What would you submit to MoVid ‘13?

Landon Cox

Duke University

Want to share sensitive data.

Devices have **sensors** and talk to the **cloud**.

Data is often sensitive (e.g., location, images).

Mobile sensing services

- **Tremendous opportunities**
  - Citizen journalism (CNN's iReport, Al Jazeera Sharek)
  - Mobile social services (Foursquare, Micro-Blog)
  - Many kinds of monitoring (traffic, parking, prices)
- **Authenticity is crucial for correctness**
  - **Garbage in garbage out**
  - Hard to cover many events (Iran, Egypt, Libya, etc.)
  - User-generated content is increasingly important
  - Injection of false data can have dire consequences

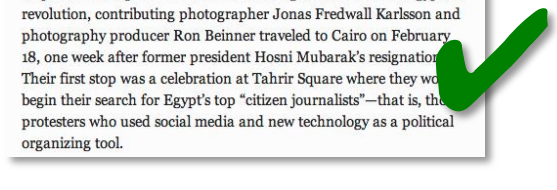
POLITICS • VIDEO

Citizen Journalism: Life on the Ground at the Egyptian Revolution

by **Bennett Allen** April 4, 2011, 12:01 AM

Photograph by Jonas Fredwall Karlsson.

As part of *Vanity Fair*'s continued coverage of this winter's Egyptian revolution, contributing photographer Jonas Fredwall Karlsson and photography producer Ron Beinner traveled to Cairo on February 18, one week after former president Hosni Mubarak's resignation. Their first stop was a celebration at Tahrir Square where they would begin their search for Egypt's top "citizen journalists"—that is, the protesters who used social media and new technology as a political organizing tool.



the vote blog
politics, opinion, humor

That photo of the 9/12 march on Washington? It's fake.

Demonstrators hold signs during a '9/12' march on Washington. The Washington Monument is in the background. Some conservative blogs have been circulating photos allegedly taken during the rally. But at least one fact-checking site says the photos are fakes.

Jose Luis Magana/AP

Enlarge

Sickening tsunami of faked photos

Wade Laube
March 16, 2011

Comments 52

The Washington Post

Back to previous page

Images of Gaddafi's death highlight visual distrust in the digital age

By Philip Kennicott, Published: October 20

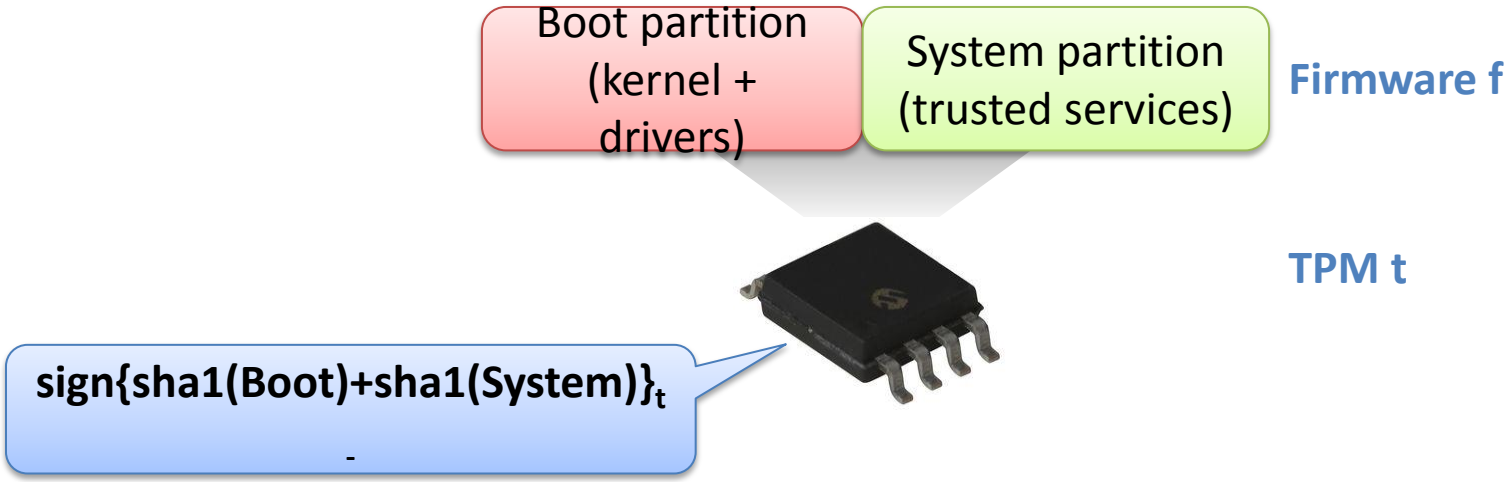
http://www.vanityfair.com/online/daily/2011/04/citizen-journalism.html
http://ireport.cnn.com
http://www.csmonitor.com/USA/Politics/The-Vote/2009/0914/that-photo-of-the-912-march-on-washington-its-fake
http://www.smh.com.au/opinion/society-and-culture/sickening-tsunami-of-faked-photos-20110315-1bvuo.html
http://www.washingtonpost.com/lifestyle/style/images-of-gaddafis-death-highlight-visual-distrust-in-the-digital-age/2011/10/20/gIQArJNm1L_story.html

Existing approaches

- **Rely on reputations**
  - Users often require anonymity
  - Users only contribute at most critical moments
  - Reputations may be vulnerable to Sybil attacks
- **Rely on voting, statistical analysis**
  - Sybil attacks can also skew votes
  - May be only a few observers
  - How to vote among rich data like images?

