InnoVote Database Access Matrix

User Security Model

By
Erin Thead
Software Engineer
erin@erinthead.com

Table of Contents – Database Access Matrix

1. Introduction

1.1. Purpose.

The purpose of this document is to communicate a privilege or access policy for the databases used by InnoVote software products. The document provides a list of privileges that every software operation of an InnoVote software product will need for correct functionality.

The intended audience of this document is the developer and any other persons interested in the project, including election reform activists, computer security professionals, political figures with an interest in election reform, and potential buyers of the design.

1.2. Scope.

The InnoVote line of election products will need to store election data in databases. In deployment, every InnoVote system will have a local database and DBMS. Since the integrity of the election data is of paramount importance, these databases must be designed to protect sensitive data. Existing election databases allow easy modification of sensitive data and rely on an "honor system" for election officials and election software vendors.

As is described in references [2], [6], [7], and [8], numerous software functions of InnoVote products require a secure database to operate correctly. These software operations need to have access to certain tables, and in some cases, certain fields in tables, but do not need access to others. In some cases, date and time constraints exist on when the software can perform certain operations. The user privilege model proposed in this document will provide the required security to protect the integrity of sensitive election data.

Reference [3] describes the structure of the database tables, proposes authentication methods for granting access to the database, and suggests two user privilege models. The first of these models proposes that each InnoVote software product be treated as a separate user. The second model proposes granting user status to each separate software *operation*. The second model, while more expensive in computation and storage requirements, is demonstrably more secure. This document expands upon it and describes exactly what privileges each software operation (taken from the requirements of each Functional Design document) will need to operate correctly.

1.3. References.

[1] Thead, E. *InnoVote CardReader Hardware Requirements Overview,* 2005
[2] Thead, E. *InnoVote CardReader Functional Design*, 2005
[3] Thead, E. *InnoVote Database Detailed Design*, 2005
[4] Thead, E. *InnoVote MyVotronic Hardware and Operating System Overview*, 2005
[5] Thead, E. *InnoVote Network Detailed Design*, 2005
[6] Thead, E. *InnoVote ReliaVote Central Server Functional Design*, 2005
[7] Thead, E. *InnoVote ReliaVote Precinct Edition Functional Design*, 2005
[8] Thead, E. *InnoVote SecureDRE Functional Design*, 2005
[9] Thead, E. *Security Analysis of InnoVote Products*, 2005.

1.4. Overview.

The remainder of this document is organized in the following fashion:

Section 2: Contains a list of assumptions for the access matrix. Also contains a list of all functional requirements (taken from the Functional Design documents) for each InnoVote software product. The table shows the access levels that each software operation will have to every table in the database. Some operations have time constraints that are shown in the list as separate items; it is assumed that when an operation has only one entry in the list, the privileges apply no matter what the date and time are.

2. Access Matrix

2.1. Assumptions and Dependencies.

2.1.1. Local authentication assumption

The document assumes that network security policies and the database management system will disallow remote logins to any database stored on a device running an InnoVote software product. All user authentications must have originated on the local machine. This assumption implies that the only database that any installation of an InnoVote software product will be able to use is the database for its own machine.

2.1.2. Software operation user assumption

This document assumes that the database management system is configured to allow access as described in reference [3], section 5.2.2: "This configuration involves creating separate 'users' for every software operation (described in the Functional Design documents […] that needs to use a table. Each operation needs to authenticate itself to the DBMS, which then grants it the proper privileges."

2.2. Matrix

Legend

FR = Functional Requirement (from the Functional Design)
CRDR = InnoVote CardReader Software
RVCS = InnoVote ReliaVote Central Server
RVPE = InnoVote ReliaVote Precinct Edition
SDRE = InnoVote SecureDRE
PRE = Time before Election Day
PST = Time from Election Day to time at which votes can be deleted
R = Read entries
A = Add entries
M = Modify existing entries
D = Delete existing entries

