Temporal Key Integrity Protocol

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#searchInput)

|  |  |
| --- | --- |
| **Temporal Key Integrity Protocol** | |
| **General** | |
| **Designers** | [Wi-Fi Alliance](https://en.wikipedia.org/wiki/Wi-Fi_Alliance) |
| **First published** | October 31, 2002; 17 years ago |
| **Derived from** | [Wired Equivalent Privacy](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) |
| **Cipher detail** | |
| [**Key sizes**](https://en.wikipedia.org/wiki/Key_size) | 128 bits |
| **Best public**[**cryptanalysis**](https://en.wikipedia.org/wiki/Cryptanalysis) | |
| Deprecated | |

**Temporal Key Integrity Protocol** (**TKIP** [/tiːˈkɪp/](https://en.wikipedia.org/wiki/Help:IPA/English)) is a [security protocol](https://en.wikipedia.org/wiki/Security_protocol) used in the [IEEE 802.11](https://en.wikipedia.org/wiki/IEEE_802.11) wireless networking standard. TKIP was designed by the [IEEE 802.11i](https://en.wikipedia.org/wiki/IEEE_802.11i) task group and the [Wi-Fi Alliance](https://en.wikipedia.org/wiki/Wi-Fi_Alliance) as an interim solution to replace [WEP](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) without requiring the replacement of legacy hardware. This was necessary because the breaking of WEP had left Wi-Fi networks without viable [link-layer](https://en.wikipedia.org/wiki/Data_link_layer#Logical_link_control_sublayer) security, and a solution was required for already deployed hardware. However, TKIP itself is no longer considered secure, and was deprecated in the 2012 revision of the 802.11 standard.[[1]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-deprecate-1)



**Contents**

* [1Background](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Background)
* [2Technical details](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Technical_details)
* [3Security](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Security)
  + [3.1Packet spoofing and decryption](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Packet_spoofing_and_decryption)
  + [3.2Royal Holloway attack](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Royal_Holloway_attack)
* [4Legacy](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#Legacy)
* [5See also](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#See_also)
* [6References](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#References)

Background[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=1)]

On October 31, 2002, the Wi-Fi Alliance endorsed TKIP under the name [Wi-Fi Protected Access (WPA)](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access).[[2]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-WPA_announcement-2) The IEEE endorsed the final version of TKIP, along with more robust solutions such as [802.1X](https://en.wikipedia.org/wiki/802.1X) and the [AES](https://en.wikipedia.org/wiki/Advanced_Encryption_Standard) based [CCMP](https://en.wikipedia.org/wiki/CCMP_(cryptography)), when they published IEEE 802.11i-2004 on 23 July 2004.[[3]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-80211i-3) The Wi-Fi Alliance soon afterwards adopted the full specification under the marketing name [WPA2](https://en.wikipedia.org/wiki/WPA2).[[4]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-WPA2_announcement-4)

TKIP was resolved to be deprecated by the IEEE in January 2009.[[1]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-deprecate-1)

Technical details[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=2)]

TKIP and the related WPA standard implement three new security features to address security problems encountered in WEP protected networks. First, TKIP implements a key mixing function[[*which?*](https://en.wikipedia.org/wiki/Wikipedia:Avoid_weasel_words)] that combines the secret root key with the [initialization vector](https://en.wikipedia.org/wiki/Initialization_vector) before passing it to the [RC4 cipher](https://en.wikipedia.org/wiki/RC4) initialization. WEP, in comparison, merely concatenated the initialization vector to the root key, and passed this value to the RC4 routine. This permitted the vast majority of the RC4 based WEP [related key attacks](https://en.wikipedia.org/wiki/Related_key_attack).[[5]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-edney-5) Second, WPA implements a sequence counter to protect against replay attacks. Packets received out of order will be rejected by the access point. Finally, TKIP implements a 64-bit [Message Integrity Check (MIC)](https://en.wikipedia.org/wiki/Message_Integrity_Code#Message_integrity_codes) and re-initialize the sequence number each time when a new key(Temporal key) is used.[[6]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-6)

