Understanding the WPA/WPA2 Break

Joshua Wright
josh@inguardians.com
Office/Mobile: 401-524-2911
www.inguardians.com
Your Speaker

- Joshua Wright, josh@inguardians.com
- Senior Security Analyst, InGuardians
- Author – SANS Wireless Ethical Hacking course (SEC617)
- Senior SANS Instructor
- Wireless security enthusiast
  - Wireless insecurity enthusiast

Understanding the WPA/WPA2 Break © 2008, Joshua Wright
Outline

- Attack Overview
  - Attack Analysis
  - Enterprise Defenses
  - Summary, Question and Answer
The Bad News

- Martin Beck from the Technical University of Dresden discovered a flaw in the TKIP protocol
  - Assisted by Erik Tews from the Technical University of Darmstadt
- Allows an attacker to decrypt data to a wireless client, slowly
- Once a packet is decrypted, opportunity to transmit up to 7 forged packets of any content
- No authorization needed for success
The Good News

• Not a key recovery attack
  – Attacker can only decrypt one packet at a time; does not allow earlier/later frame decryption
• Does not affect AES-CCMP networks (required for FIPS 140-2)
• Workarounds will mitigate this flaw
  – Not perfect, but will buy some time
• Some APs can be configured to mitigate this flaw (at some cost)
Who Is Affected?

- All deployments of TKIP
  - Regardless of WPA or WPA2 use
  - Regardless of PSK or 802.1X/EAP authentication

- Current *exploits* target TKIP networks with QoS enabled
  - QoS is required for much of 802.11n
Attacker Opportunity

- Attacker can decrypt a plaintext packet from AP to station (not station to AP)
  - Not more than 1 unknown byte per minute
  - Any packet can be selected for partial data
- Targeting an ARP packet, between 14 and 17 unknown bytes
  - 8 MIC, 4 ICV, 2-5 IP source and dest.

Once plaintext is known, attacker can inject not more than 15 arbitrary packets
- ARP poisoning, DNS manipulation, TCP/SYN request
Outline

• Attack Overview

→ Attack Analysis

• Enterprise Defenses

• Summary, Question and Answer
April 2003: TKIP Fixes WEP Flaw

- No replay protection with WEP

- TKIP Sequence Counter (TSC)
July 2005:
QoS Complicates Matters

- QoS relies on the ability to reorder packets for delivery
- This requirement conflicts with TKIP sequence delivery
- Solution: Maintain multiple independent, unsynchronized sequence counters
Wait ... Really? They Did That?

- Yes, they really did.
- 802.11e displaced sequence enforcement across multiple queues (Wireless MultiMedia)
- This is a significant security failure
- The WMM author was informed ... and chose not to act to resolve
However, the sequence number became part of the per-packet hash (MIC). Changing the queue defeated sequence enforcement but made the packet invalid, DoS’ing all stations on a target AP.
WEP ICV Attack - ChopChop

- Integrity Check Value (ICV) – WEP 32-bit CRC
- Vulnerable to modification and repeated guess until positive response observed (chopchop attack)
- Repeated to recover entire plaintext packet contents
Fixed(?) in TKIP

- TKIP adds a new per-packet hashing algorithm (MIC) known as Michael
- Weak algorithm, but best that could be accommodated on legacy WEP hardware
- Includes provision for countermeasures
  - Two invalid MIC’s within 60 seconds shuts down AP and STA’s for 60 seconds
  - Must pass ICV and TSC check first
TKIP Encryption/Decryption

**Encryption Process**
- Calculate MIC
- Calculate ICV
- Get Next TSC
- Encryption Key Calculation
- Encrypt P+MIC+ICV

**Decryption Process**
- TSC + Encrypted P+MIC+ICV
- Check TSC
  - Valid: Encryption Key Calculation
  - Drop
- Decrypt Data
- Check ICV
  - Valid: Drop
  - Invalid: Check MIC
    - Valid: Transmit
    - Invalid: Error

plaintext packet (P)

TSC +

Wireless Transmission
And This is Exploited How?

