

# [REVS] War Nibbling: Bluetooth Insecurity

*Source:* <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-10/0039.html>

---

*From:* SecuriTeam ([support\\_at\\_securiteam.com](mailto:support_at_securiteam.com))

*Date:* 10/09/03

To: [list@securiteam.com](mailto:list@securiteam.com)

Date: 9 Oct 2003 15:34:37 +0200

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

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.

<http://www.securiteam.com/maillinglist.html>

-----

War Nibbling: Bluetooth Insecurity

---

## SUMMARY

The paper linked below is an introduction on how to pragmatically assess your environment for Bluetooth deployments using the latest vulnerabilities and attacks vectors. It also is an introduction to the Bluetooth protocol implementation and design in relation to security that need further research from the industry.

In summary, there are very real risks for Bluetooth enabled devices. These risks will proliferate as adoption becomes more widespread and the devices vary from their default configurations. We have also demonstrated the power of RedFang when trying to locate devices to assess [19].; Unlike 802.11 Bluetooth devices are harder to locate due to their low power, and potentially contain very sensitive information and/or interfaces that could be exposed to rogue third parties without the obstacles of hunting through corporate networks.

With the mass arrival of Class 1 devices, we now have the same potential security crisis as with 802.11. This may even be worse due to the proliferation of the types of devices that are Bluetooth enabled, including everything from headphones to laptop computers. Vendors should understand these issues and risks and develop an effective mechanism of delivering the device as secure out of the box. This will not only enhance

## Securiteam: [REVS] War Nibbling: Bluetooth Insecurity

the default security posture of Bluetooth, but will also educate users as to the need to ensure security for these devices. While things are improving with the introduction of an 'Anonymity Mode' in the forthcoming Bluetooth 1.2 specifications, the real outcome will largely depend on both the design and the implementation of the final specifications and how quickly they are adopted. We already have millions of 1.0 and 1.1-based devices in the hands of users today.

### DETAILS

#### Abstract:

The Bluetooth protocol, which is deployed in millions of products ranging from cellular telephones to laptops, is quickly becoming the new standard for intra-device wireless communications. The paper linked below examines methods of assessing the security of Bluetooth devices in relation to the protocol's design and implementation flaws. We will also discuss ways to proactively approach Bluetooth security and what security professionals can do to defend their organizations against unwanted compromise.

### ADDITIONAL INFORMATION

The complete paper can be downloaded from:

<[http://www.atstake.com/research/reports/acrobat/atstake\\_war\\_nibbling.pdf](http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf)>  
[http://www.atstake.com/research/reports/acrobat/atstake\\_war\\_nibbling.pdf](http://www.atstake.com/research/reports/acrobat/atstake_war_nibbling.pdf).

The paper has been written by <mailto:ollie@atstake.com> Ollie Whitehouse of @Stake.

=====

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

=====  
=====

#### 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.