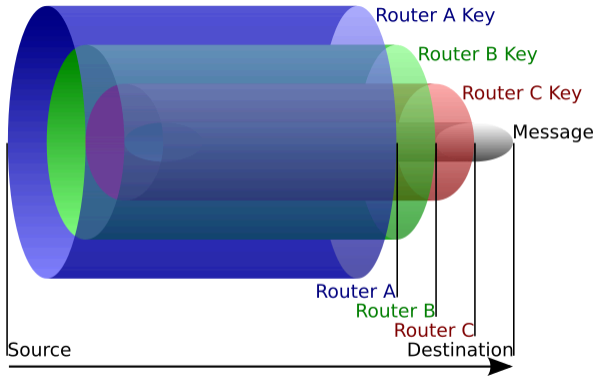
Onion routing

Onion routing is a technique for anonymous communication over a computer network. In an **onion network**, messages are encapsulated in layers of encryption, analogous to the layers of an onion. The encrypted data is transmitted through a series of network nodes called "**onion routers**," each of which "peels" away a single layer, revealing the data's next destination. When the final layer is decrypted, the message arrives at its destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.[1] While onion routing provides a high level of security and anonymity, there are methods to break the anonymity of this technique, such as timing analysis.[2]



In this example onion, the source of the data sends the onion to Router A, which removes a layer of encryption to learn only where to send it next and where it came from (though it does not know if the sender is the origin or just another node). Router A sends it to Router B, which decrypts another layer to learn its next destination. Router B sends it to Router C, which removes the final layer of encryption and transmits the original message to its destination.

History

Onion routing was developed in the mid-1990s at the U.S. Naval Research Laboratory by employees Paul Syverson, Michael G. Reed, and David Goldschlag[3][4] to protect U.S. intelligence communications online.[5] It was then refined by the Defense Advanced Research Projects Agency (DARPA) and patented by the Navy in 1998.[4][6][7]

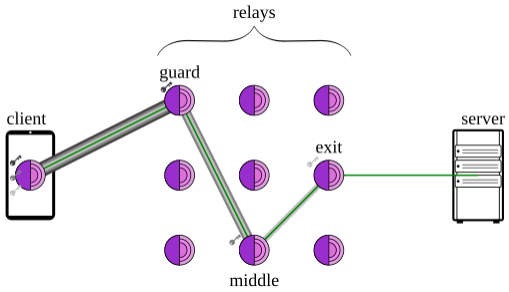
This method was publicly released by the same employees through publishing an article in the IEEE Journal on Selected Areas in Communications the same year. It depicted the use of the method to

protect the user from the network and outside observers who eavesdrop and conduct traffic analysis attacks. The most important part of this research is the configurations and applications of onion routing on the existing e-services, such as Virtual private network, Web-browsing, Email, Remote login, and Electronic cash.[8]

Based on the existing onion routing technology, computer scientists Roger Dingledine and Nick Mathewson joined Paul Syverson in 2002 to develop what has become the largest and best-known implementation of onion routing, then called The Onion Routing project (Tor project).

After the Naval Research Laboratory released the code for Tor under a free license,[5][9][10] Dingledine, Mathewson and five others founded The Tor Project as a non-profit organization in 2006, with the financial support of the Electronic Frontier Foundation and several other organizations.[11][12]

Data



A diagram of an onion routed connection, using Tor's terminology of guard, middle, and exit relays

Metaphorically, an onion is the data structure formed by "wrapping" a message with successive layers of encryption to be decrypted ("peeled" or "unwrapped") by as many intermediary computers as there are layers before arriving at its destination. The original message remains hidden as it is transferred from one node to the next, and no intermediary knows both the origin and final destination of the data, allowing the sender to remain anonymous.[13]

Onion creation and transmission

To create and transmit an onion, the originator selects a set of nodes from a list provided by a "directory node". The chosen nodes are arranged into a path, called a "chain" or "circuit", through which the message will be transmitted. To preserve the anonymity of the sender, no node in the circuit is able to tell whether the node before it is the originator or another intermediary like itself.

Likewise, no node in the circuit is able to tell how many other nodes are in the circuit and only the final node, the "exit node", is able to determine its own location in the chain.[13]

An onion node in use.

