Minutes from EMU WG at IETF 83

The meeting started at 1521 CEST. Joe and Alan were chairing. The NOTE WELL was displayed and explained.

Agenda-bashing and WG status

The agenda was reviewed. No changes needed.

Channel Bindings

Sam gave an implementation report on channel bindings. He worked on implementing channel bindings for EAP-TTLS. Should be easy, right? Just allocate a Diameter AVP and use it. But many people use RADIUS-based EAP servers for TTLS and they don't know what to do with a Diameter AVP that isn't a RADIUS AVP. Many of them just throw away the whole packet, which totally messes things up. They decided to try stuffing the Diameter AVP inside a RADIUS VSA but that also resulted in the whole packet being discarded. So what should they do? Squat on an unused RADIUS attribute? Another problem is that many RADIUS servers throw out EAP Success without waiting for channel bindings. The bottom line is that they got it working in the end but it was messy. You should expect problems when using channel bindings, especially with older EAP methods and RADIUS servers.

TEAP (Tunnel EAP)

Hao presented on the TEAP method. Thanks to all those who have submitted comments. He reviewed all the comments submitted and explained how they were resolved.

Joe Salowey asked why we don't just use EST for certificate provisioning. Hao said this our technique a lot simpler. We don't need all the stuff in EST. Joe said the EST offers some good advice about putting tls-unique in the PKCS#10. At least, we should leverage as much of that work as possible. Sean Turner said we should the PKCS#10 request as in EST. Hao asked if we want to put a dependency on EST. Sean said we can copy for now to avoid a dependency and change to a pointer if EST gets finished before TEAP or about at the same time. Dan Harkins said using tls-unique isn't a good idea if an anonymous ciphersuite is used. Sam said that's not a problem. We'll be saying "I want to establish a certificate using this TLS channel". The tls-unique value is the right way to do that. Hao asked if it's OK to use tls-unique for multiple purposes. Sam said that's fine.

On Issue 42 (SASLPrep), Sam recommended not doing any prep on the client. Just send the data to the server and let it do the processing. Jim Schaad said we might be changing the set of characters permitted in usernames and passwords. Sam said it's OK to permit indications from server to client about that sort of thing but often they won't know because there may be multiple layers behind the server. Jim said we should remove all text about SASLPrep from this spec. Sam said it's probably OK to advise the server to do something like SASLPrep. Sean said it's better to stop mentioning SASLPrep. Just say "send UTF-8".

On Issue 47 (Session-Id), Sam pointed out that the current definition is not cryptographically strong. Either we should choose something stronger or warn people to not use it anywhere that cryptographic properties are needed. Hao asked where EAP Session-Id is used. Joe said it's used in MACsec for a table lookup. Hao said we could use tls-unique. That's more secure. Hao asked people to review the current draft. Sean asked when we can get the WGLC. Can we do the WGLC in May and send the document to the IESG before the next IETF meeting? Sam said no way. This is important and difficult work. More issues will come up. Joe said that's right. New issues will come up. But we should get the next draft done in April. Sam said this method is a big improvement and a good basis for future work. Thanks to the authors.

Crypto Binding

Sam presented on Crypto Binding. He thanked his co-authors for their valuable assistance. With NEA and Channel Bindings, the peer needs to trust the EAP Server more. Today, peers generally use the server's certificate to decide whether it's trustworthy. In the past, tunnel-based attacks have been concerned with making sure that attackers can't get onto the network by using the credentials of an authorized user. But with channel bindings, we need to make sure the statement comes from a trustworthy EAP server. Unfortunately, there's an attack where the peer creates an EAP tunnel to an attacker instead of the proper EAP server. The attacker might be a valid AAA server but not a very trustworthy one.

Sam pointed out that crypto binding is not enough. It's based on the MSK, which is revealed to everyone in the AAA fabric. How can we prevent this? Policy is a hard way to solve it.

Sam suggests using EMSK to decide when the server is trusted. But he says that's not a panacea.

He recommends improving certificate handling, supporting EMSK crypto binding, and finding additional solutions.

Steve Hanna asked how this helps. How can the supplicant use the EMSK to verify server identity? Sam explained that it's a good way to ensure that the inner and outer method terminated at the same place. Of course, it's only useful with inner methods that export an EMSK.

We did a hum on whether EMU should consider mutual crypto binding in the TEAP method. The hum was unanimously positive. This will be taken to the list.

Joe asked whether we should take on mutual crypto binding as a WG activity. Nobody objected. This will be taken to the list.

Dan asked that we not make this slow down TEAP. Sam agreed. We should not have a normative reference from TEAP to mutual crypto bindings.

Certificate Validation

Jim Schaad presented on certificate validation for EMU. There are several interesting issues: trust anchor, matching PKIX cert to EAP server name, certificate revocation checking, etc.

He described how DANE works. Certificates are stored in signed DNS records, thereby allowing DNSSEC to be used to verify certificate validity. You can also do PKIX or not.

With DANE Stapling, all the DANE records are sent in a TLS extension. This can be used with tunnel EAP methods. It addresses the Trust Anchor and name matching issues.

A new draft on multiple OCSP stapling in TLS without PKIX can be used to send OCSP responses but it has some issues.

Several things need to happen: getting a DANE naming convention in EMU, a DANE stapling TLS extension, and the multiple OCSP stapling draft.

Stefan Winter raises concerns about the amount of data that would need to be sent over EAP.

Steve says we definitely need to get our PKIX validation text right in TEAP. Doing DANE would be nice also but it will take a few years.

EAP Support in Smartcards

Pascal Urien presented on draft-urien-eap-smartcard-22.txt. SIM cards, smartcards, NFC controllers, and other things have "Secure Elements", tamper-resistant microcontrollers. The draft defines a standard API for EAP on smartcards. He has created an open implementation of EAP-SIM, EAP-AKA, and EAP-TLS with this API. The benefit is that the MSK cannot be captured by malware on the endpoint. He recommends taking this draft to Experimental.

The meeting closed at 1705 CEST.