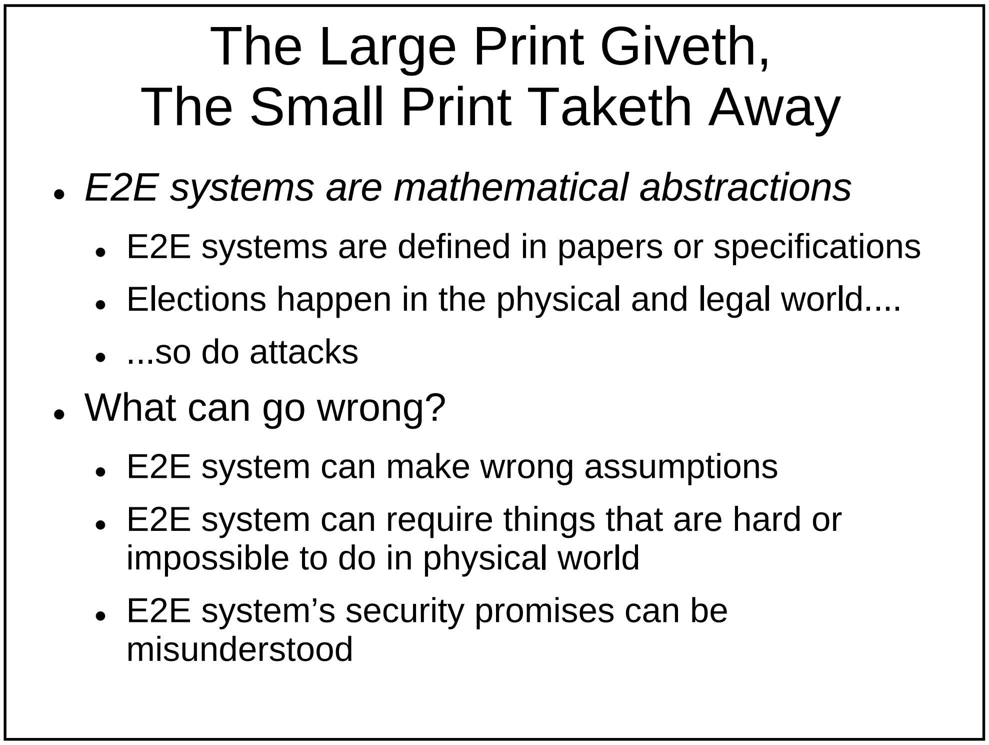
The Large Print Giveth,
The Small Print Taketh Away*

