Getting Baseline Definitions for
draft-hoffman-uta-opportunistic-tls

Paul Hoffman, VPN Consortium

IETF London, March 2014

v2

History of “opportunistic encryption”

- 15ish years ago, FreeSWAN and others started promoting the idea of encrypting network-to-network traffic using IPsec without any hosts needing to ask for it
- Folks considered it cryptographically sound and a reasonable design, but it saw nearly no deployment.

History of “unauthenticated TLS”

- Using a web browser to go to an https: URL where the certificate doesn’t chain to a trusted root CA, name mis-match, etc.
- “Are you really sure you want to do this?” with text that only the smartest users will understand
- “Do you want me to remember forever that you clicked through this dialog?”

Agreeing on definitions will help application protocol developers

- Applications that set up TLS with encryption without being asked will make passive snooping harder to do, particularly when using PFS
- Applications that allow unauthenticated TLS without lots of warnings will make active MITM attacks worse
- This ***is*** going to involve talking about user interfaces

Opportunistic TLS (from the -00 draft)

- “An application supports opportunistic encryption using TLS if the application attempts to perform TLS negotiation without the user who is running the application knowing whether or not TLS is in use.”
- “The application MUST NOT have any user-visible configuration that enables opportunistic encryption using TLS.”

Two ways that this definition affects the UI of applications

- It is impossible for a program to have a configuration option for opportunistic encryption
  - Having such an option inherently is not for opportunistic encryption
- An application doing opportunistic encryption MUST NOT show the user any indication that TLS is in use, including for errors
- This part may be controversial

Unauthenticated TLS (from the -00 draft)

- “Unauthenticated encryption for TLS is the act of setting up a TLS session at the request of a user where the TLS client does not authenticate the TLS server.”
- We have this today with the all-too-familiar dialog warnings
- This is stuck in an appendix of the draft, and with lots of warnings, to show that it is not parallel to opportunistic

Next steps

- Maybe coalesce with definitions of opportunistic encryption for other security protocols (IPsec, S/MIME ...) and non-security protocols (MPLS, TCP, ...)
- Maybe add examples, but maybe keep the document really short