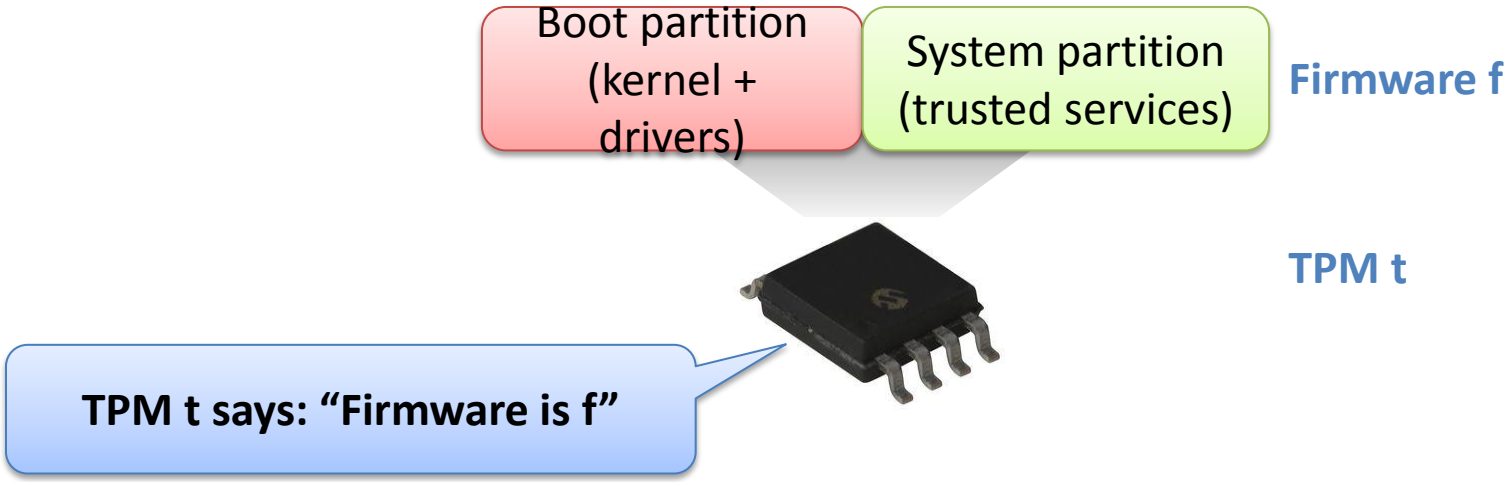
Root of trust: secure hardware

- **Trusted Platform Module (TPM)**
  - Includes private key, can compute hashes, sign statements
- **Pertinent functionality**
  - Trustworthy attestation of trusted computing base (i.e., the firmware)



Root of trust: secure hardware

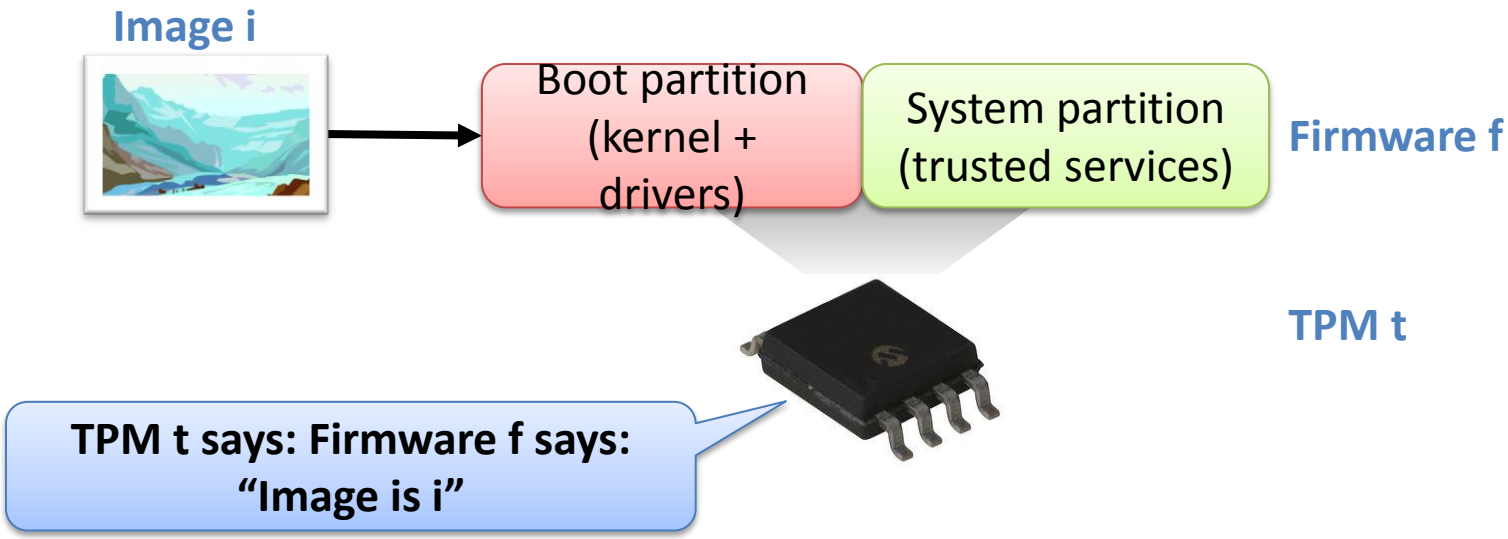
- **Trusted Platform Module (TPM)**
  - Includes private key, can compute hashes, sign statements
- **Pertinent functionality**
  - Trustworthy attestation of trusted computing base (i.e., the firmware)



