How Do Hardware Token Devices work? [closed]

Asked 10 years, 4 months ago Modified 4 years ago Viewed 60k times

39

Closed. This question needs to be more focused. It is not currently accepting answers.

Want to improve this question? Update the question so it focuses on one problem only by editing this post.

Closed 3 years ago.

Improve this question

Recently, my bank sent me this tiny device that generates a unique code that must be used when performing online transactions, all the device does is generate this unique code when I press a particular white button and it doesn't look like it connects to a remote server or anything of such.

I did some research and ended up in cryptography with something called the Hash function but I still don't get it.

My Questions

- How does my bank's servers know the code generated by this device is correct?

- Since it just generates five random digits every 30 seconds, why won't the server authenticate a random number I have also decided to use?

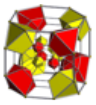
hash cryptography hmac two-factor-authentication one-time-password

Share

Improve this question

Follow

edited Oct 28, 2015 at 16:44



Patrick M

11k ● 9 ● 71 ● 104

asked Aug 11, 2014 at 17:26

Feyisayo Sonubi

1,072 ● 5 ● 15 ● 28

6 If it's time based the obvious choice is TOTP, if it generates on each button press the obvious choice is HOTP. (They're essentially the same thing, the former using the time, the latter a counter) – CodesInChaos Aug 11, 2014 at 17:28

2 Actually, it generates the digits on a time-based interval, if I press the button for it to generate the digits, it generates the digits and after about 25 seconds, I press it again, the digits change not when I press it again immediately after I'd just pressed it. – Feyisayo Sonubi Aug 11, 2014 at 17:34

2 This question appears to be off-topic because it is not about programming. – Eugene Mayevski 'Callback Aug 11, 2014 at 20:13

3 It may also interest you that some two-factor authentication schemes actually receive a code from the server, usually via a cell phone over SMS. The idea is that if you're in

possession of your phone, you're more likely to be you than not. This can make use of any number of encryption schemes to ensure that the transmissions are not intercepted. – Patrick M Oct 28, 2015 at 16:42

3 I'm voting to close this question because it's not a programming question. – cigien Dec 8, 2020 at 22:05

1 Answer

Sorted by: Highest score (default)

54

This has very little to do with hash functions. A cryptographic hash function may be part of the implementation, but it's not required.

> Actually, it generates the digits on a time-based interval, if I press the button for it to generate the digits, it generates the digits and after about 25 seconds, and I press it again, the digits change not when I press it again immediately after I'd just pressed it.

There's your hint. It's a time based pseudo-random or cryptographic algorithm. Based on the time, there is a code. The dongle and the server know – or rather, can compute – the code for every window. This is a shared secret - the dongle does not connect to a remote server. The server will probably allow one or two of the most recent secret keys, to prevent the situation where you enter a key that has *just* expired while the transmission was en route.

(Although my recent experience with Amazon Web Service multi-factor authentication has definitely resulted in login failures within 5 seconds of a code being displayed to me. In other words, some vendors are very strict with their timing windows. As always, it's a trade-off between security and usability.)

The abbreviations **CodesInChaos** mention are Time-based One-Time Password (TOTP) and HMAC-based One-Time Password (HOTP), two algorithms commonly used in two-factor authentication.

Wikipedia has this to say about the RSA SecurID, a particular brand of two-factor-authentication dongle.

> The RSA SecurID authentication mechanism consists of a "token" — either hardware (e.g. a USB dongle) or software (a soft token) — which is assigned to a computer user and which generates an authentication code at fixed intervals (usually 60 seconds) using a built-in clock and the card's factory-encoded random key (known as the "seed"). The seed is different for each token, and is loaded into the corresponding RSA SecurID server (RSA Authentication Manager, formerly ACE/Server) as the tokens are purchased.

I chose this article because it has a reasonable, physical description; the higher-level articles focus on the theoretical over the physical implementation.

The article also confirms that you need to keep the secrecy of the token, or someone else can impersonate your logins by knowing what the codes are as easily as you do.

> The token hardware is designed to be tamper-resistant to deter reverse engineering. When software implementations of the same algorithm ("software tokens") appeared on the market, public code has been developed by the security community allowing a user to emulate RSA SecurID in software, but only if they have access to a current RSA SecurID code, and the original 64-bit RSA SecurID seed file introduced to the server.

However, since the verifying server *has to have foreknowledge of the tokens*, the two-factor secrets are vulnerable to attacks on the source as well. SecurID was the victim of a high-profile theft that targeted their own servers and eventually led to secondary incursions on their clients' servers as well.

Finally, there is more information available on the security.stackexchange sister-site under the multi-factor tag, and also on this site under the `two-factor-authentication` tag.

Share Improve this answer

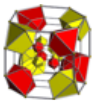
Follow

edited May 22, 2018 at 4:24

pensebien

554 ● 5 ● 16

answered Aug 11, 2014 at 18:03



Patrick M

11k ● 9 ● 71 ● 104

1 I have a device from Rabobank, a bank in Netherland which displays all the information about my transaction before I approve. How is this enabled in the hardware device?
– Anand Sep 6, 2016 at 7:40

And you approve with a button push, not a code you type into their online transaction form? That would necessitate some form of 2-way communication on the device: wifi, bluetooth or cellular. Or maybe a lower-tech 2-way pager system. Do you have to charge this device or replace the batteries on it?
@Anand – Patrick M Sep 6, 2016 at 15:10

1 The comes with 2 AA batteries and I am using it for more than a year. So the procedure works as follows: For login, I insert the card, scan the QR code on the screen and type my password for authentication in the device. When I do a transaction, the system shows a QR code which I scan to get purchase info and authenticate. When I just say authenticate in the device, the system moves to the next screen stating the successful transaction (I don't type any code or scan anything. It is just a click in the device). I have tried this device from many countries and it works very reliably.
– Anand Sep 7, 2016 at 13:51

2 AA batteries sounds like it definitely has to be a pager. Pagers operate by radio signal: lower power, longer range and less bandwidth than cellular signal. I'm sure they have a very specific frequency modulation and encryption scheme, but your bank would be the one to ask for more details. They might be reluctant to disclose, but disclosure is the only way to know if they're actually securing your verifications.
– Patrick M Sep 7, 2016 at 15:56

I googled about pager! I think this should be the only way they can communicate. But if there is a low-bandwidth comunication link all over the world with very less power consumption why it is not very popular?? – Anand Sep 8, 2016 at 12:35

Highly active question. Earn 10 reputation (not counting the association bonus) in order to answer this question. The reputation requirement helps protect this question from spam and non-answer activity.