CRYPTOGRAPHY

Definitions of secrecy

Asked 3 years, 3 months ago Active 1 year, 2 months ago Viewed 2k times

9

I found terms like "forward secrecy", "future secrecy", "backwards secrecy" and "perfect forward secrecy" and I would like to know their definitions and to understand the differences among them. I found several confusing definitions online, especially mixing up the meanings of forward secrecy with perfect forward secrecy, or the meanings of forward with backwards secrecy. Thank you.

★ 3

perfect-secrecy forward-secrecy

edited Sep 5 '16 at 13:07

asked Sep 3 '16 at 15:55
M-elman
978 ● 1 ● 7 ● 19

1 The question is quite broad. Maybe you could narrow it down by indicating the exact notions of security you want to know more about? – Guut Boy Sep 3 '16 at 19:00

2 Forward Secrecy and Perfect Forward Secrecy are often used interchangeably. In the context of e.g. TLS it means if a long term key (i.e. the one in a cert) is compromised previous sessions are not also compromised as a result. – puzzlepalace Sep 3 '16 at 19:35

@GuutBoy I just need to define the concepts of forward, backwards (which I understood from online researches may be a synonym of future, even if I don' get why: backward = past while future= ...future) and perfect forward secrecy. – M-elman Sep 5 '16 at 12:57

@puzzlepalace What do you mean with "the one in a cert"? And then, is there no difference between forward secrecy and perfect forward secrecy? – M-elman Sep 5 '16 at 12:57

2 Answers

3

✓

In cryptography, forward secrecy = perfect forward secrecy, backward secrecy = future secrecy.

First, recall some background. The above terms are often discussed in the setting of secure channel establishment protocols, e.g., TLS, Signal, etc. In such a protocol, consider two parties, a client and a server, try to communicate with each other securely. The server (and the client if client-authentication is needed) is granted a certificate that shows its public key, and the server (and the client) itself knows the corresponding private key (a.k.a. the long-term secret). They essentially use the long-term secret and some randomness to compute and

Forward secrecy means if the long-term secret (together with the party's current session key and all other secret states) is corrupted (i.e., revealed), then the *past* sessions are still secure, i.e., the confidentiality of the previous messages exchanged between the client and the server is not compromised. I think people call this forward secrecy because they want the encrypted messages in a session to be secure even if "forward" long-term key corruption occurs. [TLS](#) is an example that achieves forward secrecy with [Diffie-Hellman key exchange](#).

Then, as you may guess, backward secrecy guarantees the "opposite direction" of forward secrecy. In other words, this security guarantees that the encrypted messages in a session should remain secure even if "backward" long-term key corruption occurs. People more often call this future secrecy perhaps because they want to emphasize that even if at some point the long-term secret (together with the party's current session key and all other secret states) is corrupted the *future* messages can still be secure (if the previously corrupted party somehow becomes "clean" again). (I agree that the terms are a mess because "future secrecy" looks and sounds almost the same as "forward secrecy".) [Signal](#) is an example that achieves backward secrecy with the [Double Ratchet Algorithm](#) which can self-heal itself soon after corruption.

edited Sep 14 '18 at 5:34

answered Sep 14 '18 at 4:49

Shan Chen
2,340 ● 1 ● 6 ● 14

Thanks a lot for your answer to this old question! I chose your answer over @ShobhanMandal's one - whom I thank, too - because reflects better the definitions I found in some further researchs I've done (google.it/url?sa=t&source=web&rct=j&url=https://…) and matches the same interpretation I gave to the terms involved. – M-elman Sep 15 '18 at 16:05

@M-elman My pleasure! Yes, I provided an answer because I don't think Shobhan's answer matches the current security notions in crypto research about secure channel establishment protocols. But my answer also glosses over some subtleties. – Shan Chen Sep 15 '18 at 16:42

3

Forward secrecy: When a node (user) leaves the network, it must not read any future messages after its departure. **Backward secrecy:** When a new node (user) joins in the network, it must not read any previously transmitted message. [Crytographics properties](#)

Perfect Forward Secrecy : Perfect forward secrecy means that a piece of an encryption system automatically and frequently changes the keys it uses to encrypt and decrypt information, such that if the latest key is compromised, it exposes only a small portion of the user’s sensitive data. Encryption tools with perfect forward secrecy switch their keys as frequently as every message in text-based conversation, every phone call in the case of encrypted calling apps, or every time a user loads or reloads an encrypted web page in his or her browser. [What is perfect forward secrecy?](#)

If you search out for [Double Ratchet Alogrithm](#), you will find that it has the property of **future secrecy**.

> The developers refer to the algorithm as self-healing because under certain conditions, it
>
> disables an attacker from accessing the cleartext of messages ("the communication") after having compromised a session key.[3] This condition is that between the compromise of the key and the communication in question, there has been at least one message which was

> key and the communication in question, there has been at least one message which was not tampered with by the attacker. This effectively forces the attacker to intercept all communication between the honest parties, since he loses access as soon as one uncompromised message is passed between them. This property was later named Future Secrecy, or Post-Compromise Security

answered Sep 13 '18 at 18:22
Shobhan Mandal
39 ● 2

IMHO for perfect forward secrecy we would require even master key leakage to keep past intercepted messages safe. Safety in the face of loosing a session key is easy. – Meir Maor Sep 14 '18 at 3:55

Meir, certainly! In Handbook of Applied Cryptography, the Perfect Forward Secrecy is defined as ability to face losing long-term keys, without compromising the past messages. So, if key master key is lost, the past communication is still locked - we can only move forward (like impersonating the party, as we have master key compromised). – Victor Farazdagi Dec 3 at 16:37