Escola Politécnica da Universidade de São Paulo

Segurança em Redes de Dados sem Fio

Caio Augustus Morais Bolzani
© 2004 – caio@bolzani.com.br

Nos últimos anos, a comunicação sem fio ganhou um espaço considerável no mercado de transmissão de dados, deixando de existir apenas nas comunicações de longa distância através de satélite, para fazer parte de ambientes locais. Essa tendência foi fortalecida pelo investimento de instituições e empresas no sentido de aplicar a transmissão sem fio em redes de computadores. Um padrão amplamente adotado é o IEEE 802.11b, também conhecido como Wi-Fi (Wireless Fidelity), que permite a interconexão de computadores a uma taxa de 11 Mbps. Em um ambiente de redes de dados com características pervasivas, muitas soluções podem ser usadas para possibilitar a comunicação entre dispositivos inteligentes, eliminando os fios e tornando mais flexível e prático o uso desses equipamentos. Outras gerações de Wi-Fi (a,g,i), Bluetooth e ZigBee são outros exemplos dessas soluções [2].

Há uma tendência moderna de se implantar cada vez mais as redes sem fio em ambientes desse tipo, motivada pela facilidade da instalação e, muitas vezes, pela inviabilidade do uso de redes cabeadas. Outros fatores relacionam-se com a mobilidade e flexibilidade que as comunicações sem fio oferecem e pelo barateamento dos equipamentos. A adoção vem crescendo significativamente em ambientes corporativos, comerciais e residenciais e muitas soluções de WLANs (Wireless Local Area Networks) são muito apropriadas para a interligação de dispositivos inteligentes e na implementação dos ambientes denominados pervasivos. Isso indica, sem dúvida, que as redes de computadores sem fio são uma realidade e, provavelmente, nos próximos anos, substituirão grande parte dos sistemas cabeados existentes.

A tecnologia sem fio não é recente, mas seus produtos caros e sua baixa taxa de transferência inviabilizaram seu uso no passado. Uma WLAN converte pacotes de dados em ondas de rádio ou infravermelho e os envia para outros dispositivos ou para um ponto de acesso que serve como uma conexão para uma LAN cabeada. Locais onde não existe a possibilidade de se transpassar fios como construções antigas ou tombadas são fortes candidatos a usarem estas soluções.

A WECA (Wireless Ethernet Compatibility Alliance) é uma organização independente que monitora os fabricantes de dispositivos WLAN, atribuindo o rótulo Wi-Fi a todas as entidades que cumpram as normas estabelecidas pela IEEE 802.11b. Atualmente, existem centenas de produtos certificados, o que representa um leque bastante variado de opções para os que querem escolher uma solução deste tipo. Como resultado, os equipamentos passaram a custar cerca de um terço do preço de três anos atrás.

Por outro lado, o problema da segurança é um ponto crucial na escolha de redes de sem fio em aplicações críticas ou que necessitam de privacidade. Com a digitalização de todas as informações, não seria interessante deixá-las escapar, literalmente, pela janela. Alguns protocolos de segurança e sistemas de criptografia estão sendo emprestados das redes cabeadas e muitos outros estão sendo criados para suprir as necessidades das redes e dispositivos sem fio. A mobilidade desses aparelhinhos também cria um enorme gama de problemas e vulnerabilidades que estão sendo analisadas atualmente.

Segundo S. Ravi et. al [1], existem alguns desafios na implementação de sistemas de segurança nestes dispositivos móveis e são denominados de *Wireless Security Gaps*. Os principais são o baixo poder de processamento destes equipamentos, insuficiente para manejar todo os cálculos matemáticos necessários pelos sistemas criptográficos. Outro fator preponderante é a pequena capacidade da bateria para lidar com esse substancial aumento de processamento. O incremento de carga tem sido de 5 a 8% ao ano o que deve ser, em breve, um empecilho para a implementação de sistemas de segurança nestes dispositivos. Porém, diante de todo esse emaranhado tecnológico de segurança de dados, manter a flexibilidade do funcionamento de um dispositivo móvel em frente a toda a avalanche de algoritmos de segurança e tipos de rede deve ser outro desafio dos projetistas, bem como prever e prover métodos para que todo esse aparato não seja destruído se, por ventura, tais equipamentos sejam utilizados por pessoas não autorizadas (em caso de roubo do celular ou palmtop, por exemplo).

Dentre os problemas que surgiram com a necessidade de se implementar sistemas de segurança em equipamentos móveis e sem fio, alguns listados anteriormente, o *Wireless Security Processing Gap*, que corresponde às necessidades de poder de processamento impostas pelos protocolos de segurança a serem implementadas em sistemas sem fio é o tema principal do trabalho de Ravi [1]. Com o intuito de minimizar o problema, os autores utilizam protocolos de segurança e criptografia de baixa complexidade e utilizam processadores com capacidade de processamento criptográfico avançado. Como exemplo, é mencionado o processador

fabricado pela NEC intitulado MOSES (*MObile SEcurity processing System*) que permite a utilização de criptografia e protocolos de segurança na próxima geração de equipamentos portáteis e sem fio. O MOSES apresenta uma arquitetura de software dividida em camadas, o que permite o desenvolvimento paralelo e concomitante dos pacotes e APIs, por outro lado, o hardware foi também desenvolvido com seções dedicadas ao processamento de operações matemáticas complexas exigidas pelos sistemas de criptografia e segurança. O caminho adotado no trabalho de Ravi demonstra uma preocupação de muitos centros de estudo mundiais com o grande crescimento dos sistemas *wireless* e da segurança dos dados que trafegam nessas redes. Esta em particular evidencia a necessidade de alterações tanto em camadas de software como de hardware dos pequenos dispositivos móveis a fim de acomodar toda a bagagem de segurança e criptografia necessária para a utilização comercial e plena das tecnologias sem fio.

Bibliografia

[1] Ravi, S., ***Securing Wireless Data: System Architecture Challenges***, University of Princeton, http://www.princeton.edu/~sravi/papers/ 2002_isss_invited.pdf
[2] Bolzani, C. A. M, **Residências Inteligentes**, Editora Livraria da Física, 2004