Digital Inequalities in the Heartland: Exploring the Information Security Experiences of Marginalized Internet Users
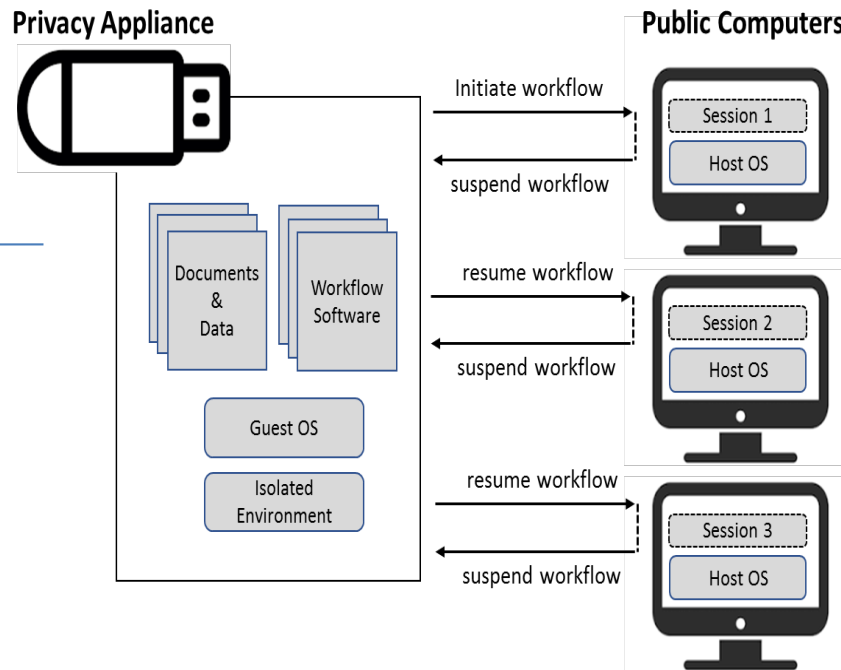
KU

Challenge:

Address privacy and security threats/computing challenges of the practically "disconnected," those economically poor and vulnerable who rely on public libraries for computing needs and broadband access

Solution:

Following extensive qualitative research on patrons' needs, skills, and experiences we developed the Public User Privacy and Security (PUPS) appliance: An isolated, virtual computing environment on a USB stick provides users a safe, functional, seamless, computing experience from session-to-session.

Privacy Appliance

Documents & Data Workflow Software

Guest OS

Isolated Environment

Public Computers

Initiate workflow
suspend workflow
Session 1
Host OS

resume workflow
suspend workflow
Session 2
Host OS

resume workflow
suspend workflow
Session 3
Host OS

Intellectual Merit:

Interdisciplinary research generating new scholarship on digital privacy, trust, data-veillance, and informal STEM education for the underserve-ed; PUPS appliance involves low-level system engineering contributing to the open-source virtualization community and pioneers an understudied threat model

Broader Impact:

Inexpensive and scalable technology that may be adopted widely to address security threats of the underserved. Contributes to a secure and trustworthy cyberspace; advances broad participation in computing and informal STEM education through collaborations with staff and users; and enhances opportunities and infra-structure for research and education at our university