

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 ∞ 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.

Simplified Chinese

流氓无线硬件很容易侵入。无线接入点不但相当便宜，而且配置起来也非常便捷。一个为会议室工作的咨询小组也许会安装一个无线接入点，用来共同分享会议室内的单线端口。而一个怀有恶意的黑客可能坐在咖啡厅内，用装有无线上网卡的手提电脑搜寻没有加密的或用 WEP 加密的网络数据流。在这两种情况下，都会发生无法接受的风险，不论他是否怀有恶意企图，这一流氓硬件的侵入都能破坏网络传输的机密性和完整性。通过网络装置的仔细检查可以探测出流氓无线电设备（正如大家所熟知的“网络防卫战”），使用无线电频率（RF）扫描仪来测定无线装置的位置，或通过专门设计用于分析网络传输的系统探测未经授权的装置。

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, 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>