strongSwan - Feature #1559

Expose received XAUTH/EAP username/password prompts via VICI, send secrets via VICI on prompt

07.07.2016 20:19 - Noel Kuntze

Status:	Feedback	**Start date:**	07.07.2016
Priority:	Normal	**Due date:**	
Assignee:		**Estimated time:**	0.00 hour
Category:			
Target version:			
Resolution:			

Description

Hello,

In order to build a usable IPsec client for Desktop users on the basis of charon, it would be necessary to expose any received XAUTH/EAP username/password (or OTP) prompts to the user.
As can be seen on the article about the eap-radius plugin, a responder can send arbitrary fields and descriptions to the initiator. The number and description of the fields can not be foreknown or actually configured in ipsec.secrets or swanctl.conf (therefore probably currently also not configured via VICI itself).
Furthermore, exposing a password prompt to access a known pkcs11 card would be nice, too.

I am asking for the implementation of a feature that exposes the received XAUTH/EAP profiles via VICI and waits for a response in a configurable timeout.
When the user has entered his secrets, the information should be conveyed to charon via VICI and used to continue the authentication.

Implementing such a feature would allow me to implement a largely functional IPsec/IKE client on Windows with support for arbitrary authentication profiles.

Kind Regards,
Noel

History

#1 - 11.07.2016 16:31 - Tobias Brunner

- Status changed from New to Feedback

> As can be seen on the article about the eap-radius plugin, a responder can send arbitrary fields and descriptions to the initiator. The number and description of the fields can not be foreknown or actually configured in ipsec.secrets or swanctl.conf (therefore probably currently also not configured via VICI itself).

That's a legacy feature, which only some proprietary clients support. strongSwan as a client does not really support multiple secrets anyway as these are tied to identities of which there is only one (unless there are multiple authentication rounds, which is not the case with that XAuth thingy). And supporting XAuth in a new client seems futile as IKEv1 should finally die, die, die! And the most common use case is definitely a single password (perhaps combined with a certificate).

By implementing callback_cred_t a plugin could theoretically prompt a user for a shared secret dynamically. However, besides the identities and type (SHARED_EAP in this case) the callback does not receive any information. So there is currently no way to pass a message or subtype received via XAuth so it could be displayed to the user (I suppose identities could be misused for that somehow, or by implementing an XAuth client so these things could be intercepted). callback_cred_t is currently used by the *stroke* plugin to implement %prompt in ipsec.secrets, however, this happens only temporarily when reloading the secrets, not when secrets are actually used while establishing a connection (there is no interface to prompt the user at that point). *charon-cmd* does use it more dynamically as does *charon-xpc*. The other clients (NM, Android) prompt the user before initiating the connection.

> I am asking for the implementation of a feature that exposes the received XAUTH/EAP profiles via VICI and waits for a response in a configurable timeout.

Again, this is an XAuth-specific legacy feature. So I don't see us adding something like that.

There is currently also no way to request any information from a VICI client. I guess in the future we could add some kind of callback/event feature that allows providing shared secrets via VICI dynamically (basically via callback_cred_t and similar to what *charon-cmd/xpc* implement).

#2 - 09.05.2017 16:28 - Noel Kuntze

Okay, so I guess I'd need to write it myself, if I need/want it.
I agree, that IKEv1 should die. But we can't force other people to do that. Giving users the option to connect to proprietary IKE responders using strongSwan would give them more freedom regarding their choice of operating system, because a lot of vendors that have their own IKE daemons in their firewalls need/use a proprietary client that only works on Windows. A good desktop client for Windows based on strongSwan would be pretty rad, because it gives people the option to avoid the problems that the native Windows client has.

PS: Would a patch set be acceptable?