

Forum:[Hack Forums](#)

Thread: [Review my new SSP MAZE HandShake for Vulnerabilities](#)

DragonHunter - August 3, 2014, 11:26 am

Hey whats up,

I wrote a doc about my new Handshake for a library I'm going to make SSP3 (<https://github.com/AnguisCaptor/SecureSocketProtocol3>)

I did not completely finished the doc yet but it looks good so far so I was hoping to see some opinions.

Let me know what you think, I hope I explained enough in the doc,
If you find any vulnerabilities which could occur let me know in a PM or just as post here.

<https://docs.google.com/document/d/1SBUniJcKrHFzGDfBhX3rGU17TDVJi1WF1wQXbiZ1rK0/edit?usp=sharing>

It starts at the second page ?

My goal in this Handshake is to make it so secure as possible.

crazyycast13 - August 3, 2014, 2:15 pm

I'll check it out. Have you posted this algo on other forums, or am I doing the first run through? If anyone ever makes changes to whatever, make sure they do it in a different color and also make sure it's color coded.

DragonHunter - August 3, 2014, 2:35 pm

(Aug 3, 2014 02:15 PM)crazyycast13 Wrote: [\[CITE\]](#) I'll check it out. Have you posted this algo on other forums, or am I doing the first run through? If anyone ever makes changes to whatever, make sure they do it in a different color and also make sure it's color coded.I suppose you're the first one, only posted it in HF

DragonHunter - August 3, 2014, 11:14 pm

(Aug 3, 2014 03:32 PM)crazyycast13 Wrote: [\[CITE\]](#) I do not understand what you meant by
Can you explain what you mean by that or how you came to that conclusion?

<https://hackforums.net/showthread.php?tid=3166960>
<https://hackforums.net/showthread.php?tid=4048467>
<https://twitter.com/AnguisCaptor/status/493137224486367232>

And more private stuff but ain't going to show that

crazyycast13 - August 3, 2014, 11:14 pm

I do not understand what you meant by Quote:RSA and Diffie-Hellman are both vulnerable because they both generate a new key, it's TOO RANDOM to be secure

Can you explain what you mean by that or how you came to that conclusion?

I don't see how this could work out. I was looking at the documents, but do you understand how DH works? If you reeeeeaaaaally want to try it out, go ahead, I won't stop you. But I will say that I don't see the point of your MAZE algorithm. There are too many security flaws in the algorithm for it to be even remotely safe. You're doing the equivalent of storing plaintext passwords inside of a database.

hmm.

I saw your videos, I'll post what I wrote on the doc on the thread too.

Quote:There's nothing you can do when someone implements cryptography the wrong way. That's what all hackers look for, and I assume you look for this too, as I saw in the videos.

And that's why people like me will always have a job. We're here to check out if you implemented whatever crazy ass crypto algo correctly. If someone uses a weak algorithm to create random numbers, then it is their fault, not DH's. However, it is DH's fault that it provides ABSOLUTELY FUCK ALL protection from proper MITM attacks, which you did in those videos. So I guess either make a stronger random number generator or make an easy way for a server to recognize the difference between a masked man and the poor 13 gamer who wants to play (but is going to wind up DDOSing their servers anyways).

DragonHunter - August 3, 2014, 11:25 pm

(Aug 3, 2014 11:14 PM)crazyycast13 Wrote: [\[CITE\]](#) I do not understand what you meant by Can you explain what you mean by that or how you came to that conclusion?

I don't see how this could work out. I was looking at the documents, but do you understand how DH works? If you reeeeeaaaaally want to try it out, go ahead, I won't stop you. But I will say that I don't see the point of your MAZE algorithm. There are too many security flaws in the algorithm for it to be even remotely safe. You're doing the equivalent of storing plaintext passwords inside of a database. Could you point out the flaws, and yes I know how DH works and it's just cheese with a lot of holes in it

Added you on Skype btw

ytlayol - August 19, 2014, 7:38 am

your algorithm requires a pre-sync right?

OFF-Topic: well it is known that DH is vulnerable to Man In The Middle attacks but so far it is the best way to establish a shared secret between two hosts which don't have a prior contact with each other.

Quote:The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. -wiki

In DH the only possible way for an attacker to do a MITM attack is by establishing two shared secrets. one between attacker and client, the other one between attacker and server. This can be prevented by the use of RSA(Given that the public key is not transmitted).

I was just going through it but I don't quite get the reason why are you sending prime/non-prime could have used 0 or 1...? There is no apparent reason for doing so...the 32 byte preamble is enough to let the attacker know its MAZE we are talking about...and yeah a 32 byte preamble isn't a little too much.

"I'll post when I go through the whole paper

Step 10:

Quote: The server will send a Big Prime number back so the client can verify if the connection went successful, the Prime Number will get encrypted by using the hashed Username as Key and the User's Hashed Password as Salt, the client knows both already.

lets say an attacker is bridging the data between client and server, he manages to save to responses i.e an encrypted Prime number and an encrypted non-prime number. as the username and password will remain the same so these responses will be valid forever right....?until or unless the password is changed. Just by forwarding these responses an attacker can manage to force the client/server to recalculate the private key even though the authentication was unsuccessful?which will lead to....

Step 11) what kind of ACK we are taking about?