- ICV failure generates no network activity
- MIC failure causes the client to generate a notice the attacker can observe
- If MIC failure observed, ICV passed!
- Take a packet, chop last byte, guess fix and TX until MIC failure observed
- Wait 60 seconds to not trigger countermeasures
- Repeat for next-to-last byte
TKIP Chopchop ICV Attack

1. Attacker captures TKIP encrypted packet that looks like ARP
2. Attacker removes last payload byte, invalidating ICV and MIC. Attempts to fix ICV with guess 0 and sends to station.
3. Client receives frame, most have ICV failures and are dropped. One passes ICV, but fails MIC.
4. A MIC failure message is sent to AP to coordinate Michael countermeasures. Though encrypted, attacker can observe this frame to identify valid ICV, revealing one byte of plaintext.

Attacker waits 60 seconds to avoid MIC countermeasures, then repeats process with 66 byte packet. Continues until all packet plaintext is known.
Attack Result

- Not more than 1 byte per minute decrypted
- ARP is mostly known plaintext
  - Five bytes unknown assuming /24 (A.B.C.Y and A.B.C.Z)
- Also need to determine ICV and MIC values (12 bytes)
- Only 17 bytes to recover, 14 if network is known (RFC1918 guess?)

Result: 68 bytes ARP, 8 bytes MIC, 4 bytes ICV known plaintext to the attacker in 14-17 minutes
Another Michael Weakness

- Michael is *invertible*; you can determine the key from plaintext + MIC
- Attacker decrypts ARP, knows Michael key and can craft any packet up to 68 bytes
- Attacker can use other QoS queues where attacked TSC is lower to inject arbitrary packets into network (can target any destination or protocol)
- Injection is blind, attacker cannot decrypt responses
- Attacker can only inject up to 7 packets (3 other standard 802.11e queues and 4 non-standard)
  - Potential for 15 injected packets, yet untested
Practical TKIP Attack Example

1. Attacker decrypts ARP packet, can inject up to 7 packets into network

2. Attacker injects TCP SYN packets with source=4.1.1.2 testing common ports (443, 135, etc), up to 7 packets

3. Attacker’s agent receives responses from victim, identifying open (SYN/ACK) and closed (FIN/ACK) ports. Opportunity for agent to complete 3-way handshake for further communication with the victim.

Other attack possibilities include:
- DNS manipulation
- Delivering UDP-based exploits
- ARP manipulation on LAN
tkiptun-ng

- Attack tool in Aircrack-ng source repository
- Incomplete, doesn’t work in current form
- Likely to implement attack described here, extracting plaintext, injecting new packets
- May be accompanied by TUN interface
  - Attacker uses any tool to inject packets
MIC DoS Attacks Easy Now

- Michael algorithm countermeasures
  - AP must disconnect all stations and shutdown the network following two MIC failures within 60 seconds
- Very easy for an attacker to trigger, shutting down AP for 60 seconds

DOT11-TKIP_MIC_FAILURE: TKIP Michael MIC failure was detected on a packet (TSC=0x0) received from [mac-address]
Outline

• Attack Overview
• Attack Analysis

Enterprise Defenses

• Summary, Question and Answer
Defense Strategies (1)

- Best approach: migrate away from TKIP to AES-CCMP
  - Will likely require moving to WPA2
- Difficult to implement if you need to support any legacy devices
  - Laptops and embedded devices (VoIP phones, handhelds, etc)
- Client re-configuration will be necessary, making this resource-intensive
  - Active Directory simplifies deployment
Defense Strategies (2)

- Forcing more frequent key rotation will limit how much plaintext can be derived
  - Each minute of key life can be used to determine a byte of plaintext
  - 4 minute key rotation = 4 bytes plaintext
- Consensus is to reduce key to 2 minutes
- Reducing key lifetime may burden AP

This defense is the best immediate-term option, but requires testing to understand the impact to all devices.
## Product-Specific Steps

