CS 395T

Internet Voting

Ashok

What is “E-voting”

Thomas Edison received US patent number 90,646 for an electrographic vote recorder in 1869.

Specific implementations :

1) electronic counting
2) kiosk voting – Direct Recording Electronic (DRE) machines
3) remote electronic voting (REV) – Internet (voting applet, website), text messaging, touch-tone phone, etc.

DREs and REVs fail to provide voter-verifiable audit trails, undermining voter confidence.

Security Criteria

Criteria fall in 2 categories - keep votes secret, and provide secure and reliable voting infrastructure.

Most popularly accepted (technological) :

1) system integrity and reliability – vote counting must produce <u>reproducibly</u> correct results
2) data integrity and reliability
3) voter anonymity and data confidentiality – voting counts must be protected from outside reading during voting process
4) operator authentication – no trapdoors for maintenance or setup!
5) system accountability

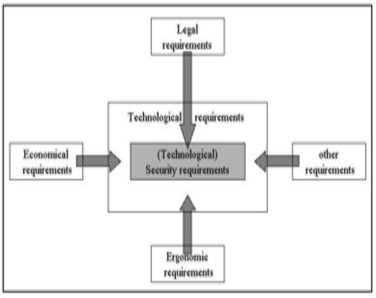
Security Criteria cont’d

6) system disclosability
7) system availability
8) usability

Challenge comes from contradiction between voter confidentiality and system accountability.

Problems & Attacks

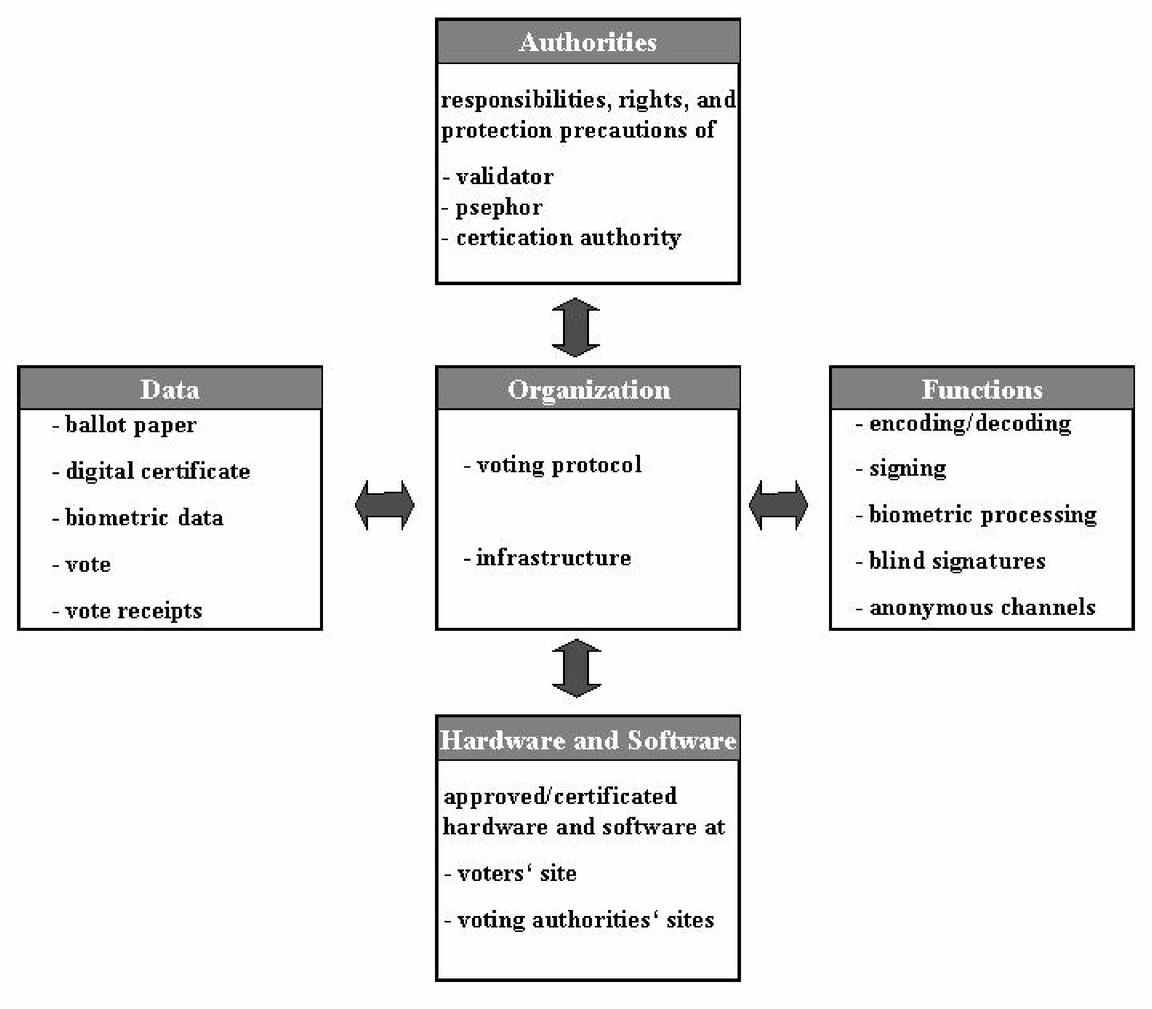
Overriding problem is voter disenfranchisement



