

# **What Exploring Space Taught Me About Systems Architecture and Personal Computing**

Patrick F. Wilbur

*Department of Computer Science,  
Clarkson University*

November 28, 2011

# Copyright Notice

Copyright 2011, Patrick F. Wilbur.

Last modified: November 28, 2011 8:06 PM EST.

Some images have been taken from Public Domain or other copyrighted sources. For more information concerning the licensing of those images, please consult the References list at the end of this document. The author of this work believes that use of those images constitutes Fair Use according to U.S. Copyright Law.

==

LICENSE:

Patrick F. Wilbur  
Department of Computer Science  
Clarkson University  
Potsdam, NY USA

<http://pdub.net>

These slides and content are released under the Creative Commons Attribution-Share Alike 3.0 Unported license, available online at <http://creativecommons.org/licenses/by-sa/3.0/>

You may share (copy, distribute, and transmit) this work, and remix (adapt) this work, as long as you attribute this work to the author and share adapted works under the same or similar license by leaving this entire notice in place (including the original author's name/contact information/URL and this license notice).

# Acknowledgments

Special thanks to my advisor, Dr. Jeanna Matthews, for her virtualization, virtual appliance, and virtual machine contracts support, interests, and insights.

Special thanks to my friend, Dr. Todd Deshane, for helping with OSCKAR Core implementation, asking me difficult questions, and using OSCKAR Core in his work.

# Research Topic

- Intersection of:
  - **Personal computing**
  - **Security**
  - **Usability**
- Virtualization as a means to contribute to these areas by:
  - Improving **software distribution**
  - Improving **data protection**
  - Maintaining **trust** (established security & reliability)