To be able to run on legacy WEP hardware with minor upgrades, TKIP uses [RC4](https://en.wikipedia.org/wiki/RC4) as its cipher. TKIP also provides a [rekeying](https://en.wikipedia.org/wiki/Rekeying_(cryptography)) mechanism. TKIP ensures that every data [packet](https://en.wikipedia.org/wiki/Packet_(information_technology)) is sent with a unique [encryption key](https://en.wikipedia.org/wiki/Encryption_key)(Interim Key/Temporal Key + Packet Sequence Counter).[[*citation needed*](https://en.wikipedia.org/wiki/Wikipedia:Citation_needed)]

Key mixing increases the complexity of decoding the keys by giving an attacker substantially less data that has been encrypted using any one key. WPA2 also implements a new message integrity code, MIC. The message integrity check prevents forged packets from being accepted. Under WEP it was possible to alter a packet whose content was known even if it had not been decrypted.

Security[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=3)]

TKIP uses the same underlying mechanism as WEP, and consequently is vulnerable to a number of similar attacks. The message integrity check, per-packet key [hashing](https://en.wikipedia.org/wiki/Hash_function), broadcast key rotation, and a sequence counter discourage many attacks. The key mixing function also eliminates the WEP key recovery attacks.

Notwithstanding these changes, the weakness of some of these additions have allowed for new, although narrower, attacks.

**Packet spoofing and decryption**[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=4)]

TKIP is vulnerable to a [MIC key](https://en.wikipedia.org/wiki/Message_Integrity_Code#Message_integrity_codes) recovery attack that, if successfully executed, permits an attacker to transmit and decrypt arbitrary packets on the network being attacked.[[7]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-vanhoef-piessens-7) The current publicly available TKIP-specific attacks do not reveal the Pairwise Master Key or the Pairwise Temporal Keys. On November 8, 2008, Martin Beck and Erik Tews released a paper detailing how to recover the MIC key and transmit a few packets.[[8]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-beck-tews-8) This attack was improved by Mathy Vanhoef and Frank Piessens in 2013, where they increase the amount of packets an attacker can transmit, and show how an attacker can also decrypt arbitrary packets.[[7]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-vanhoef-piessens-7)

The basis of the attack is an extension of the [WEP](https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy) [chop-chop attack](https://en.wikipedia.org/w/index.php?title=Chop-chop_attack&action=edit&redlink=1). Because WEP uses a cryptographically insecure checksum mechanism ([CRC32](https://en.wikipedia.org/wiki/CRC32)), an attacker can guess individual bytes of a packet, and the wireless access point will confirm or deny whether or not the guess is correct. If the guess is correct, the attacker will be able to detect the guess is correct and continue to guess other bytes of the packet. However, unlike the chop-chop attack against a WEP network, the attacker must wait for at least 60 seconds after an incorrect guess (a successful circumvention of the CRC32 mechanism) before continuing the attack. This is because although TKIP continues to use the CRC32 checksum mechanism, it implements an additional [MIC code](https://en.wikipedia.org/w/index.php?title=MIC_code&action=edit&redlink=1) named Michael. If two incorrect Michael MIC codes are received within 60 seconds, the access point will implement countermeasures, meaning it will rekey the TKIP session key, thus changing future keystreams. Accordingly, attacks on TKIP will wait an appropriate amount of time to avoid these countermeasures. Because [ARP](https://en.wikipedia.org/wiki/Address_resolution_protocol) packets are easily identified by their size, and the vast majority of the contents of this packet would be known to an attacker, the number of bytes an attacker must guess using the above method is rather small (approximately 14 bytes). Beck and Tews estimate recovery of 12 bytes is possible in about 12 minutes on a typical network, which would allow an attacker to transmit 3–7 packets of at most 28 bytes.[[8]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-beck-tews-8) Vanhoef and Piessens improved this technique by relying on [fragmentation](https://en.wikipedia.org/w/index.php?title=Fragmented_distribution_attack&action=edit&redlink=1), allowing an attacker to transmit arbitrary many packets, each at most 112 bytes in size.[[7]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-vanhoef-piessens-7) The Vanhoef–Piessens attacks also can be used to decrypt arbitrary packets of the attack's choice.

