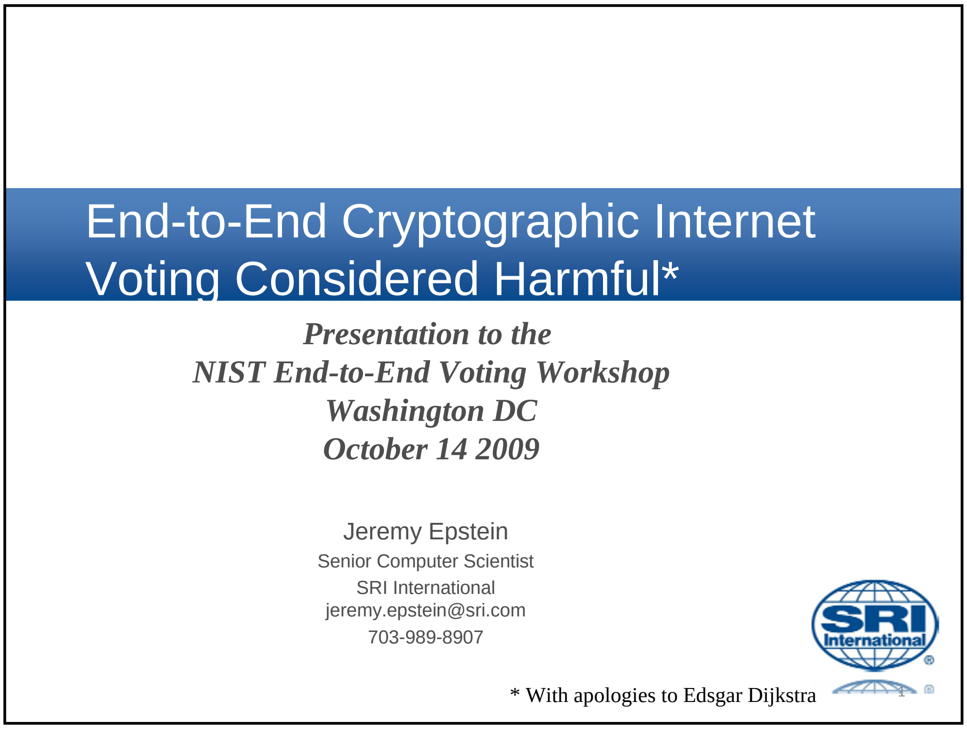
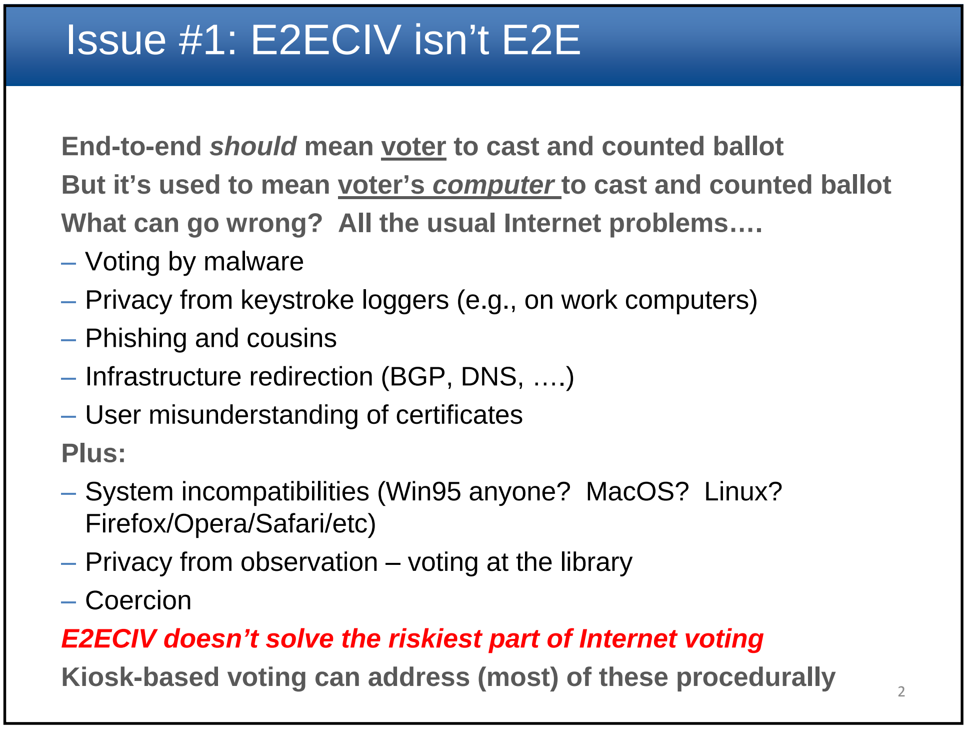


End-to-End Cryptographic Internet Voting Considered Harmful*

Presentation to the
NIST End-to-End Voting Workshop
Washington DC
October 14 2009

Jeremy Epstein
Senior Computer Scientist
SRI International
jeremy.epstein@sri.com
703-989-8907

* With apologies to Edsgar Dijkstra



Issue #1: E2ECIV isn't E2E

End-to-end *should* mean voter to cast and counted ballot

But it's used to mean voter's *computer* to cast and counted ballot

What can go wrong? All the usual Internet problems….

- Voting by malware
- Privacy from keystroke loggers (e.g., on work computers)
- Phishing and cousins
- Infrastructure redirection (BGP, DNS, ….)
- User misunderstanding of certificates

Plus:

- System incompatibilities (Win95 anyone? MacOS? Linux? Firefox/Opera/Safari/etc)
- Privacy from observation – voting at the library
- Coercion

E2ECIV doesn't solve the riskiest part of Internet voting

Kiosk-based voting can address (most) of these procedurally

Issue #2: Now Harry, this is very advanced magic

What happens

Voter selects candidates

Some crypto mumbo-jumbo occurs

Voter gets a receipt that gives a code

Voter takes the receipt home and (maybe) enters it into a computer system

Voter is told that proves her vote was counted

What the voter perceives

I told the computer what to do

It did something

Something magical happens

And I'm supposed to believe that my vote was counted accurately and privately?

Issue #3: Certifiably Insane

How to write certification requirements that

– Allow "good" E2ECIV

– Disallow "bad" E2ECIV (e.g., E1C)

… and can be enforced by state and local election officials who

– Have little technical expertise

– Can be misled by salespeople

Issue #4: Transparency to elected and election officials

Audience for voting systems is elected officials (e.g., legislators)

- Vested interest in reelection
- Minimal technical skills (usually)
- Short attention spans
- Perceive themselves as experts because they got elected!

… who look to election officials

- Can they understand well enough to explain to legislators?
- Will they risk getting burned again after the DRE fiasco?

What should happen next?

Usability studies

- Can elected and election officials understand?
- Can average voters understand?
- Will voters accept without understanding?

How do we make the system truly E2E, all the way to the voter?

How can E2ECIV systems get certified properly?

Questions?

End-to-End Cryptographic Internet Voting Considered Harmful

Jeremy Epstein
Senior Computer Scientist
SRI International
jeremy.epstein@sri.com
703-989-8907