

# This will be a cool title

Will Dietz, Kevin Larson, Shivaram Venkataraman  
University of Illinois at Urbana Champaign

## 1 Introduction

In recent years, virtual machines have become prevalent in cluster computing environments [1] as they lower power costs and help in conserving data center space. Hardware improvements have meant that smart phone configurations found today resemble desktop machines from few years ago and many of them run commodity operating systems. There is a growing interest in academia [9] and industry [5] about the virtualization on these devices. We believe that virtualization can provide better security guarantees in mobile devices and enable useful applications like environment migration.

Mobile devices today run many third party applications to perform complex tasks like web browsing, banking and gaming. Recent studies have found that smartphones are the target of an increasing number of malware attacks [7], [3], [4] and their security is important as personal data such as contacts, credit card numbers and passwords are often stored on the device. While some security models [2] provide a stronger process level isolation among applications, operating system bugs [6] can still allow malicious applications to take over the device. We believe that virtualization can be useful for secure isolation of third party code from confidential data and provide a greater defence-in-depth against attacks on the system.

Environment migration has been studied earlier, in the context of servers in a cluster [8] and enables administrators of clusters to perform maintenance tasks without interruption. Migrating an OS to a mobile device can be useful as it can take advantage of network or computation facilities that are closer to the user's location and provide the user with a consistent experience irrespective of the network connectivity.

## 2 Timeline

## 3 Evaluation plan

## 4 Anticipated results

## References

- [1] 16 percent of workloads are running Virtual Machines. <http://www.gartner.com/it/page.jsp?id=1211813>.
- [2] Android Security and Permissions. <http://developer.android.com/guide/topics/security/security.html>.
- [3] Cyber-criminals target mobile banking. <http://www.v3.co.uk/vnunet/news/2173161/cyber-criminals-target-mobile>.
- [4] iPhone privacy. [http://seriot.ch/resources/talks\\_papers/iPhonePrivacy.pdf](http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf).
- [5] Mobile Phones, The Next Frontier. <http://blogs.vmware.com/console/2009/08/mobile-phones-the-next-frontier.html>.
- [6] Vulnerability Summary for CVE-2009-2692. <http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2009-2692>.
- [7] A. Bose and K. Shin. On Mobile Viruses Exploiting Messaging and Bluetooth Services. *Securecomm and Workshops, 2006*, pages 1–10, 2006.
- [8] C. Clark, K. Fraser, S. Hand, J. Hansen, E. Jul, C. Limpach, I. Pratt, and A. Warfield. Live migration of virtual machines. In *Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation-Volume 2*, page 286. USENIX Association, 2005.
- [9] L. Cox and P. Chen. Pocket Hypervisors: Opportunities and Challenges. In *Eighth IEEE Workshop on Mobile Computing Systems and Applications, 2007. Hot-Mobile 2007*, pages 46–50, 2007.