An attacker already has access to the entire ciphertext packet. Upon retrieving the entire plaintext of the same packet, the attacker has access to the keystream of the packet, as well as the MIC code of the session. Using this information the attacker can construct a new packet and transmit it on the network. To circumvent the WPA implemented replay protection, the attacks use [QoS](https://en.wikipedia.org/wiki/Quality_of_service) channels to transmit these newly constructed packets. An attacker able to transmit these packets may be able to implement any number of attacks, including [ARP poisoning](https://en.wikipedia.org/wiki/ARP_poisoning) attacks, denial of service, and other similar attacks, with no need of being associated with the network.

**Royal Holloway attack**[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=5)]

A group of security researchers at the Information Security Group at Royal Holloway, University of London reported a theoretical attack on TKIP which exploits the underlying [RC4](https://en.wikipedia.org/wiki/RC4) encryption mechanism. TKIP uses a similar key structure to WEP with the low 16-bit value of a sequence counter (used to prevent replay attacks) being expanded into the 24-bit "IV", and this sequence counter always increment on every new packet. An attacker can use this key structure to improve existing attacks on RC4. In particular, if the same data is encrypted multiple times, an attacker can learn this information from only 224 connections.[[9]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-9)[[10]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-10)[[11]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-11) While they claim that this attack is on the verge of practicality, only simulations were performed, and the attack has not been demonstrated in practice.

**NOMORE attack**

In 2015, security researchers from KU Leuven presented new attacks against RC4 in both TLS and WPA-TKIP. Dubbed the Numerous Occurrence MOnitoring & Recovery Exploit (NOMORE) attack, it is the first attack of its kind that was demonstrated in practice. The attack against WPA-TKIP can be completed within an hour, and allows an attacker to decrypt and inject arbitrary packets.[[12]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-12)

Legacy[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=6)]

ZDNet reported on June 18, 2010 that WEP & TKIP would soon be disallowed on Wi-Fi devices by the Wi-Fi alliance.[[13]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-13) However, a survey in 2013 showed that it was still in widespread use.[[14]](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_note-14)

See also[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=7)]

* [Wireless network interface controller](https://en.wikipedia.org/wiki/Wireless_network_interface_controller)
* [CCMP](https://en.wikipedia.org/wiki/CCMP_(cryptography))
* [Wi-Fi Protected Access](https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access)
* [IEEE 802.11i-2004](https://en.wikipedia.org/wiki/IEEE_802.11i-2004)

