

Privacy and Security in Radio Frequency Identification

David Molnar

University of California, Berkeley
presentation for the California Research Bureau





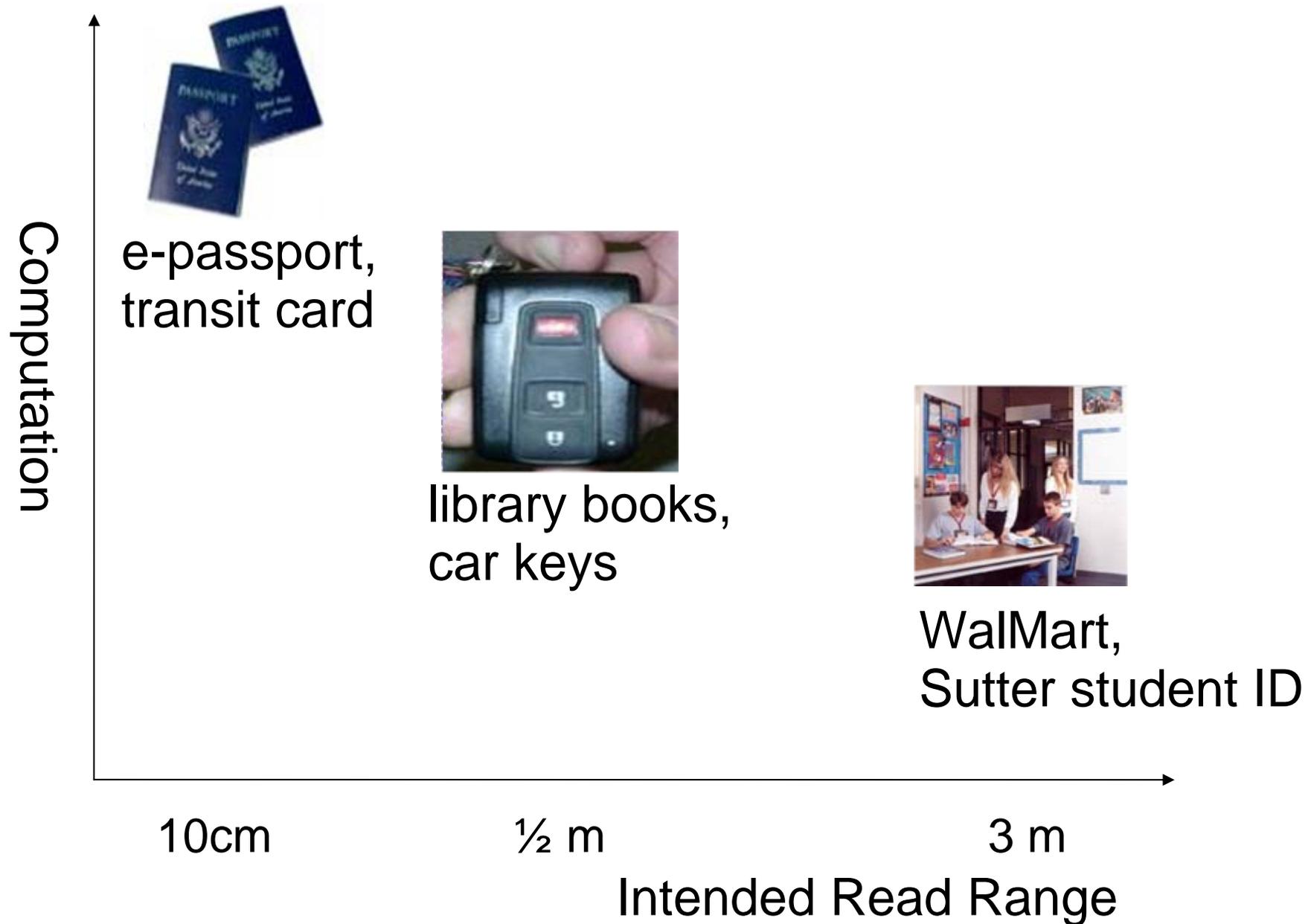
RFID Applications



They're Everywhere!



RFID – A Range of Technologies



“Intended” read range

- Several different ranges
 - Direct reading vs. Eavesdropping
- Some public data points available
 - EPC Gen 1 tags direct read at 63 feet (2005)
 - E-passport eavesdropping 4m, read at 25cm
 - G. Hancke. IEEE Symposium on Security and Privacy 2006.
- Attacker can build special-purpose readers

What's On These Tags?

- Minimum of a unique ID number
 - library books : bar code
 - wal-mart tags : electronic product code
 - building access cards : ID number
- Some applications have more
 - e-passports : photograph, full name, birthdate
 - 1st gen credit cards : full name, credit card #

Attack: Skimming

- Surreptitious, unauthorized read of RFID
- Special concern if tag carries sensitive data

Attack: Skimming

- Surreptitious, unauthorized read of RFID
- Special concern if tag carries sensitive data



Vulnerabilities in first-generation RFID-enabled credit cards.
Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and
Tom O'Hare. Proceedings of *Financial Cryptography* 2007.

Attack: Skimming

- Surreptitious, unauthorized read of RFID
- Special concern if tag carries sensitive data



Vulnerabilities in first-generation RFID-enabled credit cards.
Thomas S. Heydt-Benjamin, Dan V. Bailey, Kevin Fu, Ari Juels, and
Tom O'Hare. Proceedings of *Financial Cryptography* 2007.

Attack: Cloning

- Create device that looks like RFID to reader
- Violates assumption that RFID is “unique”
- Even a short read range is a problem!
 - Car Keys (Green et al. Usenix Security 2005)
 - Prox Cards (Westhues 2003)
 - VeriChip (Westhues et al. 2004)
- More on this shortly...

Attack: Tracking

- Read unique ID from RFID, track movements



Devices That Tell On You: The Nike+iPod Sport Kit
T. Scott Saponas, Jonathan Lester, Carl Hartung, and Tadayoshi Kohno.
Usenix Security Conference 2007.

Attack: Hotlisting

- Want to know if item is on a “hot list”
- FBI looking for almanacs
- Hypothetical: Gun shows & political rallies
- Demo'd: RFID-triggered bomb

“It's Only a Number” - ?

- Cloning, Tracking, and Hotlisting
- Market for mapping ID to name
 - License plate databases
- No notice or choice when RFID is read
- No control over data retained

Chris Paget cloning demo
and Dan Kaminsky on RFID

Recap

- Defined vulnerabilities of RFID
- Demonstrated cloning
- Discussed read ranges
- Key point: adversaries change the game
- Key point: gov't ID leads to target

Attacks Always Get Worse

- We've seen vulnerabilities “baked-in” before
- Cell Phones
 - No protection of cell signal in analog phones
 - Newt Gingrich intercepted in 1996
 - Cell phone cryptography turned out flawed
- Internet bugs
 - In 1989, Internet designed for cooperating servers
 - In 2000, “Mafiaboy” takes down Yahoo!, Dell, et al.
- Time answers “Who would do that?”