Could sign raw sensor data

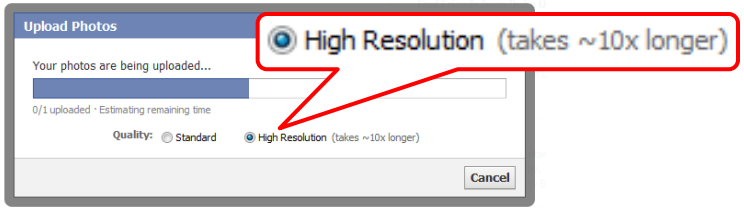
- **Allows services to verify authenticity of raw data**
  - Service must trust TPM and device firmware
  - Verify hash in signed statement matches hash of received image

Problem: data cannot be modified



Modifying data locally

- **Mobile clients need to control data fidelity**
  - Efficient resource usage (energy, bandwidth)
  - Privacy (cropping, blurring faces)
- **Any legitimate modification alters data hash**
  - Statement about raw data no longer useful



"You're welcome to upload any image that is **3MB or smaller**."

Need resolve tension between **authenticity** and **fidelity**

YouProve approach: trusted media analysis
(see SenSys '11 paper for details)

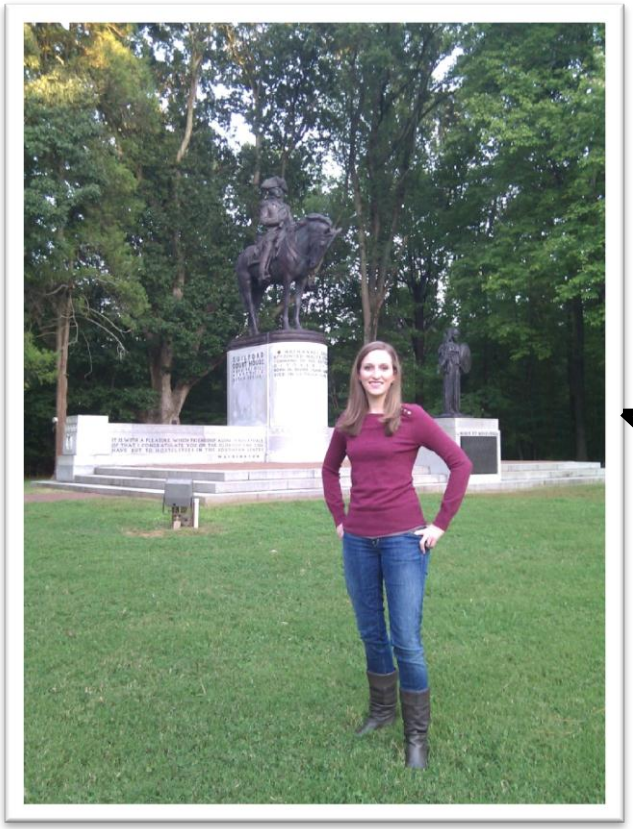


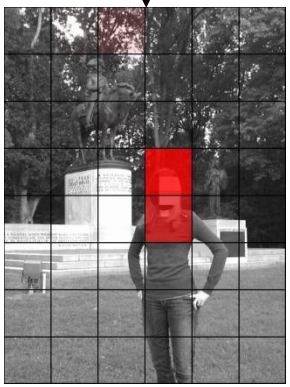
Image i

App

Fidelity reducer

Image i'

Type-specific analyzer



Fidelity certificate

Conclusions

- **Key challenge**
  - Need to balance **authenticity** and **fidelity**
- **How do you generate these "heat maps" for video?**
  - Analysis is very computationally intensive
  - Can this be done in a timely manner?
  - Can this be done without killing a device's battery?
  - How do you keep the trusted computing base small?
- **Lots of hard problems, that we don't know how to answer**
  - Email me if you know how! (**Landon Cox: lpcox@cs.duke.edu**)