Scribed notes from the vulnerability publishing session at RFID CUSP workshop (2008): Session led by Adam Stubblefield.

Legal Issues:

- Issues are different than typical vulnerability work
- Usually, there are no (genuine) DMCA concerns
- There is typically no copyrighted content to protect on RFID tags due to their small storage capacity
- As long no part of the work is particularly nefarious (i.e., knowledge is gained through reverse engineering only), there is generally no concern about violating trade secrets protections
- Depending on your organization, there may be litigation cost concerns

Ethical concerns:

- Balancing test: how does the disclosure benefit society versus how it may harm society?
    - There is usually some scientific merit to any disclosure
    - In particular:
        - Disclosure can validate new techniques (may be difficult to convince people of their merit without proof)
        - Can demonstrate new types of vulnerabilities
    - Allows people affected by vulnerability to make informed decisions (e.g., consumers) so they can guage their risks
    - Must also remember that “bad guys” now also have information

Case study: Texas Instruments DST

- Decided to disclose vulnerability information in stages
- All companies involved were notified first
- 1 month later, reported vulnerability with videos demonstrating its existence (without details)
- 6 months later, published full vulnerability details
- Stimulated a market that did not exist before (e.g., remote starters, replacement keys)
- Allowed consumers to make informed decisions and generated additional benefits as well
- In general, company engineers are perfectly aware of device performance characteristics (and restrictions)
    - This knowledge immediately evaporates one level above engineers
    - Creates tension between technical staff and management/legal staff

Other topics:

- How to find the correct point of contact in an organization when preparing disclosure report