Problems & Attacks cont'd

- Internet voting should at a minimum address issues and doubts of absentee voting
- Coercion even more problematic with Internet voting
  - Internet facilitates large-scale vote selling and buying, perhaps automated
- Malicious software and access to shared computers
- Data in system need not need modification but public disclosure, even after polling period
- (last-day) DoS attacks
- DNS attacks
- Priority of electronic vs. traditional ballots

Framework



Authorities

responsibilities, rights, and protection precautions of

- validator
- psephor
- certication authority

Data

- ballot paper
- digital certificate
- biometric data
- vote
- vote receipts

Organization

- voting protocol
- infrastructure

Functions

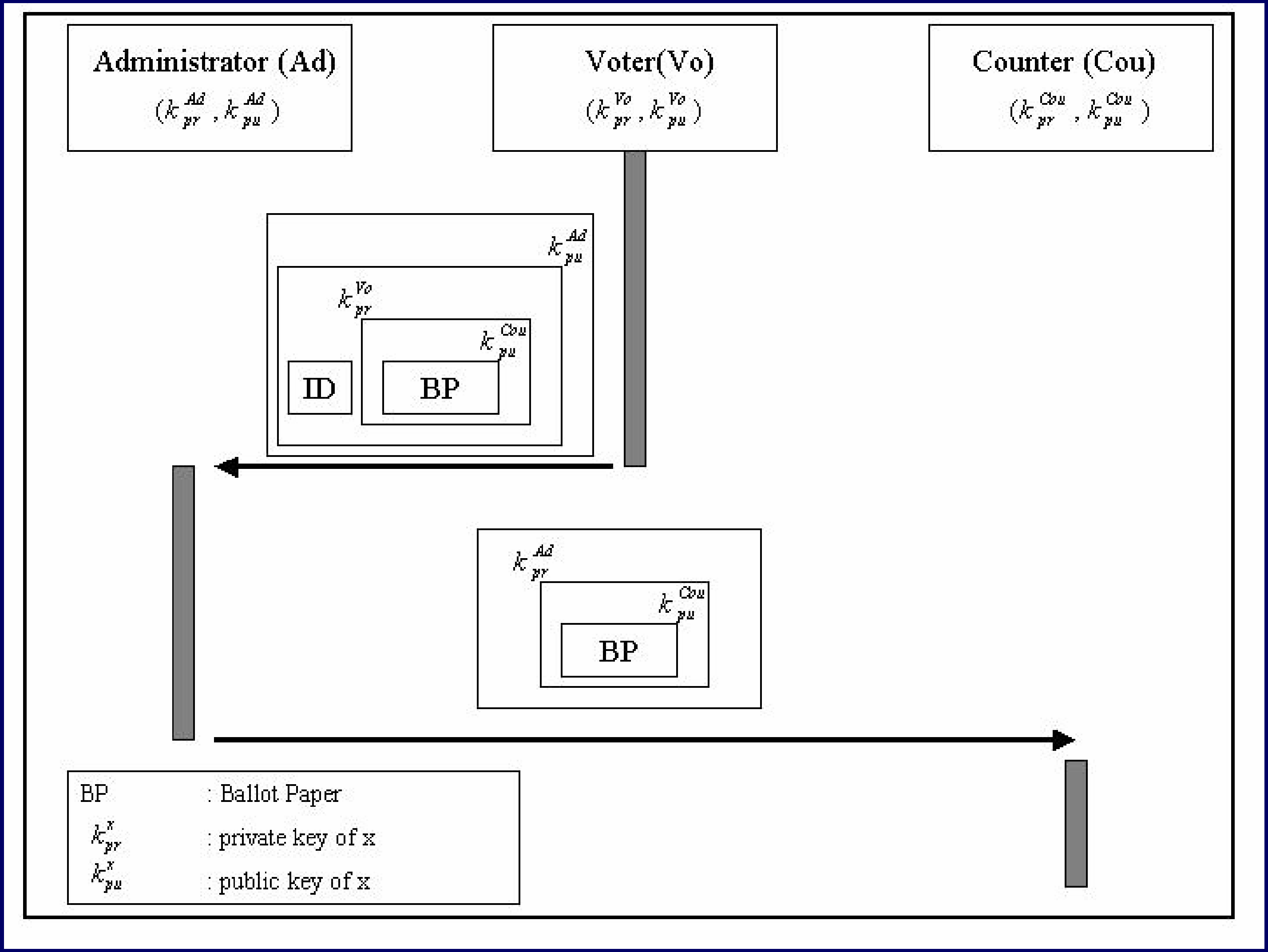
- encoding/decoding
- signing
- biometric processing
- blind signatures
- anonymous channels

