

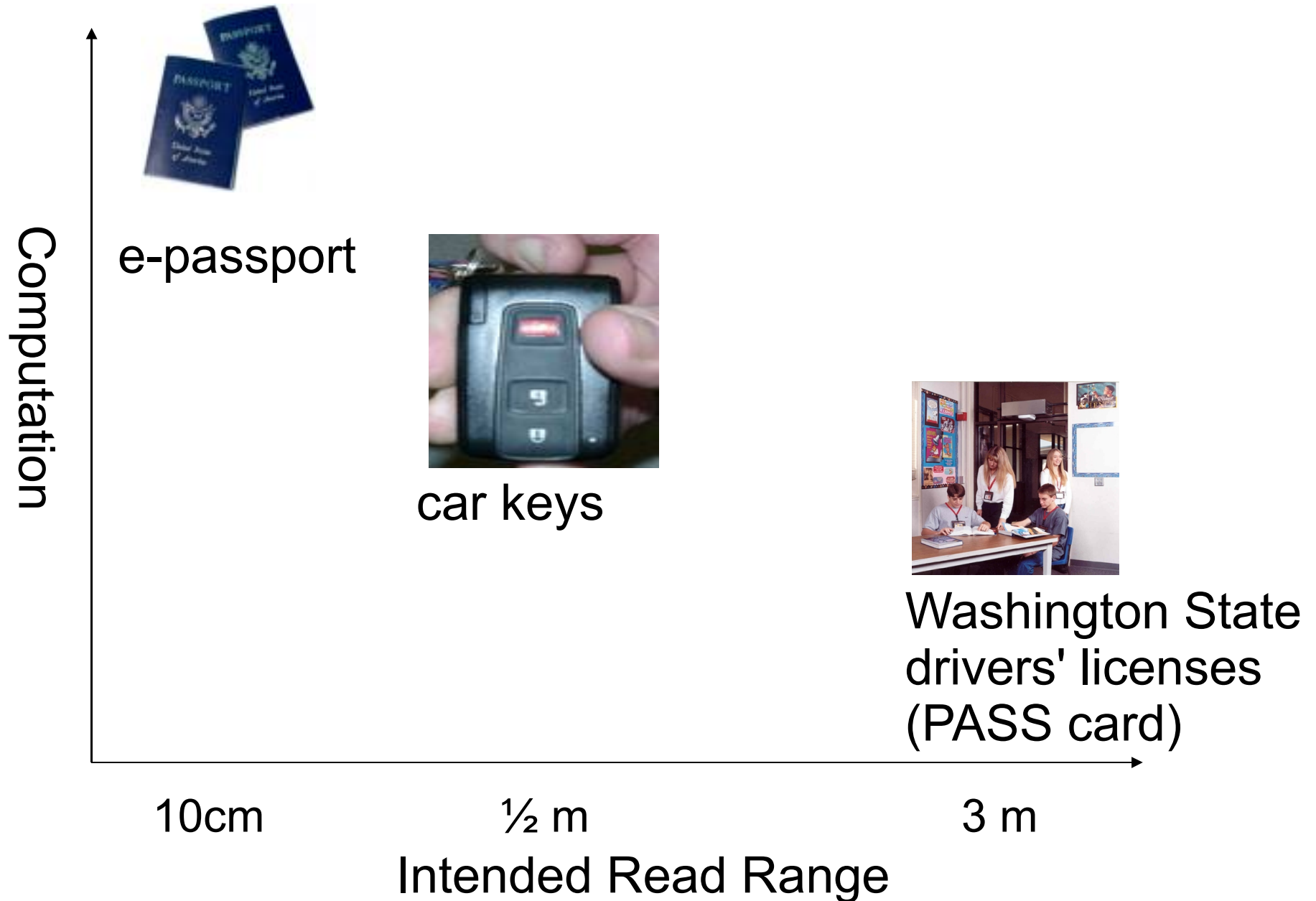
RFID: Long-Term Research or Short-Term Tinkering?

Both will happen –
do we want to be involved?

David Molnar
ACM Wireless Security 2008
Panel Discussion

Thanks to: Nikita Borisov, Erinn Clark, David Farris, Craig K. Harmon, David M. Shaw, Szuszkó László, David Wagner, and the SV_RFID list, for pointers, discussion, etc.
All errors, omissions, and opinions belong to David Molnar.

RFID – Real Deployments, Today



Research Will Happen

- Deployments = market opportunities
 - “RFID security” start-ups (PUFCo, SecureRF)
- Hacker research
 - e.g. Chris Paget cloning, Johnny Long SQL injection, Nohl/Plotz MIFARE attacks
- RFID manufacturers' own research
 - e.g. RFID Experts Group draft ISO Standard for evaluating RFID security (ed. Craig K. Harmon)

How Can We Be Relevant?

- Partnerships with people building/deploying
 - Example: RFID CUSP (RSA/UMass/JHU/ETHZ)
 - Example: e-passports at SFO airport (UCB Law)
- Identify problems with RFID deployments
 - “Short-term tinkering” is valuable!
- Figure out key problems unique to RFID
- Participate in policy discussions
- Industry/hackers/others **will** do all this

Is This Area Worth Cost/Benefit?

- High startup costs for most research
 - Test platforms, partnerships, real deployments
- Crypto has lower startup cost, harder impact
 - Requirements? Capabilities?
- Unclear pipeline from research to impact
 - **Partial** Exception: breaking deployments
 - Contrast with other areas, e.g. software security