

# Dynamic Isolated Domains

Thomas Nyman and Elena Reshetova



UNIVERSITY OF HELSINKI

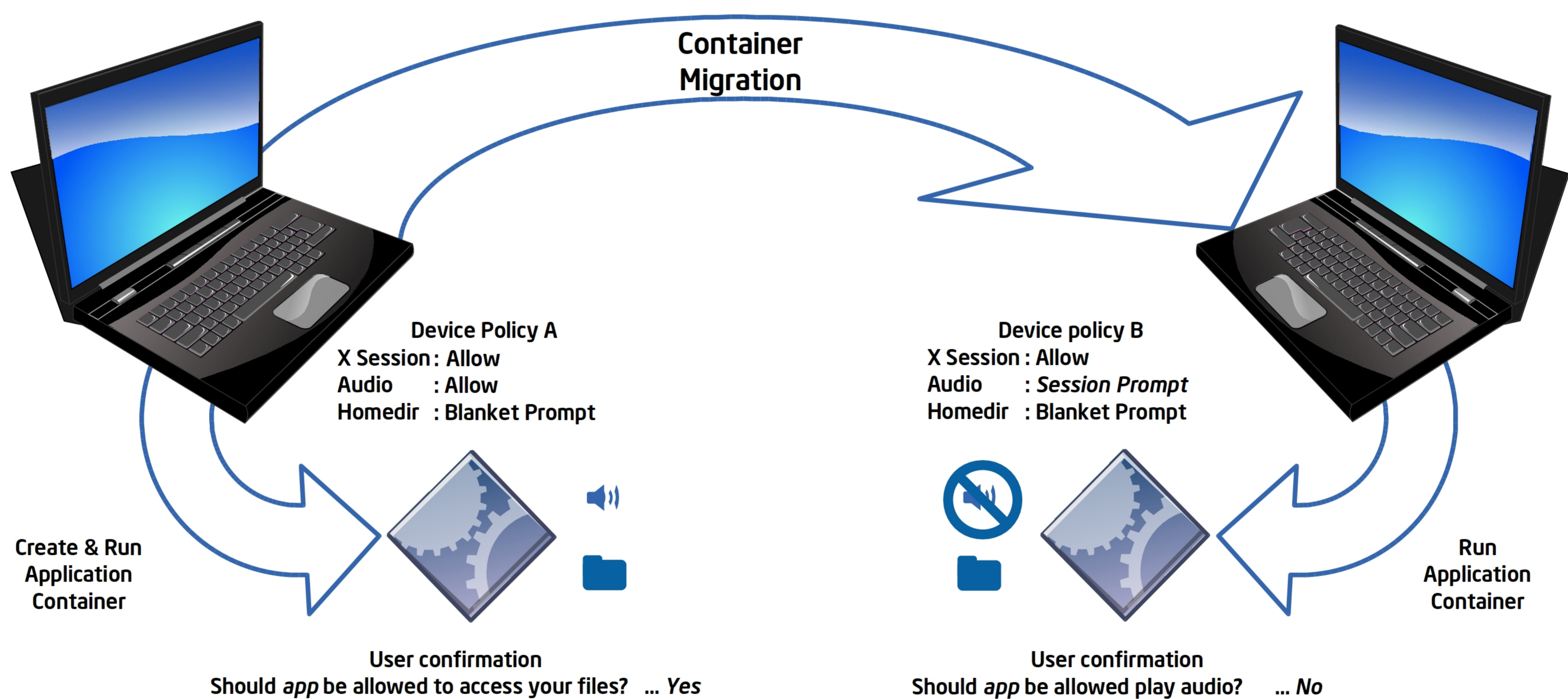
- Are off-the-shelf security mechanisms in the Linux kernel sufficient for new purposes?
- Applying operating system-level virtualization for lightweight, isolated, and seamlessly transferable application domains

**Use cases** involve temporary transfer of application data and user preferences between devices, e.g

- **Shared computing environment**, such as an IIV system used simultaneously by other passengers
- **Rental device**, controlled by service provider
- **Personal device** in a corporate environment

**Challenges** addressed:

- Application-agnostic transfer of application data and user preferences allowing for reliable cleanup
- Retain security policy approved by user, while consolidating conflicting policies in order to adhere to local policy
- Isolation of applications using container-based virtualization suitable for resource-constrained mobile devices



*Overview of policy migration*

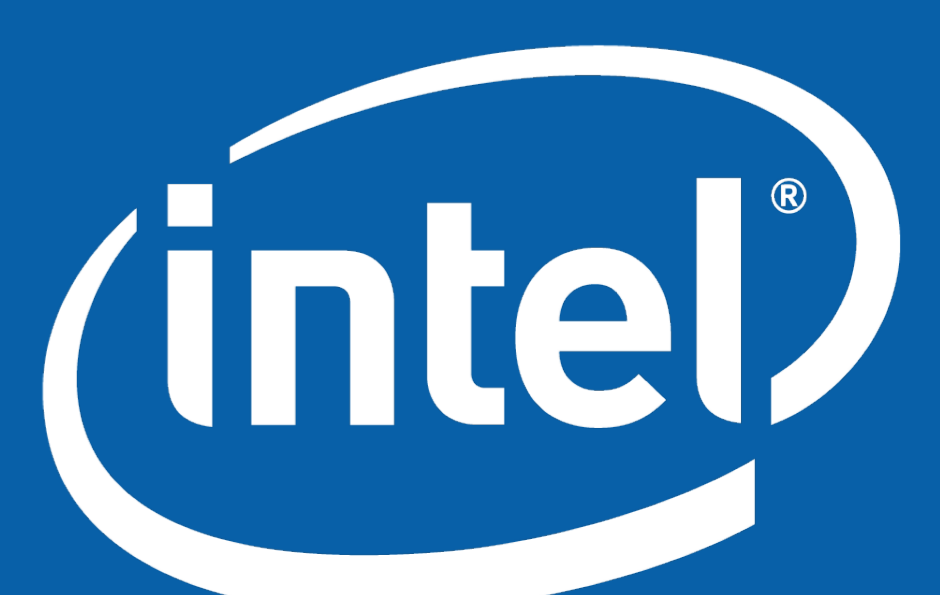
**Our approach** consists of:

- Use of off-the-shelf **OS-level virtualization** features and **mandatory access control** to confine applications
- Filesystem translucency through **overlay filesystems**

**Our contribution** to Intel and the scientific community:

- Novel use cases for operating system-level virtualization
- Proof-of-concept prototype showcasing migration of application data and policy consolidation
- Development of expertise with emerging technology

## Intel CRI for Secure Computing



Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.  
\*Other names and brands may be claimed as the property of others.