e a confidencialidade das informações armazenadas em seu dispositivo móvel.

Para auxiliar os usuários a configurar suas políticas de segurança em função de sua localização corrente, é proposto neste trabalho um firewall pessoal chamado *Fênix Firewall System*. Este firewall pode impedir o acesso de pessoas não autorizadas e evitar que informações sejam extraídas através da exploração de serviços que estão em execução. O **Fênix Firewall System** foi projetado como um firewall pessoal que, quando instalado e configurado no dispositivo móvel, aumenta o nível de segurança e o controle do usuário, bloqueando ou permitindo as conexões (entrantes/saintes) e notificando o usuário sobre conexões, portas abertas ou serviços suspeitos que estejam em execução no dispositivo móvel.

O restante deste artigo está organizado da seguinte forma: a Seção 2 apresenta uma visão geral da arquitetura do Fênix Firewall; a Seção 3 apresenta a plataforma embarcada e seus componentes internos; a Seção 4 descreve a implementação realizada; a Seção 5 mostra um estudo de caso em um ambiente universitário; a Seção 6 descreve brevemente alguns trabalhos relacionados e a Seção 7 conclui o artigo, apresentando considerações finais e perspectivas de trabalhos futuros.

2. A Arquitetura do Fênix Firewall

3. O Projeto da Plataforma Embarcada

4. Implementação

5. Estudo de Caso

6. Projetos Relacionados

7. Conclusões e Trabalhos Futuros

Referências

Chaokai, H. (2007). Design and implementation of a personal firewall based on ndis intermediate drivers. *Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing*.

Cremonini, M., Damiani, E., di Vimercati, S. D. C., and Samarati, P. (2004). An xml-based approach to combine firewalls and web services security specifications. *Universitá di Milano - Italy*.

Hager, C. T. R. (November, 2004). Context aware and adaptive security for wireless networks. *Virginia Polytechnic Institute and State University*.

Qiu, Y., Zhou, J., and Bao, F. (2004). Design and optimize firewall for mobile networks. *IEEE Vehicular Technology Conference*.

Silberschatz, A., Galvin, P. B., and Gagne, G. (2005). *Operating system concepts. 7.ed.* Hoboken: Wiley.

Sinha, A. and Chandrakasan, A. (San Jose, November, 2001.). Energy efficient real-time scheduling. *International Conference on Computer Aided Design (ICCAD)*.

Snekkenes, E. (2001). Concepts for personal location privacy polices. *Norwegian Computing Center*.

Tan, H. C., Zhou, J., and Qiu, Y. (2007). A mobile firewall framework - design and implementation. *WCNC 2007 - IEEE Communications*.

Weiser, M. (1993). Hot topics: Ubiquitous computing. IEEE Computer.