Reflections on Scoping Trust

Wendy Seltzer
wseltzer@w3.org @wseltzer
Technology & Society Domain Lead, W3C
OWASP AppSec Europe, 24 June 2014

Trust

1. Assured resting of the mind on the integrity, veracity, justice, friendship, or other sound principle, of another person; confidence; reliance; reliance. (Webster, 1918)

“Trust, but verify”

Don't trust; you can't verify

“The moral is obvious. You can't trust code that you did not totally create yourself.”

Ken Thompson (*Reflections on Trusting Trust*,1984)

Delegate?

Dourish, Grinter, Delgado & Joseph, *Security in the Wild*

Seda Gürses, *Security Origami*

Trust

How do we produce a web application environment in which we can reasonably ask users to trust?

Open Web Platform

Trusted?

Trustable?

Trustworthy?

Trusted !(necessarily)= Trustworthy

According to the end-to-end argument, the platform need not be trusted

But we need trustworthy endpoints

User-centric trust and security

- Trust anchors

Trusted by whom?

Lately, trust has been misplaced

DigiNotar

Hushmail and Lavabit

BULLRUN

More secure trust roots

Code?

Law?

Distributed systems?

New models and primitives?

Transparency

- Public logs and notaries
- Open source

Signing

- Code
- Channels

Pinning

- Server-side cert pinning
- User-side code pinning?

Secure storage

- Isolated key storage

Capabilities and commitments

Thanks!

Wendy Seltzer
wseltzer@w3.org
World Wide Web Consortium
+1 617.715.4883