

Hiding the service set identifier (SSID) on 802.11¹ Wireless networks WHITEPAPER

by Stefan Bauer – August 2007 – stefan.bauer@plzk.de

This whitepaper describes the so called security Option "SSID-hiding" and explains the pitfalls in this scenario.

A few technical informations at first:

In a wireless network, the connection is associated between a client and a server.

We assume that there is an accesspoint called "server" and a client whose name is "client". Additionally we need a client which tries to find out the hidden ssid called "badhost".

Every Wireless network needs a unique service set identifier (SSID)² which is limited to 32 alphanumeric characters and needs to be the same on every client aswell as on the host which distributes service like an accesspoint does.

Without active SSID-hiding an accesspoint broadcasts the own SSID frequently over the air in a broadcast beacon to tell other clients the own name and mac-address. This can be tracked with tools like wireshark³ (which is a frontend to tcpdump⁴).

We assume now, that SSID-hiding has been activated in our accesspoint and we try to understand this with the tools mentioned above.

The SSID in the broadcast beacon is:

```
"\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000\000"
```

Though hiding the ssid is not! a security improvement because only in the broadcast frames send by the accesspoint the ssid is hidden. Everytime a client associates, deauths or even probes for an available network the SSID is still send over air in cleartext.

How can this be displayed in software? The common unix tool for this task is kismet which is called a passive scanning tool. It only collects packages and does not generate any.

With this knowledge it is only a matter of time until a client associates or deauths. Within a rock-solid network, there wouldn't be an auth or deauth frequently, so we need to persuade a host to do this manually.

The principal idea behind this attack is to inject packages in the wireless network and let the accesspoint send some of the following packages to the client with tools like aircrack⁵:

PROBE Requests, PROBE Responses, ASSOCIATION Requests, REASSOCIATION Requests

All of them contain the SSID in cleartext. The 802.11w⁶ group is trying to prevent paket injection by authenticating wireless management frames.

1 <http://www.ieee802.org/11/>

2 <http://en.wikipedia.org/wiki/SSID>

3 <http://www.wireshark.org/>

4 <http://www.tcpdump.org/>

5 <http://www.aircrack-ng.org/>

6 http://en.wikipedia.org/wiki/IEEE_802.11w