Using asymmetric key cryptography, the originator obtains a public key from the directory node to send an encrypted message to the first ("entry") node, establishing a connection and a shared secret ("session key"). Using the established encrypted link to the entry node, the originator can then relay a message through the first node to a second node in the chain using encryption that only the second node, and not the first, can decrypt. When the second node receives the message, it establishes a connection with the first node. While this extends the encrypted link from the originator, the second node cannot determine whether the first node is the originator or just another node in the circuit. The originator can then send a message through the first and second nodes to a third node, encrypted such that only the third node is able to decrypt it. The third, as with the second, becomes linked to the originator but connects only with the second. This process can be repeated to build larger and larger chains but is typically limited to preserve performance.[13]

When the chain is complete, the originator can send data over the Internet anonymously. When the final recipient of the data sends data back, the intermediary nodes maintain the same link back to the originator, with data again layered, but in reverse such that the final node this time adds the first layer of encryption and the first node adds the last layer of encryption before sending the data, for example a web page, to the originator, who is able to decrypt all layers.[13]

Weaknesses

Timing analysis

One of the reasons why the typical Internet connections are not considered anonymous is the ability of Internet service providers to trace and log connections between computers. For example, when a person accesses a particular website, the data itself may be secured through a connection like HTTPS such that the user's password, emails, or other content is not visible to an outside party, but there is a record of the connection itself, what time it occurred, and the amount of data transferred. Onion routing creates and obscures a path between two computers such that there is no discernible connection directly from a person to a website, but there still exist records of connections between computers. Traffic analysis searches those records of connections made by a potential originator and tries to match the timing and data transfers to connections made to a potential recipient. If an attacker has compromised both ends of a route, a sender may be seen to have transferred an amount of data to an unknown computer a specified amount of seconds before a different unknown computer transferred data of the same exact size to a particular destination.[14][15] Factors that may facilitate traffic analysis include nodes failing or leaving the network[15] and a compromised node keeping track of a session as it occurs when chains are periodically rebuilt.[16]

Garlic routing is a variant of onion routing associated with the I2P network that encrypts multiple messages together, which both increases the speed of data transfer and makes it more difficult[17] for attackers to perform traffic analysis.[18]

Exit node vulnerability

Although the message being sent is transmitted inside several layers of encryption, the job of the exit node, as the final node in the chain, is to decrypt the final layer and deliver the message to the recipient. A compromised exit node is thus able to acquire the raw data being transmitted, potentially including passwords, private messages, bank account numbers, and other forms of personal information. Dan Egerstad, a Swedish researcher, used such an attack to collect the passwords of over 100 email accounts related to foreign embassies.[19]

Exit node vulnerabilities are similar to those on unsecured wireless networks, where the data being transmitted by a user on the network may be intercepted by another user or by the router operator. Both issues are solved by using a secure end-to-end connection like SSL/TLS or secure HTTP (S-HTTP). If there is end-to-end encryption between the sender and the recipient, and the sender isn't

lured into trusting a false SSL certificate offered by the exit node, then not even the last intermediary can view the original message.

See also

- Anonymous remailer
- Bitblinder
- Chaum mixes
- Cryptography
- Degree of anonymity
- Diffie–Hellman key exchange
- Java Anon Proxy
- Key-based routing
- Matryoshka doll
- Mix network
- Mixmaster anonymous remailer
- Public-key cryptography
- Proxy server
- Tox – implements onion routing
- Tribler – implements onion routing

References

1. Goldschlag D., Reed M., Syverson P. (1999.) Onion Routing for Anonymous and Private Internet Connections (http://www.onion-router.net/Publications/CACM-1999.pdf) , Onion Router.
2. Soltani, Ramin; Goeckel, Dennis; Towsley, Don; Houmansadr, Amir (2017-11-27). "Towards Provably Invisible Network Flow Fingerprints". *2017 51st Asilomar Conference on Signals, Systems, and Computers*. pp. 258–262. arXiv:1711.10079 (https://arxiv.org/abs/1711.10079) . doi:10.1109/ACSSC.2017.8335179 (https://doi.org/10.1109%2FACSSC.2017.8335179) . ISBN 978-1-5386-1823-3. S2CID 4943955 (https://api.semanticscholar.org/CorpusID:4943955) .
3. Reed M. G., Syverson P. F., Goldschlag D. M. (1998) "Anonymous connections and onion routing", IEEE Journal on Selected Areas in Communications, 16(4):482–494.
4. US patent 6266704 (https://worldwide.espacenet.com/textdoc?DB=EPODOC&IDX=US6266704) , Reed; Michael G. (Bethesda, MD), Syverson; Paul F. (Silver Spring, MD), Goldschlag; David M. (Silver Spring, MD), "Onion routing network for securely moving data through communication networks", assigned to The United States of America as represented by the Secretary of the Navy (Washington, DC)

