Outlook and SMIME/DNSSEC missing link found

Rick Lamb

- Microsoft Outlook is still very popular email client
- History of SMIME support
- Dan Kaminsky demoed a hack that pulled SMIME certs from DNS secured with DNSSEC in 2009
- Secure global distribution of SMIME certs – sounds like a killer app for DNSSEC to me….and I have said that for some time.
- So why hasn't anyone done this? Lets see…

- “our group” doesn’t like Microsoft? Maybe don’t like me.
- Unfamiliar world: CryptoAPI, Outlook plugins, CompletionPortIO, ..
- To be useful, must be supported, maintained, product
- No motivation?
- … > 3 million users in one organization, so maybe some reasons :-)

Demo: On machine A
(Demo A+B will take 10 minutes)

- Create a new email account
- Setup Outlook with this account
- Get an SMIME certificate for this account from CA
- Install the certificate in Outlook
- Generate SMIMEA DNS record
- Publish in DNS/DNSSEC

Demo: On machine B

- Try to send encrypted mail to new email - FAILS
- Download lvdt.exe and run
- Add entry to Outlook address book and restart Outlook
- Try to send encrypted mail again
- WORKS!

Hows it work?

- LDAP to DNSSEC validating DNS translator
- Converts DER.1 LDAP requests to DANE SMIMEA* DNS lookups
- DNSSEC validates responses in the same program on the local machine
- Converts back to DER.1 LDAP responses for Outlook to use as part of address book function
- Outlook uses returned certificate to encrypt email

* draft-ietf-dane-smime Hoffman/Schlyter

Finally

- End-2-end secure email for many-2-many (cross-organizational, trans-national … blah blah)

Links:

- Movie: www.co.tt/files/lvdt10min.mov
- ldap.lvdt.dc.org
- https://lvdt.dc.org