References[[edit](https://en.wikipedia.org/w/index.php?title=Temporal_Key_Integrity_Protocol&action=edit&section=8)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-deprecate_1-0) [***b***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-deprecate_1-1) [*"802.11mb Issues List v12"*](https://mentor.ieee.org/802.11/file/08/11-08-1127-12-000m-tgmb-issues-list.xls)*(excel). 20 Jan 2009. p. CID 98. The use of TKIP is deprecated. The TKIP algorithm is unsuitable for the purposes of this standard*
  2. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-WPA_announcement_2-0) [*"Wi-Fi Alliance Announces Standards-Based Security Solution to Replace WEP"*](https://web.archive.org/web/20080103110456/http:/wi-fi.org/pressroom_overview.php?newsid=55)*.*[*Wi-Fi Alliance*](https://en.wikipedia.org/wiki/Wi-Fi_Alliance)*. 2002-10-31. Archived from*[*the original*](http://wi-fi.org/pressroom_overview.php?newsid=55)*on 2008-01-03. Retrieved 2007-12-21.*
  3. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-80211i_3-0) [*"IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements"*](http://standards.ieee.org/getieee802/download/802.11i-2004.pdf)*(pdf).*[*IEEE Standards*](https://en.wikipedia.org/wiki/IEEE_Standards)*. 2004-07-23. Retrieved 2007-12-21.*
  4. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-WPA2_announcement_4-0) [*"Wi-Fi Alliance Introduces Next Generation of Wi-Fi Security"*](https://web.archive.org/web/20080103105842/http:/wi-fi.org/pressroom_overview.php?newsid=31)*.*[*Wi-Fi Alliance*](https://en.wikipedia.org/wiki/Wi-Fi_Alliance)*. 2004-09-01. Archived from*[*the original*](http://wi-fi.org/pressroom_overview.php?newsid=31)*on 2008-01-03. Retrieved 2007-12-21.*
  5. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-edney_5-0) *Edney, Jon; Arbaugh, William A. (2003-07-15). Real 802.11 Security: Wi-Fi Protected Access and 802.11i.*[*Addison Wesley Professional*](https://en.wikipedia.org/wiki/Addison_Wesley)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-0-321-13620-6*](https://en.wikipedia.org/wiki/Special:BookSources/978-0-321-13620-6)*.*
  6. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-6) IEEE-SA Standards Board. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. *Communications Magazine*, IEEE, 2007.
  7. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-vanhoef-piessens_7-0) [***b***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-vanhoef-piessens_7-1) [***c***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-vanhoef-piessens_7-2) *Vanhoef, Mathy; Piessens, Frank (May 2013).*[*Practical Verification of WPA-TKIP Vulnerabilities*](https://lirias.kuleuven.be/bitstream/123456789/401042/1/wpatkip.pdf)*(PDF). Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ASIA CCS '13. pp. 427–436.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2484313.2484368*](https://doi.org/10.1145%2F2484313.2484368)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9781450317672*](https://en.wikipedia.org/wiki/Special:BookSources/9781450317672)*.*
  8. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-beck-tews_8-0) [***b***](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-beck-tews_8-1) Martin Beck & Erik Tews, "Practical attacks against WEP and WPA", available at [[1]](http://dl.aircrack-ng.org/breakingwepandwpa.pdf).
  9. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-9) *AlFardan; et al. (2013-07-08).*[*"On the Security of RC4 in TLS and WPA"*](http://www.isg.rhul.ac.uk/tls/RC4biases.pdf)*(PDF). Information Security Group, Royal Holloway, University of London.*
  10. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-10) *Paterson; et al. (2014-03-01).*[*"Plaintext Recovery Attacks Against WPA/TKIP"*](http://eprint.iacr.org/2013/748.pdf)*(PDF). Information Security Group, Royal Holloway, University of London.*
  11. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-11) *Paterson; et al. (2014-03-01). "Big Bias Hunting in Amazonia: Large-Scale Computation and Exploitation of RC4 Biases (Invited Paper)". Advances in Cryptology – ASIACRYPT 2014. Lecture Notes in Computer Science.****8874****. Information Security Group, Royal Holloway, University of London. pp. 398–419.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1007/978-3-662-45611-8\_21*](https://doi.org/10.1007%2F978-3-662-45611-8_21)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*978-3-662-45607-1*](https://en.wikipedia.org/wiki/Special:BookSources/978-3-662-45607-1)*.*
  12. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-12) [*"RC4 NOMORE"*](https://www.rc4nomore.com/)*. www.rc4nomore.com. Retrieved 2019-05-21.*
  13. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-13) [Wi-Fi Alliance to dump WEP and TKIP ... not soon enough](https://www.zdnet.com/blog/hardware/wi-fi-alliance-to-dump-wep-and-tkip-not-soon-enough/8677?tag=nl.e539)
  14. [**^**](https://en.wikipedia.org/wiki/Temporal_Key_Integrity_Protocol#cite_ref-14) *Vanhoef, Mathy; Piessens, Frank (May 2013).*[*Practical Verification of WPA-TKIP Vulnerabilities*](http://people.cs.kuleuven.be/~mathy.vanhoef/papers/wpatkip.pdf)*(PDF). Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security. ASIA CCS '13. pp. 427–436.*[*doi*](https://en.wikipedia.org/wiki/Doi_(identifier))*:*[*10.1145/2484313.2484368*](https://doi.org/10.1145%2F2484313.2484368)*.*[*ISBN*](https://en.wikipedia.org/wiki/ISBN_(identifier))[*9781450317672*](https://en.wikipedia.org/wiki/Special:BookSources/9781450317672)*.*