Hardware and Software

approved/certificated hardware and software at

- voters' site
- voting authorities' sites

Trustworthy Entities

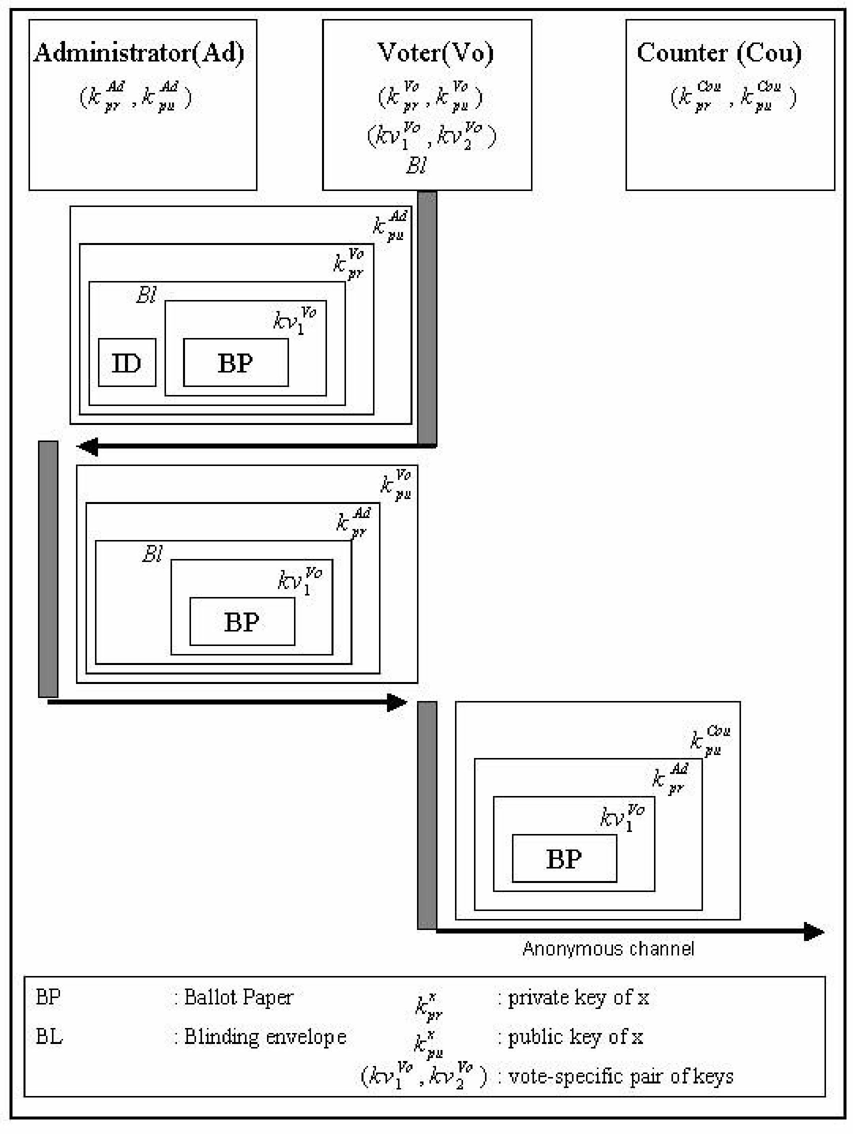


BP : Ballot Paper

k_{pr}^{x} : private key of x

k_{pu}^{x} : public key of x

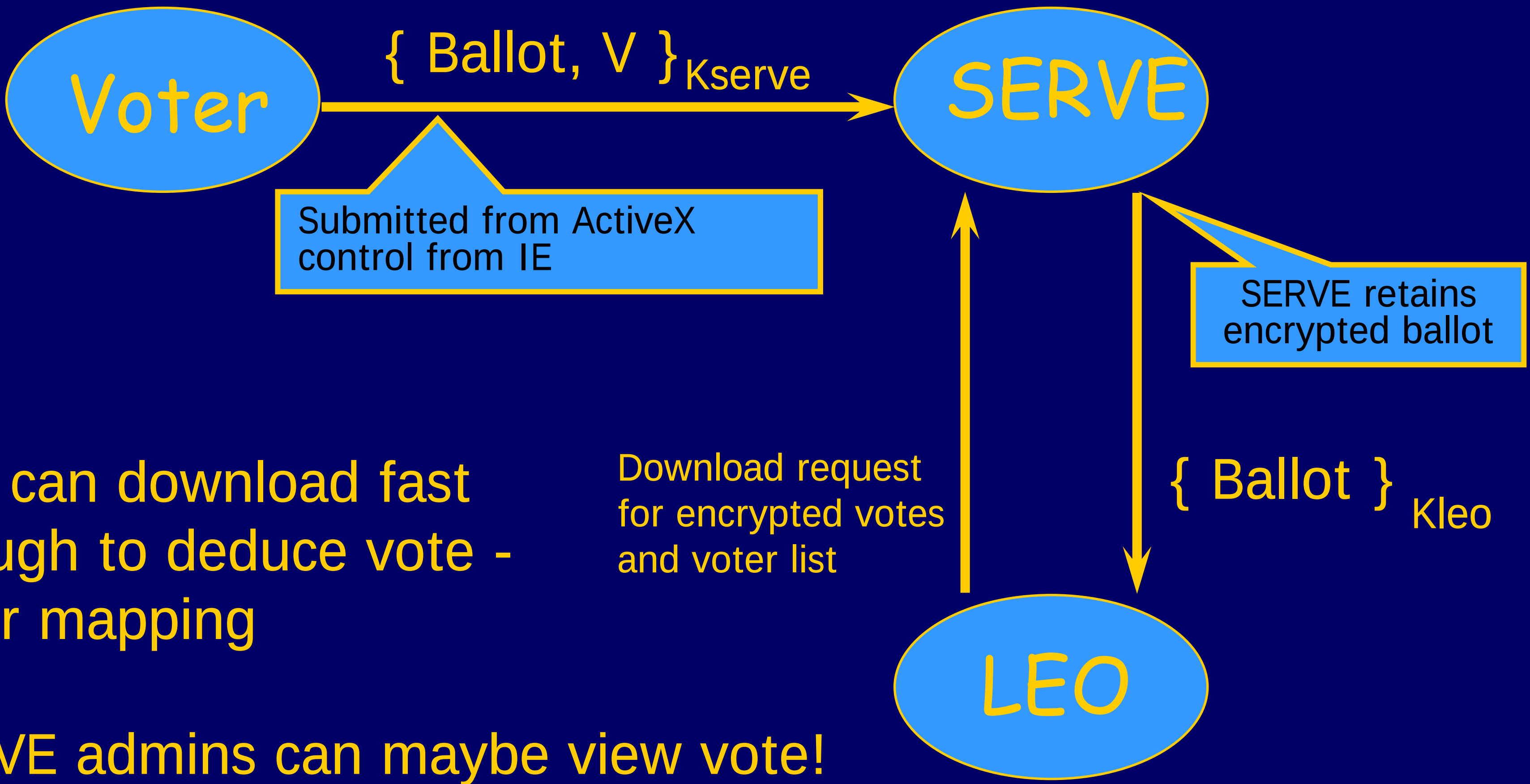
Blinding Signatures and Anonymous Channels



Secure Electronic Registration and Voting Experiment (SERVE)

- Built by Accenture and DoD Federal Voting Assistance Program (FVAP)
  - Covered by Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA)
- Follow-up to Voting Over the Internet (VOI)
  - Built by Booz-Allen & Hamilton with different architecture and codebase
  - Used in 2000 election to collect 84 votes in Florida, South Carolina, Texas, and Utah
  - FVAP's 2001 *Voting Over the Internet Pilot Project Assessment Report* - 50 votes in Florida!
  - Abandoned over DoS and malicious software exposure

SERVE cont'd



Voter

$\{ \text{Ballot, V} \}_{\text{Kserve}}$

SERVE

Submitted from ActiveX control from IE

SERVE retains encrypted ballot

Download request for encrypted votes and voter list

$\{ \text{Ballot} \}_{\text{Kleo}}$

LEO

LEO can download fast enough to deduce vote - voter mapping

SERVE admins can maybe view vote!

SERVE cont’d

- Vote selling / buying still possible
  - selling of voting credentials
  - vote from different addresses using proxy server; orgs that use same IP address from all users in domain
- Backdoors – OS, games, device drivers, multimedia, browser plugins, screen savers, etc.
  - ActiveX control itself
- No voter verification
- Adversary can spoof voting server