Introduction

2 caveats:
– This segment is nothing more than an appeal for participation, feedback, and direction
– This may not be the correct forum, but it certainly has the right people in the audience

IETF: only concerned with bits on the wire.

Stated goal of PKIX: development of Internet standards to support X.509-based PKIs
– PKIs enable assurance/trust and secure communications
– Communication is more than just syntax, there is a feedback component and an interpretation aspect by the receiving party
– Is there a responsibility to protect protocol users from themselves or at least advise them of potential issues and intended uses?
– I think this last aspect is largely missing from PKIX standards
What does your mind conjure up when think of the term “Usable Security” ??

- Most end users that I talk to see “usability” and “security” as opposite ends of the spectrum or at least inversely related
- Often in the definition, and certainly in the implementation of security protocols, the usability aspect is overlooked or forgotten

Great tools in the wrong hands, or used incorrectly, become a scourge instead of a help to their intended community

- As a community, how can we address the user safety aspect – how do we make security usable by the masses
Discussion

• So what exactly am I talking about?
  – Certs in browsers:
    • If certs are so usable, why are they buried 7 clicks deep in IE, 6 clicks in FireFox?
    • What end users understand private keys and keeping them protected?
    • Users will click any “OK” prompt if they think it will give them the access they are looking for.
  – Policy & Procedures:
    • RFC 3647 is excellent for defining all the aspects of PKI policy – but who reads them other than auditors?
    • How can an average end user be expected to make a trust decision based on the contents of a CPS?
    • What software supports Policy OIDs let alone allows an end user to?
  – TAM is fantastic for experienced PKI operators – but will it become just another attack vector on unsuspecting novices?
Summary

• How to address the usability in PKIX protocols?
  – Education of typical end users
  – Better tools for PKI implementations

• What forum makes best sense for this type of activity?

• Who is willing to participate?
For More Information

Dartmouth PKI Outreach:
http://www.dartmouth.edu/~deploypki/

Dartmouth PKI Lab:
http://www.dartmouth.edu/~pkilab/

Scott Rea – Scott.Rea@dartmouth.edu