WHAT'S SO TRICKY ABOUT DOD'S PKI THAT IT NEEDS TO EXPOSE THOUSANDS OF SERVICE MEMBERS?

Motherboard decided to call out DOD for not using STARTTLS to encrypt the transiting email of much of DOD's emails.

> [A]s encryption spreads to government sites, it hasn't reached government emails yet. Most of the military as well as the intelligence community do not use encryption to protect emails travelling across the internet.
>
> [snip]
>
> In fact, according to an online testing tool, among the military only the Air Force encrypts emails in transit using a technology called STARTTLS, which has existed since 2002. Other branches of the Pentagon, including the Army, the Navy, the Defense Security Service, and DARPA, don't use it. Even the standard military email provider mail.mil, doesn't support STARTTLS.
>
> [snip]
>
> In a statement emailed to Motherboard, a spokesperson for the Defense Information Systems Agency (DISA), the Pentagon's branch that oversees email and other technologies, said the DISA's DOD Enterprise Email (DEE) does not support STARTTLS.

This part of the story is bad enough. I take it to mean that as people stationed overseas email home, their email — and therefore significant hints about deployment — would be accessible to

anyone who wanted to steal them in transit. While more sensitive discussions would be secure, there would be plenty accessible to Russia or China or technically savvy terrorists to make stealing the email worthwhile.

But I'm just as struck by DOD's excuse.

> "STARTTLS is an extension for the Post Office Protocol 3 and Internet Message Access protocols, which rely on username and password for system access," the spokesperson wrote. "To remain compliant with DOD PKI policy, DEE does not support the use of username and password to grant access, and does not leverage either protocol."

First of all, this doesn't make any sense. The Public Key Infrastructure system, which controls access to DOD networks, should be totally separate from the email system.

Worse still: we know a little bit about what — and when — DOD implemented its PKI, because it came up in Congressional hearings in the wake of the Chelsea Manning leaks. Here's what DOD's witnesses explained back in 2011.

> One of the major contributing factors in the WikiLeaks incident was the large amount of data that was accessible with little or no access controls. Broad access to information can be combined with access controls in order to mitigate this vulnerability. While there are many sites on SIPRNet that do have access controls, these are mostly password-based and therefore do not scale well. The administration of thousands of passwords is labor intensive and it is difficult to determine who should (and should not) have access.
>
> DoD has begun to issue a Public Key Infrastructure (PKI)-based identity credential on a hardened smart card.

> This is very similar to the Common Access Card (CAC) we use on our unclassified network. We will complete issuing 500,000 cards to our SIPRNet users, along with card readers and software, by the end of 2012. This will provide very strong identification of the person accessing the network and requesting data. It will both deter bad behavior and require absolute identification of who is accessing data and managing that access.
>
> In conjunction with this, all DoD organizations will configure their SIPRNetbased systems to use the PKI credentials to strongly authenticate end-users who are accessing information in the system. This provides the link between end users and the specific data they can access – not just network access. This should, based on our experience on the unclassified networks, be straightforward.
>
> DoD's goal is that by 2013, following completion of credential issuance, all SIPRNet users will log into their local computers with their SIPRNet PKI/smart card credential. This will mirror what we already do on the unclassified networks with CACs.

Remember, this describes the log-in process to DOD's classified network, generally, not to email.

The point is, though, that in response to an internal leaker, DOD only rolled out the kind of network controls most businesses have on its Secret (not Top Secret) network in 2011. Even if there were something about that roll-out that *did* impact email, what DOD would have you believe that as late as 2011, they made decisions that resulted in keeping email insecure in transit.