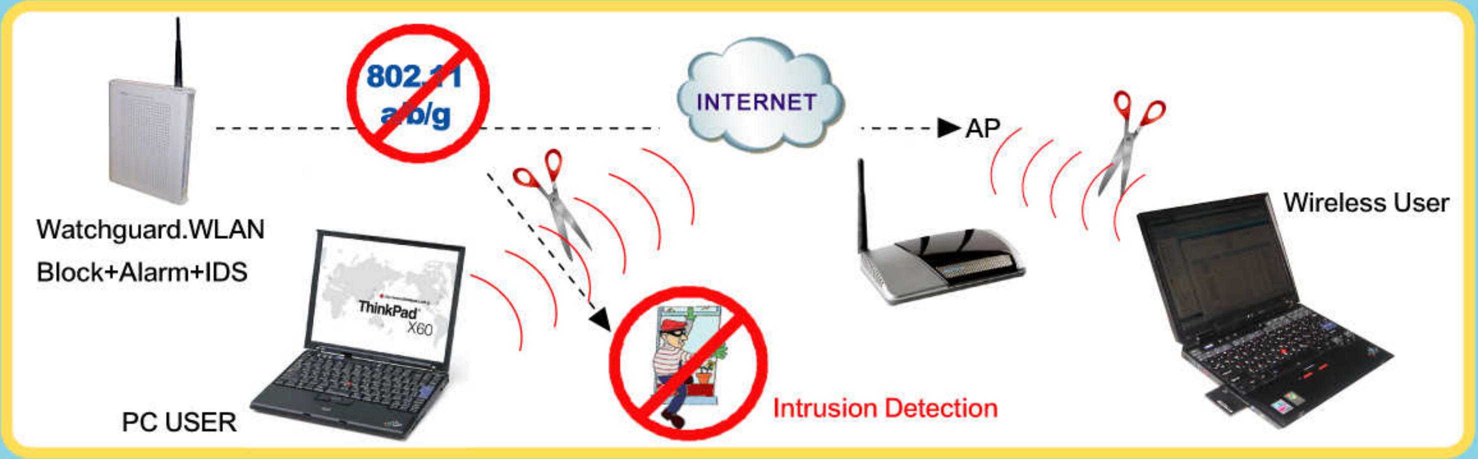
Wireless Network Guard

Jammer

WATCHGUARD.WLAN®

Wireless Network Jamming and Intruder Detecting Equipment

Intrusion Detection



Preface >>

WatchGuard.WLAN provides wireless communication diagnosis function, when WatchGuard.WLAN detects the wireless communication from access point (AP) or station that inside the coverage area of wireless network, it will forbid the wireless communication, and issue a warning message to the administrator. To prevent the wireless communication, the system can pretend as the station to inform AP to stop the communication. To emit noisy signals to station and/or AP is another method to prevent wireless communication.

During the allow communication duration, the WatchGuard.WLAN provides invasion detection function, which can be used to detect whether there is any unusual (unexpected) activities inside the coverage area of wireless network which include: the station sending out of large amount of de-authenticate or de-associate packets, unusual packets transmission for site survey process, the station that probes wireless network but does not log in, the station that already de-associates with the wireless network but still sending packets to the particular wireless network, unexpected BSS time stamp overflow electric waves that affect the wireless network.

System Standards >>

- To diagnose wireless communication under 802.11b/802.11g wireless network environment.
- When any wireless station or wireless AP is detected to communication through wireless network, it issues a warning message to the administrator, and forbids the communication.
- To prevent the wireless communication, the system can pretend as the station to inform AP to stop the communication. To emit noisy signals to station and/or AP is another method to prevent wireless communication.
- User can define allow communication and/or prohibit communication duration.
- Able to detect any unusual wireless probing packets under the wireless network environment and issue an alarm.
- Able to detect and find unusual packets transmission from SSID under the wireless network environment.
- Able to detect the station that sends large amount of de-authenticate and de-associate packets to paralyze the coverage area of wireless network.
- Able to detect unusual packets transmission for site survey process.
- Able to detect the wireless AP that changes its wireless channel.
- Able to detect the station that probes the wireless network but does not log in.
- Able to detect the station that already de-associates with the wireless network but still sending packets to the particular wireless network.
- Able to detect the 0 length probe response (error) replied from station.
- Able to detect the unexpected BSS time stamp overflow electric waves that affect the wireless AP of the wireless network.
- If any invasion is detected, the system will immediately send an email to inform the administrator.
- Support log server for recording log events
- Support MAC, SIP, DIP, BSSID, ESSID, event type, time stamp, session number, connection number log

Wireless-Detective Case Study

Taiwan Police Uses Wireless-Detective to Terminate Cyber Fraud

The Network Auction Fraud in Taiwan converted to a wireless pattern 3 years ago since 2003, and it has been not easy to be cracked by police, until the XXX Police Bureau, for the first time in Taiwanese Police Authority's history, to adopt a brand new technique innovated by Decision-Computer International Co., Ltd.

The suspect with last name called Chen lives in XXX, who uses wireless Internet accesses to avoid the police from tracing and investigating him. He pretended to be true and made fraudulent e-announcements saying that he got a special channel to purchase gift vouchers from various famous department stores like SXGX and Fxx Eastxxxx Department Stores in Taiwan with a 14% discount. Because it is impossible for the ordinary consumers to buy those gift vouchers with a discount ranging from 1 % to a maximal of 3% unless they buy it with amount of millions NT dollars and beyond. With a price difference more than 11 percent, it did attract some consumers to buy from Chen through Internet. At the very beginning, Chen sold limited amount of gift vouchers to cyber users really with a 14% discount as he pronounced, to win the trust even though he might lose money. However, after those greedy buyers trusted him and remitted substantial amount of cash money in order to buy more vouchers, then he took the cash and disappeared. In a half year time, he deceived almost 1,000 persons of cyber buyers with total fraudulent money exceed 7 million NT dollars (about US$220,000-).

The reason why suspect Chxx might succeed to deceive bigger amount of money from many people again and again, mainly because Chen hided himself behind the cyber curtain of Internet with a high ranking appraisal account number, and most importantly, he used wireless device accesses to Internet which makes the CID very difficult to trace him.

This 30-years-old suspect Chen is one of the many typical deceivers using the advantage of wireless auction surrounding on the web. Chen presumed that wireless access would hide him from been trapped. But he never imagined that a high-tech weapon of tracing apparatus call "E-Detective Internet Behavior Auditing System" has been innovated and is promoting to be commercialized by Decision-Computer International Co., Ltd.

If you like to know details of this news.
Please refer to the report of United Daily News on 18th, Jul, 2006.

DECISION COMPUTER INTERNATIONAL CO., LTD.
Address : 4/F No. 31, Alley 4, Lane 36, Sec.5, Ming-Shen East Road Taipei, Taiwan
Phone No : +886 2 2766-5753 Cell Phone: +886 933 941831
Fax No : +886 2 2766 5702
E - Mail : decision@ms1.hinet.net
URL: www.edecision4u.com/forensics.html
Contact: Casper / Managing Director