STARSS: Hardware-assisted Methods for OS Integrity

PI: Vinod Ganapathy, co-PIs: Liviu Iftode and Santosh Nagarakatte, Rutgers University

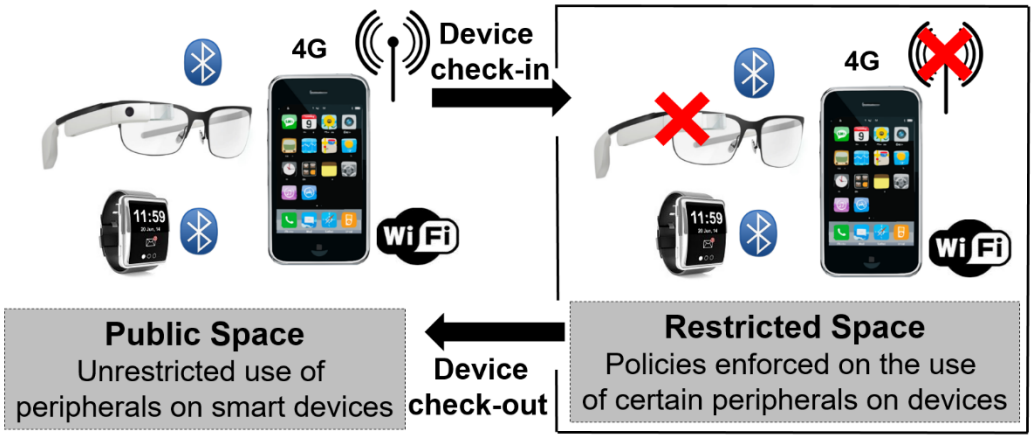
RUTGERS
THE STATE UNIVERSITY OF NEW JERSEY

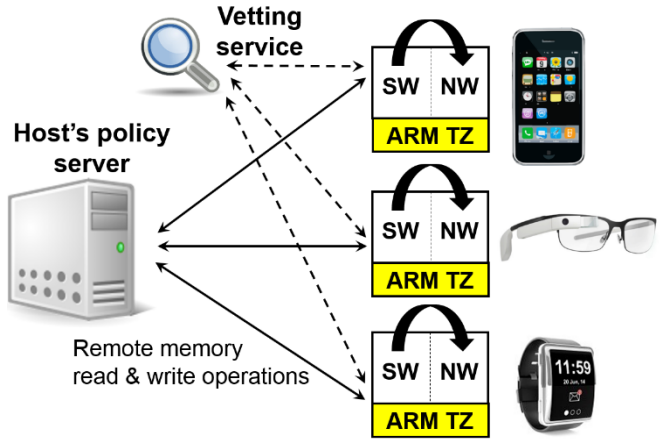
Challenge:

- Smart personal devices and IoT devices are increasing in capability, but also provide attackers with powerful new capabilities to launch new attacks.
- Needed: A method for *hosting* principals to analyze and regulate untrusted *guest* physical devices.

Scientific Impact:

- Explores novel application of trusted ARM TrustZone hardware to regulate the use of guest devices.
- Studies feasibility of using remote memory access as a core building block for device analysis and control.
- Explores minimal-TCB approaches to guest device policy enforcement.





Solution:

- Develop the notion of restricted spaces, within which hosts can enforce security policies on guest devices.
- Hosts leverage ARM TrustZone on guest devices to obtain trustworthy device analysis and control.

Broader Impact:

- Develops and studies the notion of **restricted spaces**.
- Develops a novel method, based on trusted hardware, to **ensure responsible use of IoT devices.**
- Studies the cost/benefit tradeoffs in giving restricted space hosts control over guest IoT devices.

SaTC:STARSS: Hardware-assisted methods for Operating System Integrity, NSF-1441724, PI: Vinod Ganapathy, Rutgers University, co-PIs: Liviu Iftode and Santosh Nagarakatte, Rutgers.