

# Translation Shoppe

243 Spoonbill Lane South ∞ Jupiter, FL 33458 USA ∞ 561-352-0065

KnowledgeDock Business Centre ∞ 4-6 University Way ∞ London E16 2RD UK ∞ 020-8123-6328

E-Mail: [info@translationshoppe.com](mailto:info@translationshoppe.com) ∞ Skype: Translation\_Shoppe

<http://www.translationshoppe.com>

## Sample Text

Rogue wireless hardware is easy to introduce. Wireless access points are relatively inexpensive and easily deployed. A well-intentioned team of consultants working in a conference room might install a wireless access point in order to share a single wire port in the room. A malicious hacker can sit in a cafeteria with a wireless-enabled laptop scanning for unencrypted or WEP-encrypted traffic. In both cases, unacceptable risks are introduced. Regardless of whether there is malicious intent, the introduction of rogue hardware can compromise the confidentiality and integrity of network traffic. Rogue wireless devices can be detected by physically examining installations (known as “war driving”), using radio frequency (RF) scanners to determine the location of wireless devices, or by using systems designed to analyze network traffic for unauthorized devices.

## Portuguese

O hardware wireless rogue é fácil de introduzir. Os pontos de acesso wireless são relativamente baratos e facilmente desdobrados. Uma equipe bem intencionada de consultores trabalhando em uma sala de conferência pode instalar um ponto de acesso wireless para compartilhar uma porta de conexão individual na sala. Um hacker mal intencionado pode sentar numa cafeteria com um laptop wireless habilitado, efetuando a varredura de um tráfego não criptografado ou criptografado do WEP. Em ambos os casos, são introduzidos riscos inaceitáveis. Indiferente se existir uma intenção maliciosa, a introdução do hardware nocivo pode comprometer a confidencialidade e integridade do tráfego da rede. Os dispositivos wireless nocivos podem ser detectados fisicamente examinando as instalações (conhecidas como "ação de guerra" (war driving), utilizando scanners de radiofrequência para determinar o local dos dispositivos wireless, ou utilizando-se sistemas projetados para analisar o tráfego da rede para os dispositivos não autorizados.

*Rates for our services are determined by the languages involved for each translation, the length, and complexity of material as well as the timeframe of the project. Please contact the Translation Shoppe via e-mail at: [info@translationshoppe.com](mailto:info@translationshoppe.com), Skype at Translation\_Shoppe or by telephone at 561.352.0065 in the US or 020-8123-6328 in the UK to discuss the details of your project and obtain an estimate.*

<http://www.translationshoppe.com>