**Integrating Security and Fault Tolerance**
Andrew Myers, Ken Birman, Fred Schneider (Cornell University)

**NSF Grant 0430161**

**Goal: Frameworks for developing secure, fault-tolerant distributed systems**

**Civitas: a secure remote voting system** (Oakland’08)

http://www.cs.cornell.edu/projects/civitas

with Michael Clarkson, Steve Chong

**And strong threats:**
- Adversary may compromise election machinery, coerce voters, control network
- Unsupervised voters

**Impact**
- Performance results show cost is practical (compute time: 4¢ per voter)
- Strongest known security guarantees for any implemented voting system; no reliance on single trusted DRE supplier.
- Conclusion: secure electronic voting may be practical!

**Strong, conflicting requirements:**
- Verifiability: all voters have assurance that final tally is correct
- Coercion Resistance: Voters cannot prove how they voted
- Availability during voting

System based on scheme proved cryptographically secure [JCJ’05]
- Extensions: ballot boxes for availability, distributed registration tellers for coercion resistance
- Jif [Myers et al.] captures requirements with information flow, declassification, and erasure policies.

**Insight: treat protocols as strongly typed live objects**
- Compose diverse protocols (state machine replication, multicast, transactions, membership, gossip) in a single framework
- High-level structures built with drag and drop interface, often without writing any code

**Live Objects**

http://liveobjects.cs.cornell.edu

with Kzrystof Ostrowski

"If one replica of object X receives event A on channel P, all replicas of X must eventually either crash or deliver event B on channel Q."

**http://liveobjects.cs.cornell.edu**

with Kzrystof Ostrowski

**Impact**
- Performance results show cost is practical (compute time: 4¢ per voter)
- Strongest known security guarantees for any implemented voting system; no reliance on single trusted DRE supplier.
- Conclusion: secure electronic voting may be practical!