Analyzing DANE's Identification of Fraudulent Certificates

Matthew Henry, Joseph Kirik, Emily Scheerer

Lab Set-up Progress Report

- Raspberry Pi running a DNS Server
- “Bad Guy” Server with a self-signed certificate
- “realsite” Server with self-signed certificate
- DNS sniffer script completed
- DNS spoofer script in progress

On-Paper Analysis Progress

- Discovered DANE analysis from Verisign

Their results showed that if a web site implemented DNSsec excluding DANE, they would reduce their attack surface by as much as two orders of magnitude

- Subscribed to DANE’s developer mailing list

“In this case the client still typically has no corresponding certificate in hand, and so, if the server does not provide a matching certificate in the TLS handshake, the client cannot "compare" the TLSA record with the server's chain.”

Future Plans/Issues

Plans:

- Run DANE in our lab, try running attack scripts
- Present project at WiCyS Conference (4/11)

Issues:

- DANE implementation is not a clear process
- Sniffer script is not behaving as expected