

[REVS] Hacking the Invisible Network (Insecurities in 802.11x)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2002-08/0001.html>

From: support@securiteam.com

Date: 08/01/02

From: support@securiteam.com

To: list@securiteam.com

Date: Thu, 1 Aug 2002 10:48:40 +0200 (CEST)

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>

-- promotion

When was the last time you checked your server's security?

How about a monthly report?

<http://www.AutomatedScanning.com> – Know that you're safe.

Hacking the Invisible Network (Insecurities in 802.11x)

SUMMARY

This paper addresses how to find the vulnerabilities inherent in the WEP algorithm, how to determine if a WLAN is vulnerable using freeware tools and, most importantly, how best to secure WLANs.

DETAILS

Executive summary (From the article):

Wireless network technology is becoming increasingly popular but, at the same time, has introduced many security issues. The popularity in wireless technology is driven by two primary factors – convenience and cost. A wireless local area network (WLAN) allows workers to access digital resources without being tethered to their desks. Laptops could be carried into meetings or even out to the front lawn on a nice day. This convenience has become affordable. Vendors have begun to produce compatible hardware at a reasonable price with standard such as the Institute of Electrical and Electronics Engineers Inc.'s (IEEE's) 802.11x.

However, the convenience of WLAN also introduces security concerns that do not exist in a wired world. Connecting to the network no longer requires an Ethernet cable. Instead, data packets are airborne and available to

Securiteam: [REVS] Hacking the Invisible Network (Insecurities in 802.11x)

anyone with the ability to intercept and decode them. Traditional physical security measures like walls and security guards are useless in the new domain.

Several reports have discussed weaknesses in the Wired Equivalent Privacy (WEP) algorithm employed by the 802.11x standard to encrypt wireless data. This leads to the development of automated tools, such as AirSnort and WEPCrack that automated the recovery of encryption keys. The IEEE has organized the 802.11i Task Group to address 802.11x security, and hardware vendors are racing to implement proprietary solutions. Still, securing vulnerable networks could take some time. Beyond this, research has shown that the majority of networks use no encryption at all. WEP is far from perfect, but it does at least provide a deferent to attackers.

WLANs introduce security risks that must be understood and mitigated. If not, vulnerable WLANs can compromise overall network security by allowing the following attack scenarios:

- * Vulnerable WLANs provide attackers with the ability to passively obtain confidential network data and leave no trace of the attack.
- * Vulnerable WLANs, positioned behind perimeter firewalls and considered trusted network, may provide attackers with a backdoor into a network. This access may lead to attacks on machines elsewhere on the wired LAN.
- * Vulnerable WLANs could serve as a launching pad for attacks on unrelated networks. WLANs provide convenient cover, as identifying the originator of an attack is difficult if not impossible.

Tools to identify WLANs, break WEP encryption keys, and capture network traffic are freely available. To protect against attacks, understand both vulnerabilities that exist and how attackers employ these tools to exploit the vulnerabilities. Identify compensating controls and determine if the risks can be mitigated to an acceptable level to justify the introduction of wireless network technology.

ADDITIONAL INFORMATION

The complete article can be downloaded from:
<<https://ialert.idefense.com/idcontent/2002/papers/Wireless.pdf>>
<https://ialert.idefense.com/idcontent/2002/papers/Wireless.pdf>

The information has been provided by <<mailto:msutton@idefense.com>>
Michael Sutton.

=====

This bulletin is sent to members of the SecuriTeam mailing list.
To unsubscribe from the list, send mail with an empty subject line and body to:
list-unsubscribe@securiteam.com
In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====
=====

Securiteam: [REVS] Hacking the Invisible Network (Insecurities in 802.11x)

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.

- *Previous message:* support@securiteam.com: "[NT] MS Terminal Services Vulnerable to SYN Scan"
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)