Table Name / Functional Requirement/Time	Elections	Ballots	Candidates	Parties	Contests	Precincts	Errors	Votes	Running	Affiliations	Tallies	Realtime_Votes	Recount_Votes	Recount_Tallies
CRDR FR 01						R	A							
CRDR FR 02/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
CRDR FR 02/PST	R						A							
CRDR FR 03	R		R	R	R	R	A		R	R				
CRDR FR 04	R	A	R	R	R	R	A	A	R	R	AM	A	A	AM
CRDR FR 05		M					A							
CRDR FR 06		R					A					R		
CRDR FR 07							A							
CRDR FR 08							A							
CRDR FR 09	R	M					A							
CRDR FR 10		R					A	R			R	R		
CRDR FR 11							RA							
CRDR FR 12		RAM					A						RA	RAM
CRDR FR 13/PRE	R	RD					A	RD			RD	RD	RD	RD
CRDR FR 13/PST	R						A							
RVCS FR 01/PRE						RAMD	A							
RVCS FR 01/PST							A							
RVCS FR 02							A							
RVCS FR 03/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
RVCS FR 03/PST	R						A							
RVCS FR 04/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
RVCS FR 04/PST	R						A							
RVCS FR 05		AM					A	AM			AM		AM	AM
RVCS FR 06		R					A	R			R	R	R	R
RVCS FR 07							A							
RVCS FR 08							RA							
RVCS FR 09	R					R	A		R	R	R			R
RVCS FR 10/PRE	R	RD					A	RD			RD	RD	RD	RD
RVCS FR 10/PST	R						A							
RVCS FR 11							A							
RVCS FR 12							A							
RVCS FR 13							A							
RVCS FR 14							A							
RVCS FR 15							A							
RVCS FR 16							RA							
RVCS FR 17	R		R	R	R	R	A		R	R				
RVPE FR 01/PRE						RAMD	A							
RVPE FR 01/PST							A							
RVPE FR 02							A							
RVPE FR 03/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
RVPE FR 03/PST	R						A							

Table Name / Functional Requirement/Time	Elections	Ballots	Candidates	Parties	Contests	Precincts	Errors	Votes	Running	Affiliations	Tallies	Realtime_Votes	Recount_Votes	Recount_Tallies
RVPE FR 04/PRE	R		R	R	R	R	A		R	R				
RVPE FR 04/PST	R						A							
RVPE FR 05							A					AM		
RVPE FR 06/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
RVPE FR 06/PST	R						A							
RVPE FR 07	R						A		R					
RVPE FR 08							A					AM		
RVPE FR 09							A							
RVPE FR 10							A							
RVPE FR 11	R						A							
RVPE FR 12	R						A	RA			RAM			
RVPE FR 13	R						A	RA			RAM			
RVPE FR 14		R					A	R	R		R	R		
RVPE FR 15							RA							
RVPE FR 16							RA							
RVPE FR 17							A							
RVPE FR 18		R					A	R			R	R	R	R
RVPE FR 19							A				R			
RVPE FR 20							A							
RVPE FR 21		RAM					A						RA	RAM
RVPE FR 22							A							R
RVPE FR 23/PRE	R	RD					A	RD			RD	RD	RD	RD
RVPE FR 23/PST	R						A							
RVPE FR 24	R						A							
RVPE FR 25							RA							
RVPE FR 26							A							
RVPE FR 27							A							
RVPE FR 28							A							
RVPE FR 29							A							
RVPE FR 30							A							
SDRE FR 01						R	A							
SDRE FR 02/PRE	RAMD		RAMD	RAMD	RAMD	RAMD	A		RAMD	RAMD				
SDRE FR 02/PST	R						A							
SDRE FR 03	R		R	R	R	R	A		R	R				
SDRE FR 04	R		R	R	R	R	A		R	R				
SDRE FR 05	R		R	R	R	R	A		R	R				
SDRE FR 06	R		R	R	R	R	A		R	R				
SDRE FR 07		A					A	A			AM	A		
SDRE FR 08		R					A	R						
SDRE FR 09		RAM					A	A			AM	A		
SDRE FR 10		R					A					R		

Table Name / Functional Requirement/Time	Elections	Ballots	Candidates	Parties	Contests	Precincts	Errors	Votes	Running	Affiliations	Tallies	Realtime_Votes	Recount_Votes	Recount_Tallies
SDRE FR 11		RM					A							
SDRE FR 12							A							
SDRE FR 13							A							
SDRE FR 14	R	M					A							
SDRE FR 15		R					A	R			R	R		
SDRE FR 16							A							
SDRE FR 17/PRE	R	RD					A	RD			RD	RD	RD	RD
SDRE FR 17/PST	R						A							