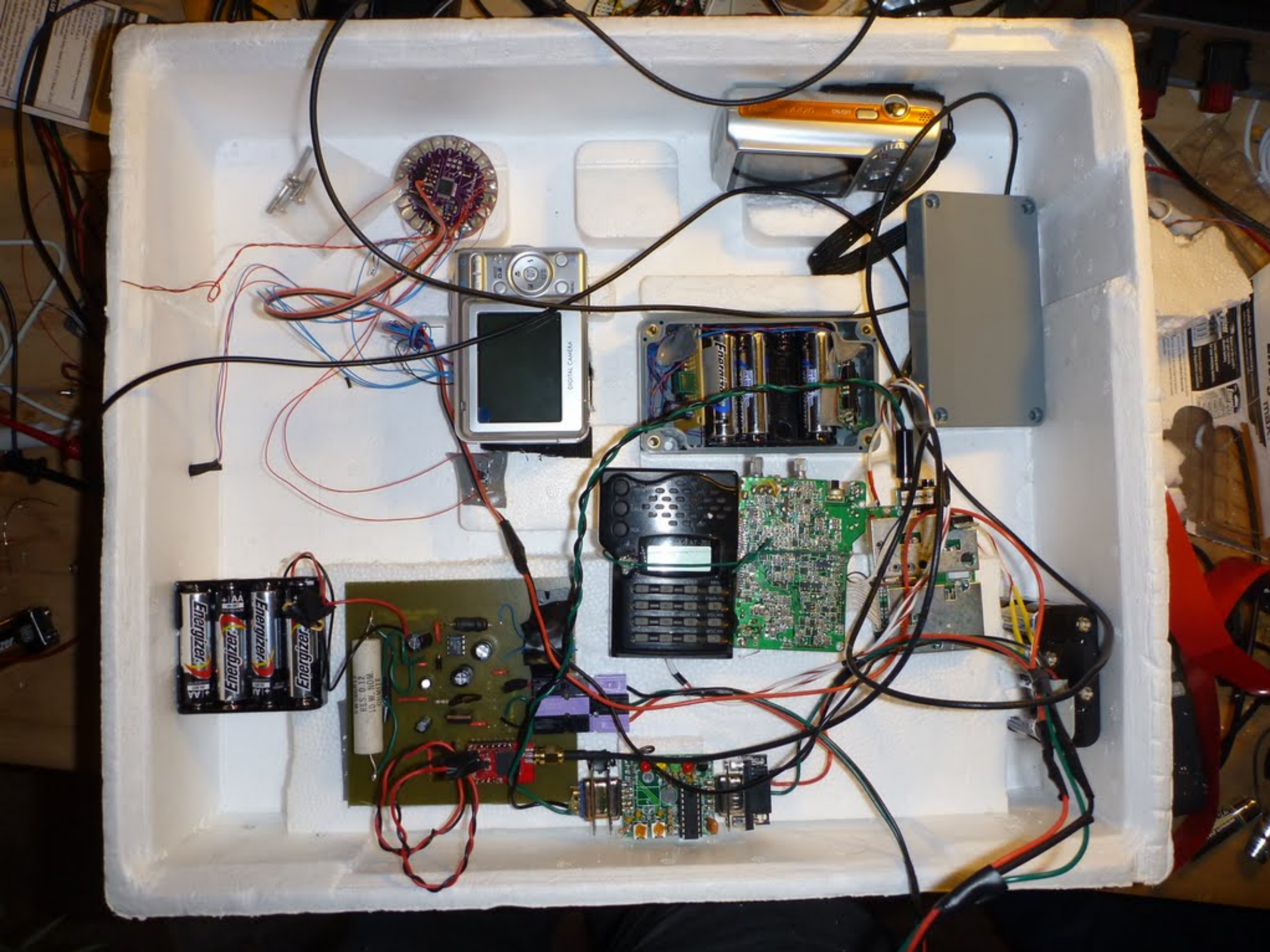
**SPACE.**

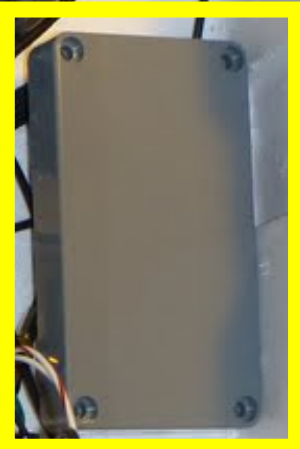