5. Levine, Yasha (16 July 2014). "Almost everyone involved in developing Tor was (or is) funded by the US government" (http://pando.com/2014/07/16/tor-spooks/) . *Pando Daily*. Retrieved 30 August 2014.
6. Fagoyinbo, Joseph Babatunde (2013-05-24). *The Armed Forces: Instrument of Peace, Strength, Development and Prosperity* (https://books.google.com/books?id=qM0uxPH8RasC&q=The+Armed+Forces%3A+Instrument+of+Peace%2C+Strength%2C+Development+and+Prosperity) . AuthorHouse. ISBN 9781477226476. Retrieved August 29, 2014.
7. Leigh, David; Harding, Luke (2011-02-08). *WikiLeaks: Inside Julian Assange's War on Secrecy* (https://books.google.com/books?id=qGLjvFNuaM4C&q=WikiLeaks%3A+Inside+Julian+Assange%27s+War+on+Secrecy) . PublicAffairs. ISBN 978-1610390620. Retrieved August 29, 2014.
8. Reed, M. G.; Syverson, P. F.; Goldschlag, D. M. (May 1998). "Anonymous connections and onion routing". *IEEE Journal on Selected Areas in Communications*. **16** (4): 482–494. doi:10.1109/49.668972 (https://doi.org/10.1109%2F49.668972) . ISSN 1558-0008 (https://search.worldcat.org/issn/1558-0008) .
9. Dingledine, Roger (20 September 2002). "pre-alpha: run an onion proxy now!" (http://archives.seul.org/or/dev/Sep-2002/msg00019.html) . *or-dev* (Mailing list). Retrieved 17 July 2008.
10. "Tor FAQ: Why is it called Tor?" (https://www.torproject.org/docs/faq#WhyCalledTor) . *Tor Project*. Retrieved 1 July 2011.
11. "Tor: Sponsors" (https://www.torproject.org/about/sponsors.html.en) . *Tor Project*. Retrieved 11 December 2010.
12. Krebs, Brian (8 August 2007). "Attacks Prompt Update for 'Tor' Anonymity Network" (https://web.archive.org/web/20110427104755/http://voices.washingtonpost.com/securityfix/2007/08/attacks_prompt_update_for_tor.html) . *Washington Post*. Archived from the original (http://voices.washingtonpost.com/securityfix/2007/08/attacks_prompt_update_for_tor.html) on April 27, 2011. Retrieved 27 October 2007.
13. Roger Dingledine; Nick Mathewson; Paul Syverson. "Tor: The Second-Generation Onion Router" (http://www.onion-router.net/Publications/tor-design.pdf) (PDF). Retrieved 26 February 2011.
14. Shmatikov, Wang; Ming-Hsiu Vitaly (2006). "Timing Analysis in Low-Latency Mix Networks: Attacks and Defenses". *Computer Security – ESORICS 2006*. ESORICS'06. Vol. 4189. pp. 18–33. CiteSeerX 10.1.1.64.8818 (https://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.64.8818) . doi:10.1007/11863908_2 (https://doi.org/10.1007%2F11863908_2) . ISBN 978-3-540-44601-9. `{{cite book}}: |journal=` ignored (help)

15. Dingledine, Roger; Mathewson, Nick; Syverson, Paul (August 2004). "Tor: The Second-Generation Onion Router" (https://svn.torproject.org/svn/projects/design-paper/tor-design.html) . San Diego, CA: USENIX Association. Retrieved 24 October 2012.
16. Wright, Matthew. K.; Adler, Micah; Levine, Brian Neil; Shields, Clay (November 2004). "The Predecessor Attack: An Analysis of a Threat to Anonymous Communications Systems" (https://web.archive.org/web/20160304185948/https://gnunet.org/sites/default/files/Wright-2004.pdf) (PDF). *ACM Transactions on Information and System Security*. **7** (4): 489–522. doi:10.1145/1042031.1042032 (https://doi.org/10.1145%2F1042031.1042032) . S2CID 7711031 (https://api.semanticscholar.org/CorpusID:7711031) . Archived from the original (https://gnunet.org/sites/default/files/Wright-2004.pdf) (PDF) on 2016-03-04. Retrieved 2012-07-04.
17. "Common Darknet Weaknesses: An Overview of Attack Strategies" (https://privacy-pc.com/articles/common-darknet-weaknesses-2-tor-and-i2p.html) . 27 January 2014.
18. Zantour, Bassam; Haraty, Ramzi A. (2011). "I2P Data Communication System". *Proceedings of ICN 2011: The Tenth International Conference on Networks*: 401–409.
19. Bangeman, Eric (2007-08-30). "Security researcher stumbles across embassy e-mail log-ins" (https://arstechnica.com/news.ars/post/20070830-security-researcher-stumbles-across-embassy-e-mail-log-ins.html) . Ars Technica. Retrieved 2010-03-17.

External links

- Onion-Router.net (http://www.onion-router.net) – site formerly hosted at the Center for High Assurance Computer Systems of the U.S. Naval Research Laboratory
- Syverson, P.F.; Goldschlag, D.M.; Reed, M.G. (1997). "Anonymous connections and onion routing" (https://apps.dtic.mil/sti/pdfs/ADA465126.pdf) (PDF). *Proceedings. 1997 IEEE Symposium on Security and Privacy*. pp. 44–54. doi:10.1109/SECPRI.1997.601314 (https://doi.org/10.1109%2FSECPRI.1997.601314) . ISBN 0-8186-7828-3. S2CID 1793921 (https://api.semanticscholar.org/CorpusID:1793921) .