PorKI: Making User PKI Safe on Machines of Heterogeneous Trustworthiness*

Sara Sinclair
sinclair@cs.dartmouth.edu

Sean W. Smith
sws@cs.dartmouth.edu

PKI/Trust Laboratory
Dartmouth College

* This work is supported in part by a grant from the Intel Corporation.

PorKI: Portable PKI

- Keep your keypair(s) on your PDA or smartphone
- Generate temporary credentials (proxy certificates)
- Transfer via Bluetooth (don't rely on its encryption or PIN!)
- Authenticate to online resources
- *The private key never leaves the PDA*

Limiting Trust, Limiting Risk

- Hard for users to recognize when a machine is trustworthy
- If the workstation has credentials...
  - Can use policy statements on the PDA before issuing temp credentials
  - Can include them in the proxy cert so the relying party can evaluate them too
- If the workstation has no credentials, default to “untrusted” (which is good!)

Future Work

- Pilot among real users
- Repository protection
- Bluetooth trust bootstrapping
- Issuance of a keypair directly to PorKI by CA
- Location-aware PorKI
- Delegation
- Trusted input/output channels

Contact

- Sara “Scout” Sinclair
- sinclair@cs.dartmouth.edu
- http://www.cs.dartmouth.edu/~sinclair