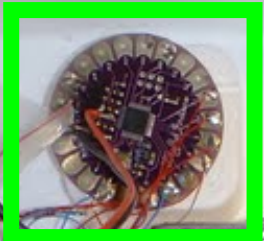
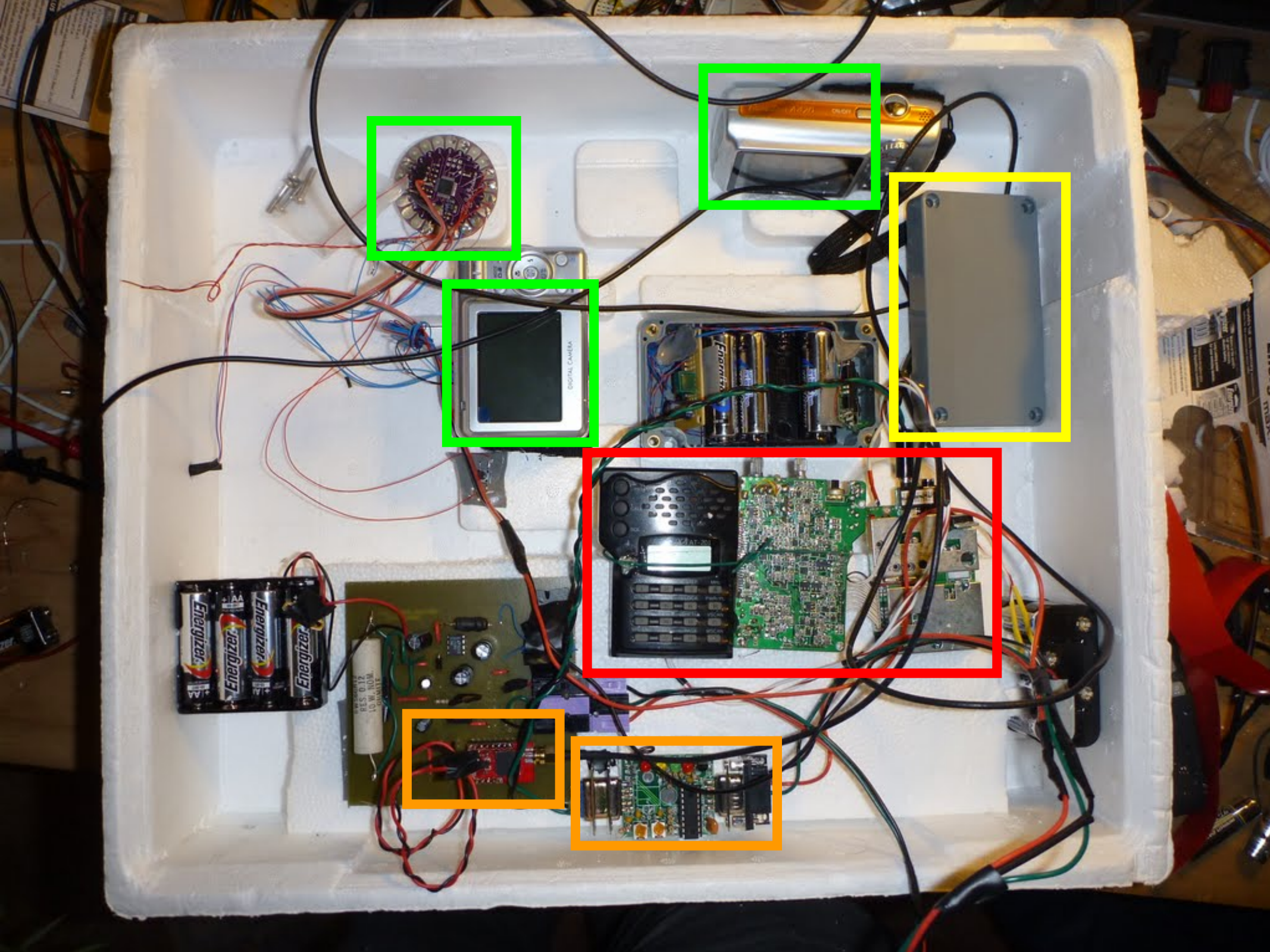














