A Consideration of Voting Accessibility for Injured OIF/OEF Service Members: Needs Assessment

July 2012

Contract E4064914
2010 Voting Technology and Accessibility Research – Military Heroes Initiative
CFDA #90.403

PREPARED FOR:
Election Assistance Commission
1201 New York Avenue, N.W.
Suite 300
Washington, D.C. 20005

PREPARED BY:
Human Systems Integration Division
Electronic Systems Laboratory
Georgia Tech Research Institute
Georgia Institute of Technology
Atlanta, Georgia 30332

Annotated Literature Review Results

Remote & Absentee Voting

Hoke, C. (2009). *Internet voting: Structural governance principles for election cyber security in democratic nations.* Paper presented at the Second International Symposium on Global Information Governance, Prague, Czech Republic.

> Internet voting may become more common in the near future, and associated security concerns will play a role in technology acceptance. Worldwide, governments often disregard opinions of computer security experts on the matter. The Internet provides little assurance of Data Security and integrity, and the transmission of information is susceptible to various attacks.
> The authors recommend that the each government appoint a policy board, whose members have the necessary technical expertise, and whose decisions are transparent to the public, to ensure end-to-end auditability of Internet voting technology. Rather than relying on a set of technical standards to be met, the policy board should assess proposals for internet voting systems on a case by case basis. Finally, democratic nations should notify each other of threats and attacks.

Krimmer, R., Triessnig, S., & Volkamer, M. (2007). *The development of remote e-voting around the world: A review of roads and directions.* Paper presented at The International Conference on E-voting and Identity, Bochum, Germany.

> Despite technological capabilities, governments have been slow to adopt remote electronic voting via the Internet. The authors surveyed 104 internet elections held worldwide. They found that documentation of security and privacy issues were scarce in these elections. Before Internet voting can become widespread, a great deal of research and documentation needs to be accomplished. Future studies should compare the effectiveness of various methods to ensure accurate voter verification, anonymity, system usability, and cost. A potential untapped data source is internet elections held in private organizations – a domain in which internet voting is much more common.

Popoveniuc, S. & Lundin, D. (2007). *A simple technique for safely using punchscan and Pret a Voter in mail-in-elections.* Paper presented at The International Conference on E-voting and Identity, Bochum, Germany.

> Traditional mail-in absentee ballots can be difficult to audit, use, and understand, and they do not ensure anonymity. This paper reviews the security of two mail-in systems –Punchscan and Pret a Voter – and discusses the novel system that overcomes their deficiencies. The proposed system employs unique serial numbers on each ballot, in combination with randomized letters associated with each choice on the ballot. Following the election, the serial number and letters from each ballot are published on the Internet. Voters can check their record against the published record to determine whether their vote was cast as intended.

Puiggali, J. & Morales-Rocha, V. (2007). *Remote voting schemes: A comparative analysis.* Paper presented at The International Conference on E-voting and Identity, Bochum, Germany.

Remote electronic voting via fax, e-mail, and the Internet can provide greater reliability than traditional mail-in ballots, which can be lost or delayed in the mail. Key considerations for the comparative evaluation of these methods including security (e.g., privacy and auditability), usability, intellect and management (e.g., vote counting). Although the public retains a general concern that internet voting is not secure, the present heuristic evaluation concluded that the risks associated with Internet voting are not more numerous than those associated with other forms of remote electronic voting, and many safeguards can mitigate the risks.

Qadah, G. Z. & Taha, R. (2007). Electronic voting systems: Requirements, design, and implementation. *Computer Standards & Interfaces, 29,* 376-386.

Remote electronic voting technology provides the possibility of lowering costs, increasing participation, and improving the accuracy of election results. This paper discusses design requirements and implementation of a remote electronic voting system, which enables voters to cast votes anytime and anywhere using personal computers, personal digital assistants, and cell phones. The voting system does not require the generation of content that is specific to each type of device. Instead, versatile technology such as extensible markup language can be used to represent the data content and style sheets, which can customize the ballot presentation for different connecting devices.

Reinhard, K. & Jung, W. (2007). *Compliance of POLYAS with the BSI protection profile - Basic requirements for remote electronic voting systems.* Paper presented at The International Conference on E-voting and Identity, Bochum, Germany.

In the past year and a half a group of experts in electronic voting developed a Common Criteria Protection Profile describing basic requirements for remote electronic voting systems. This work was lead managed by the German Federal Office for Information Security (BSI) and the German Research Center for Artificial Intelligence (DFKI) and initiated by the German Gesellschaft fur Informatik (GI - society for informatics). To complete this work Micromata's POLYAS system, which is used for the GI elections needs to be evaluated against this Protection Profile. As a first step a high-level evaluation based on the security objectives has been carried out. The results are presented in this paper.