Security Requirements for Non-political Internet Voting

R. Grimm (Universität Koblenz-Landau)
J. Helbach (GI Bonn)
R. Krimmer (Wirtschaftsuniversität Wien)
N. Meißner (PTB Berlin)
K. Reinhard (Micromata Kassel)
M. Volkamer (DFKI Saarbrücken)
M. Weinand (BSI Bonn)
Overview

• The Gesellschaft für Informatik
• GI Elections 2004 & 2005
• Restructuring of Requirements
• Meeting the Requirements
• Future of GI Elections
• International and European Standards
• Common Criteria & Protection Profiles
• Summary and Conclusions
The “Gesellschaft für Informatik”

• non-profit society with the goal to promote informatics
• about 24,000 members (mainly from Germany)
• structured in special interest groups, regional groups, advisory councils and working groups
• since July 2003 constitution allows internet voting
• parallel internet / postal elections held in ’04 and ‘05
GI Elections 2004

- Chairmanship election
- Voting system: POLYAS from Micromata
- Membership Number & PIN used for authentication
- Group of security experts accompanied election
- Circa 20,000 eligible voters
- 4,845 internet voters, 81 postal voters
- About 50% increase in turnout
GI Elections 2005

- Chairmanship and executive board elections
- improved POLYAS system used
- 4,030 internet voters, 82 postal voters
Restructuring of Requirements

• End 2004: decision to develop requirements catalogue for “Internet-based elections in societies”
  • security level not less than in postal voting
  • should be short and crisp (only a few pages)
  • used catalogues from Council of Europe, IEEE, and PTB amongst others as basis
  • published in August 2005 (GI web site)
Restructuring of Requirements

• **Structure of the catalogue:**
  • Preliminary notes and assumptions
  • General requirements on the system development and election execution
  • Requirements on the election servers
  • Requirements on the election software
Restructuring of Requirements

• Requirements on the election software:
  • General requirements on an Internet voting system and its security
  • Special functional requirements on the Internet voting system
  • Requirements with respect to the anonymity of votes
  • Specific requirements to ensure a universal and equal election
  • Ergonomic and usability requirements
Meeting the Requirements

• Micromata was requested to explain how POLYAS fulfills the requirements
• new major release of POLYAS to comply with new requirements
  • separation of ballot box and election register servers
  • third server called validator signs entries in election register and checks signature on voter before it enables him to vote
• better system recovery
• detection of manipulation w/o violating anonymity
• several mechanisms to minimise possible system attacks
• documentation of technical and organisational solutions to accomplish the security requirements
• anonymous creation of voter’s PINs for print service provider
Meeting the Requirements

• Two Workshops revealed four new challenges
  • Source code inspection: to increase trust external experts and experts from PTB inspected parts of the source code
  • simplified voter’s guide: GI expert group specified guidelines for online voters
  • CC standardisation of requirements: working group was founded to specify CC Protection Profile for Internet voting in private societies and other non-governmental organisations
  • suitable comparison of Internet voting with postal voting
Future of GI Elections

- plans for the POLYAS in 2006:
  - improvement of protocol for better system recovery after failures
  - implementation of m-n threshold scheme for key distribution
  - support of EML for easier configuration management
  - modified modules to help administer elections at GI subsections

- long term plans:
  - rich voting client using bulletin board technologies
International and European Standards

• Collections of requirements (examples):
  • “Regulations of Voting Machines for Elections of the German and European Parliament” (Germany ‘79/’99)
  • “Project 1583 - Voting Equipment Standard” (IEEE 2005)
  • “Online Voting Systems for Non-parliamentary Elections - Catalogue of Requirements” (PTB 2004)
  • “Legal, Operational and Technical Standards for E-Voting” (Council of Europe 2004)

• Election Markup Language v.4 (OASIS 2005)
Common Criteria & Protection Profiles

- Common Criteria (CC): international standard for computer security (ISO 15408)
- resulted from a standardisation of national security criteria from different sources
- allows users to specify security requirements
- allows developers to specify security attributes of their products
- allows evaluators to determine if products meet their claims
Common Criteria & Protection Profiles

• CC contains three parts:
  • Introduction and Common Model
  • Security Functional Requirements
  • Security Assurance Requirements
• related document “Common Evaluation Methodology”
  • guides the evaluator in applying CC
• CC defines two important documents:
  • Protection Profile and Security Target
Common Criteria & Protection Profiles

• Protection Profile:
  • set of security requirements for category of products
  • independent of technical solutions
  • requirements described in a semiformal way defined by CC
  • description part with security concept, threats and mapping of requirements to threats
  • can go through formal evaluation
Summary and Conclusions

• GI elections in 2004 and 2005 were very successful
• security requirements formulated by expert group
• Voting System POLYAS is developed further
• Protection Profile is standardised way to formulate security requirements
• GI initiated working group to work on Protection Profile
• first published version of PP expected late Summer 2006