Energizer  
Energizer  
Energizer  
Energizer

RES 0.12  
10 W. NOM.  
COMPOSITE

DIGITAL CAMERA

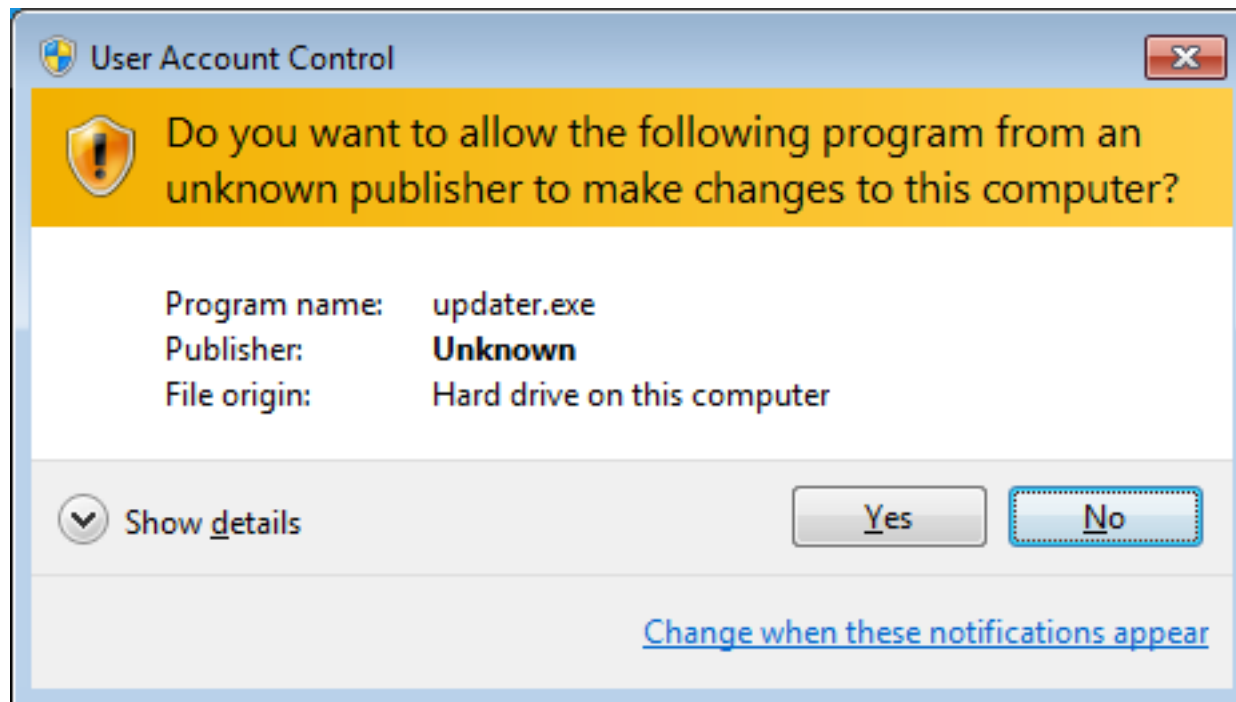
Energizer

# Some Computer Security Principles

- Reduce size of **trusted computing base (TCB)**
- Apply the **Principle of Least Privilege (POLP)**
- Attempt to **understand user intent**