<table>
<thead>
<tr>
<th>Aruba Networks – PTK and GTK rotation</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>configure terminal</code></td>
</tr>
<tr>
<td><code>aaa authentication dot1x &lt;profilename&gt;</code></td>
</tr>
<tr>
<td><code>multicast-keyrotation</code></td>
</tr>
<tr>
<td><code>unicast-keyrotation</code></td>
</tr>
<tr>
<td><code>timer mkey-rotation-period 120</code></td>
</tr>
<tr>
<td><code>timer ukey-rotation-period 120</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Aerohive Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerohive currently detects and logs Michael MIC failures and in the next maintenance release of HiveOS Aerohive is implementing a PTK rekey feature. Watch the Aerohive support page for more information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Trapeze Networks – Disable QoS</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>set radio-profile &lt;name&gt; qos-modesvp</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Motorola/Symbol</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>wlan &lt;WLAN&gt; dot11i key-rotation enable</code></td>
</tr>
<tr>
<td><code>wlan &lt;WLAN&gt; dot11i key-rotation-interval 120</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bluesocket</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bluesocket plans to add a unicast key rotation mechanism to a future product release.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco Autonomous – 802.1X reauthenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning: Significant negative impact</td>
</tr>
<tr>
<td><code>dot1x timeout reauth-period 120</code></td>
</tr>
<tr>
<td><code>broadcast-key change 120</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Cisco WLC – 802.1X reauthenticate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Warning: Significant negative impact</td>
</tr>
<tr>
<td><code>config wlan session-timeout &lt;wlanID&gt; 120</code></td>
</tr>
<tr>
<td><code>devshell dot1xUpdateBroadcastRekeyTimer 120</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Meru Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Meru Networks did not respond to multiple requests for information.</em></td>
</tr>
</tbody>
</table>
Defense Strategies (3)

- Disabling QoS support on an AP will defeat tools, does not solve issue
  - Not an option for 802.11n High-Throughput (HT) networks
- Vendors may choose to fix TKIP with implementation hacks
  - Keep an eye on your AP and client vendor software update pages
Monitoring (1)

- WIDS technology can identify this attack
  - You will need a software update to get new signature support
  - Action: contact your WIDS vendor today: "When will you detect the TKIP ICV attack?"
  - No signature in Kismet ... yet

- Log monitoring on AP’s

<table>
<thead>
<tr>
<th>Cisco Autonomous APs</th>
<th>Aruba Networks</th>
</tr>
</thead>
<tbody>
<tr>
<td>DOT11-TKIP_MIC_FAILURE_REPORT: Received TKIP Michael MIC failure report from the station [mac-address] on the packet (TSC=0x0) encrypted and protected by [key] key</td>
<td>Received TKIP Micheal MIC Failure Report from the Station [mac addr] [bssid] [apnames]</td>
</tr>
</tbody>
</table>
Monitoring (2)

Aerohive APs
AP detected Michael MIC failure in received frame from abb:ccdd:eeff(wifi0.1) for sta 1122:3344:5566(TKIP)

Cisco Wireless LAN Controller
Identifies DoS, not TKIP attack
The AP '00:0b:85:67:6b:b0' received a WPA MIC error on protocol '1' from Station '00:13:02:8d:f6:41'. Counter measures have been activated and traffic has been suspended for 60 seconds.

Trapeze Networks
Logging message not supplied before presentation deadline.

Symbol/Motorola
Station [MAC_ADDR] reported a TKIP message integrity check fail on wlan [WLAN_ID]

Bluesocket
Michael MIC failure detected in received frame MLME-MichaelMICFailure. indication(00:12:cf:00:01:02)

Meru Networks did not respond to multiple requests for information.
Outline

- Attack Overview
- Attack Analysis
- Enterprise Defenses

Summary, Question and Answer
Summary

- This is a break in TKIP, affecting WPA and WPA2 regardless of authentication
- Immediate actions:
  - Start planning transition to AES-CCMP
  - Investigate and apply TKIP key rotation every 2 minutes
  - Capture and analyze logging data on AP's
Question and Answer

- Joshua Wright, josh@inguardians.com
  - 401-524-2911 Office/Mobile
- SANS Ethical Hacking Wireless course
  - 12/11/08: Washington DC (Luallen)
  - 3/2/09: Orlando, FL (Wright)
- InGuardians, Inc.
  - Services for research, vulnerability assessment, penetration testing, incident response and more
  - www.inguardians.com
- Wireless tools and information (Josh's site)
  - www.willhackforsushi.com
More Resources

- Tkiptun-ng documentation
  - www.aircrack-ng.org/doku.php?id=tkiptun-ng
- Tews/Beck paper on TKIP and WEP
- Raul Siles attack analysis information
- Article: "Battered, but not broken: understanding the WPA crack"
  - http://arstechnica.com/articles/paedia/wpa-cracked.ars/