Bellevue University

Flaws in WEP

Because

Of RC4 Implementation

Timothy Jelinek

CIS313-T301 Cryptography

9/24/2023

How the Implementation of RC4 Created Flaws in WEP

Easy to Analyze

If an attacker can get part of the key, then they are able to receive the secret part by analyzing the initial word of keystreams with little work.

Easy to Attack Using IV

An attacker can receive the first byte in the output of the RC4. They can then search for IVs that set up an equation with they can use to find byte *B*.

Predictable

To combat the attacks that use the IVs, the industry started making the WEP keys longer. This, unfortunately, doesn't matter and the key does not become immune to the attack.

Easy to Guess

The attacker has multiple different strategies they can use. They can search for the IVs or even assume the first several bytes of the key and then search for the IVs.

Sources:

"Weakness in the Key Scheduling Algorithm of RC4" Fluhrer, Mantin, Shamir, Cisco Systems Inc., The Weizmann Institute, https://www.cs.cornell.edu/people/egs/615/rc4_ksaproc.pdf. Accessed 24 September 2023.