- Attempt to enforce **isolation** between applications

# Classic Application of Principles

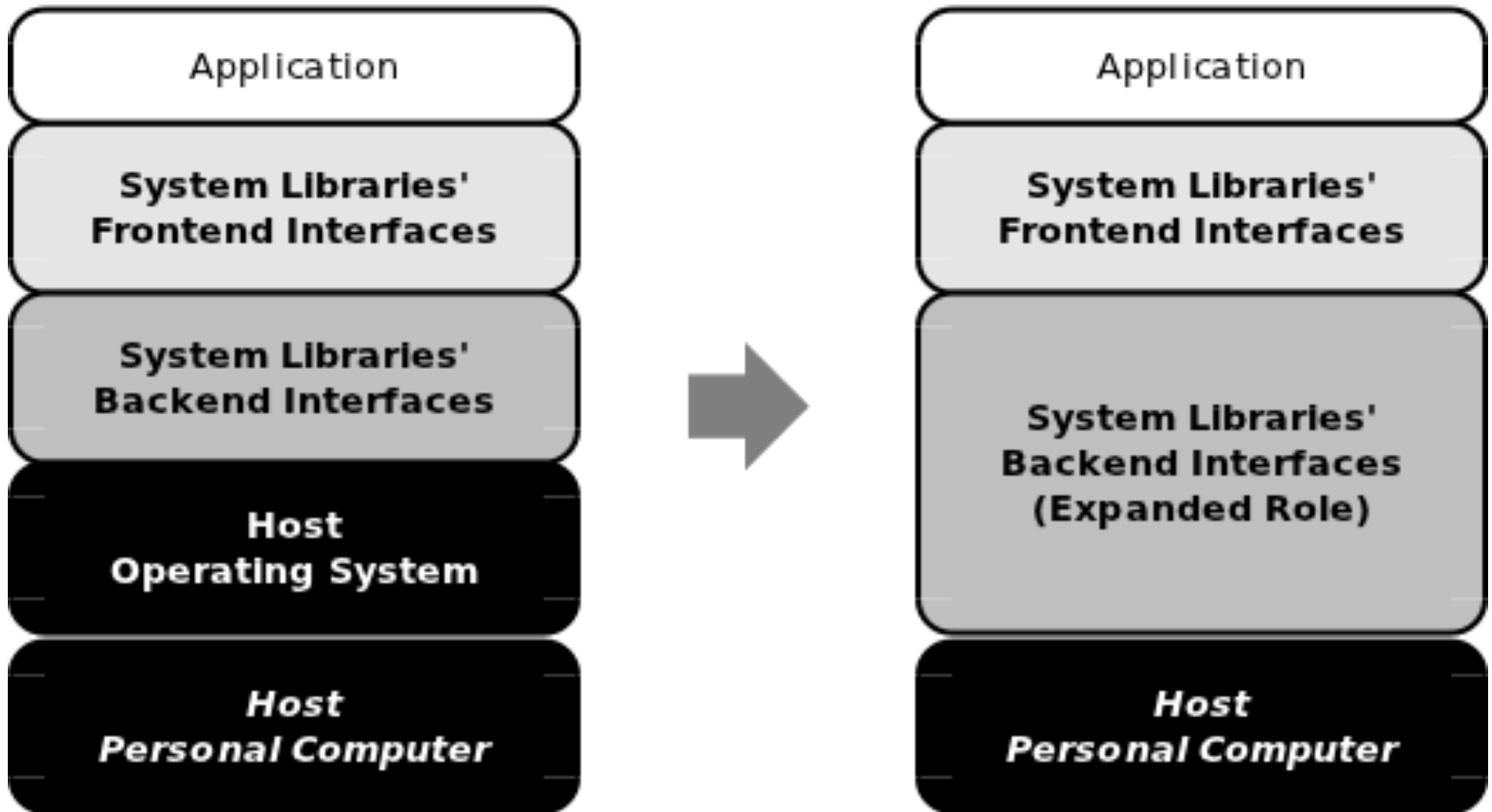
- Operating systems already do attempt to reduce TCB
- **Mandatory Access Control** (e.g. SELinux) for POLP
- **User Account Control** (UAC) for user intent
- Qubes OS (VM **sandboxing**) for selective isolation



