详解如何在一分钟内攻破WPA思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E8_AF_A6_E8_A7_A3_E5_A6_82_E4_c101_644165.htm 无线路由器的安全问题一直是局域网安全的“ 命门 ”，它们所使用的密码机制总是出现安全问题。最早WEP密码机制在1997年被开发出来，并应用在无线路由器产品上。结果几年后就被破了。随后又有了新的WPA机制，不过这套机制的命运也和WEP相差无几，去年又被两名两位研究者Martin Beck和Erik Tews给破掉了。几位日本研究者已经成功发明了一种可以在1分钟之内破解这套机制的方法。 不过他们采用Becks-Tews攻击，需要攻击目标IEEE802.11e QoS功能，没有很高的“ 使用价值 ”。并且Becks-Tews攻击的过程需要耗时12-15分钟才可以攻破密码机制，容易被管理者发觉。所以，这个事件没有造成恐慌，大家对于WPA还是相对信任。 最近，两位日本的研究者将Beck-Tews应用到MITM攻击中，并且能够伪造加密小数据包(如ARP数据包)。来自广岛大学的Toshihiro Ohigashi和神户大学Masakatu Morii提出了MITM攻击的策略以及减少攻击执行时间的方法。最终，攻击执行时间最少只需要1分钟，并且这种攻击可以在所有WPA部署中实施。 9月25日，两位日本研究者将在广岛的一次会议上详细介绍他们的攻击技术。他们还提前透露了将要在此次大会上讨论的PDF文档。 以下是该文档的导言： WPA(无线网络保护Wi-Fi Protected Access)/TKIP(临时密钥完整性协议Temporal Key Integrity Protocol)是专为保护无线局域网络通信机密性和完整性的安全协议。WPA的出现旨在弥补WEP(有线对等加密协议) 存在

的缺陷，WEP一直是用于很多无线LAN产品的安全保护协议。WPA主要使用两种形式的密钥，包括64位信息完整性检查(MIC)密钥和128位加密密钥。前者主要用于检查伪造/虚假信息，而后者主要用于加密和解密数据包。这些密钥都是从共有的主密钥(master key)中生成的。来源：考试大 很多安全研究人员一直都在潜心研究WPA的安全性，Moskowitz就发现了WPA中抵御字典攻击的弱点，不过他可以通过绕开这个弱点来从任意长度的字符组中生成主密钥。多数其他分析师都对WPA的组件进行了分析，而这些对于WPA都不能构成威胁。在2008年的时候，Beck和Tews对那些支持 IEEE802.11e QoS功能的WPA部署发动了实质性的攻击，他们的攻击(被称为Beck-Tews攻击)可以从加密的小数据包中(如APR数据包和DNS数据包)中修复 MIC密钥和纯文本，并且使用修复的MIC密钥对其加密数据包进行伪造。这种攻击的执行时间大约是12到15分钟。由于Beck-Tews攻击是一种基于应答式攻击的方法，攻击目标必须支持IEEE802.11e QoS功能。因此，他们的成果也是有限的。百考试题－全国最大教育类网站(100test.com) 在本文中，我们将提出一种针对任何WPA部署的根本性的攻击。首先，为了突破攻击目标无线LAN产品的限制，我们采用Beck-Tews攻击用于中间人攻击(MITM)。配合中间人攻击的Beck-Tews攻击并不需要目标能够支持IEEE802.11e QoS功能，这意味着我们的攻击可以攻击任何类型的WPA部署。另外，我们将探讨如何对无线局域网络实施有效的MITM攻击。在MITM攻击中，用户的通信被攻击者拦截，直到攻击结束才会解除拦截状态，这意味着当攻击时间比较长时用户可能检查到我们的攻击。因此，第三个，我

们提供了几种缩短攻击执行时间的方法，正如标题所说，我们最终可以实现一分钟内干掉WPA。 编辑特别推荐: 各个方向CCIE认证投资回报分析 思科证书的意义：技术经验的证明 我是主考官：给一位应届毕业生的回信 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com