John Kelsey, NIST, October 2009

* With apologies to Tom Waits

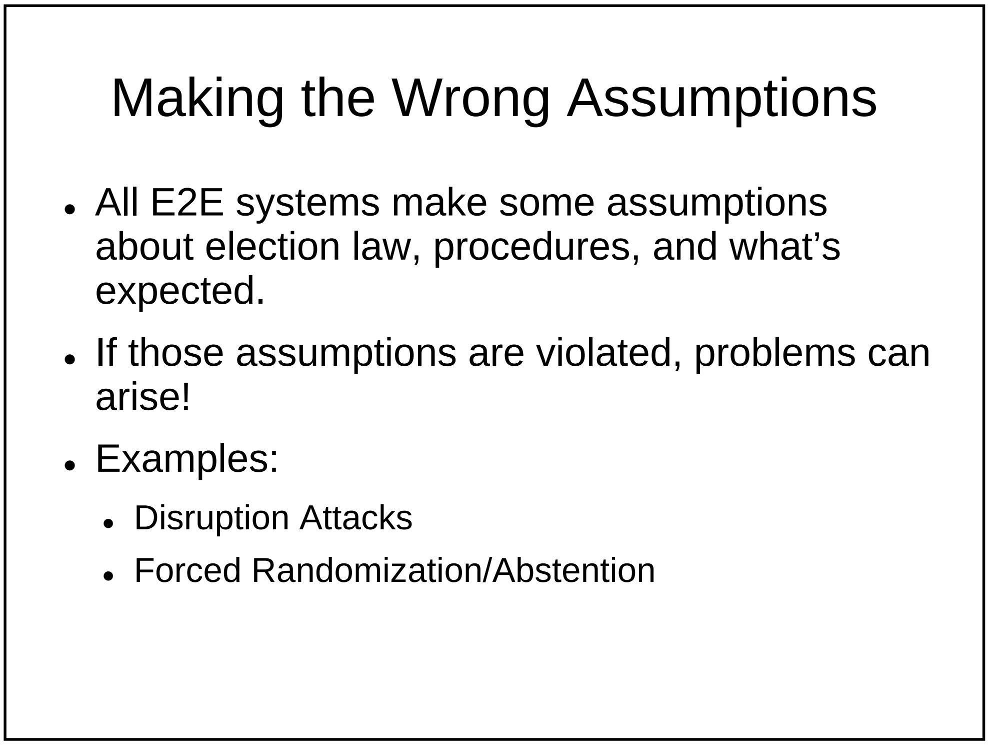
End to End Systems

- Alice interacts with voting system somehow
  - Fills out a ballot, enters votes into a computer, etc.
- Alice walks away with a receipt
- Receipts all published at end of election
  - Alice can verify her receipt is included
  - That proves her vote was cast as intended
  - Even one bad receipt calls election into question!
- Receipts are used to compute the election result in public
  - Insert cryptographic black magic here



The Large Print Giveth, The Small Print Taketh Away

- *E2E systems are mathematical abstractions*
  - E2E systems are defined in papers or specifications
  - Elections happen in the physical and legal world....
  - ...so do attacks
- What can go wrong?
  - E2E system can make wrong assumptions
  - E2E system can require things that are hard or impossible to do in physical world
  - E2E system's security promises can be misunderstood



Making the Wrong Assumptions

- All E2E systems make some assumptions about election law, procedures, and what's expected.
- If those assumptions are violated, problems can arise!
- Examples:
  - Disruption Attacks
  - Forced Randomization/Abstention

Disruption Attacks

- E2E systems are *fantastic* at detecting fraud.
    - Even a small number of tampered ballots can be detected.
    - But most don't have any way of measuring how many were tampered with!
- How to Contest Valid Elections
    - Compromise a few machines*.
    - Have your henchmen vote on those machines in a way that gets their votes tampered with.
    - If you don't like election outcome, send henchmen to New York Times with their receipts.
- In close elections, this could change results!

Forced Randomization

- Many E2E systems: Receipt = encrypted votes
    - Pret-a-Voter, Punchscan
    - You can often exert control over receipt, but this randomizes your ballot.
    - Can't prove how you voted because I can't decrypt
- Attack: I pay you to bring me a receipt that looks a certain way
    - (say, all the leftmost or topmost choices marked)
    - Result: I know your vote was randomized.
- Does it matter?
    - US vs Australian Laws

Playing with Procedures

- Pret-a-Voter and Punchscan have two-part paper ballots. To vote:
  - fill in ballots in way that depends on both halves
  - destroy one half, scan other half (that's your receipt)
- If you can bring back both halves, I can see your ballot
  - Mathematical abstraction land: procedures stop this
  - Reality: this requires a bunch of complicated extra steps!
    - For Pret-a-voter, it looks really hard to stop!

Changing Votes

- E2E is very good for election integrity

...even here, procedures & assumptions matter!

- Punchscan: misprinted ballots + tampered scanners allow election fraud
  - This violated assumptions about procedures
- Any DRE-based system: voting machine simply silently “misreads” some of your choices.
  - How can you know/prove this is attack, not error?
  - Choice of ***vote*** or ***audit*** “misread”

Summary

- E2E systems offer wonderful improvements in election security....
- ...but remember there's a difference between the abstract system (what appears in a crypto paper) and the physical system
- E2E systems open new vulnerabilities, as well as blocking older ones.
  - Receipts in particular offer lots of avenues for attack
- General nontechnical worry: Will voters/public correctly understand security guarantees?