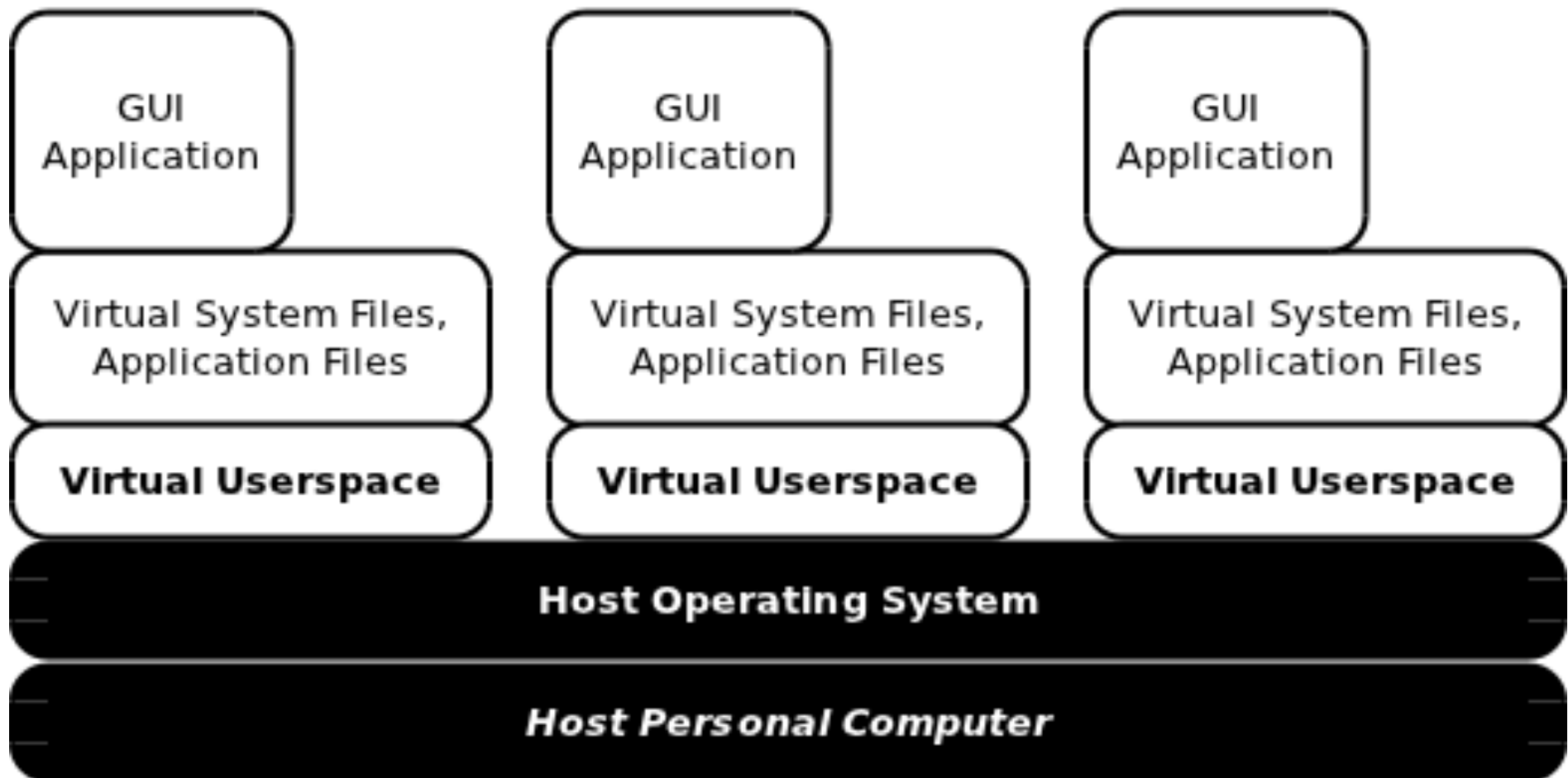
# Idealistic OS-app Model

- Historically, hardware provided multitasking/multi-tenancy
- **OS-apps:**
  - Talk to hardware without needing (much of) an OS
  - Depend upon a virtualization hypervisor for multitasking
- Desktop Decomposition:
  - Reduces size of TCB
  - Enforces extreme isolation
  - Isolation helps make POLP enforcement easier
  - Few-purpose systems easy to watch, secure





Idealistic OS-app Model



Desktop Decomposition using Virtual Appliances

# Benefits of Desktop Virtual Appliances

- Reverses disturbing trends:
  - SaaS/AaaS (Software as a Service, Application)
  - Software requiring installation/execution as Administrator
- Hardware more predictable than software-defined systems
- Reduces size of TCB: easier to engineer trustworthy (secure, reliable) systems
- Rollback (on demand, on application close, etc.)

# Virtual Machine Contracts

- Define expected *operating environment*
- Optionally define *expected operating characteristics*:
  - IDS
  - Resource usage patterns
- Allows distributing virtual appliance disk image or not

# Virtual Machine Contracts

- **OSCKAR Core:**

- VMC processing/enforcement engine
- Provides an automation platform for developing virtualization-related solutions
- Service provider/consumer architecture makes it extremely versatile and extensible

# Open Problems

- **Software licensing**
- **Determining user intent**
- **Scalability** (mem. deduplication? other types of virt.?)
- **Hardware vulnerabilities** (security issue, not a trust issue)

# Current Progress & Future Work

- Build OSCKAR Core (for automation)
- Build/test Appify tool (first generation, with poor delegation)
- Implement basic DataStore (provides selective sharing)
- **Test power consumption overhead**
- **Additional performance testing** (some done before)
- **Improve Appify tool** (with preemptive worker VM creation)
- Implement user intent systems
- Incorporate user intent into improved User DataStore

# Questions?



# References

- URL: [http://en.wikipedia.org/wiki/Trusted\\_system](http://en.wikipedia.org/wiki/Trusted_system)
- URL: [http://en.wikipedia.org/wiki/Trusted\\_computing\\_base](http://en.wikipedia.org/wiki/Trusted_computing_base)
- URL: [http://en.wikipedia.org/wiki/System\\_360](http://en.wikipedia.org/wiki/System_360)
- URL: [http://en.wikipedia.org/wiki/VM\\_\(operating\\_system\)](http://en.wikipedia.org/wiki/VM_(operating_system))
- URL: <http://pdub.net/projects/near-space-weather-balloon/>
- URL: <https://picasaweb.google.com/100543486411711719984/TheGreatGigInTheSky>
- Paper: Joshua Sunshine, Serge Egelman, Hazim Almuhiemedi, Neha Atri, and Lorrie Faith Cranor. Crying Wolf: An Empirical Study of SSL Warning Effectiveness. Proceedings of the 18th conference on USENIX security symposium (SSYM'09). 2009. USENIX Association, Berkeley, CA, USA, 399-416.
- Paper: Wilbur, Patrick F. and Todd Deshane. Johnny Can Drag and Drop: Determining User Intent Through Traditional Interactions to Improve Desktop Security. CHiMiT '10: Proceedings of the 4th Symposium on Computer Human Interaction for the Management of Information Technology. November 2010. DOI: 10.1145/1873561.1873565