Hierodiction Software

EVOTE LGG: Logging and Audit System

EVOTE IDC: Intrusion Detection Cockpit

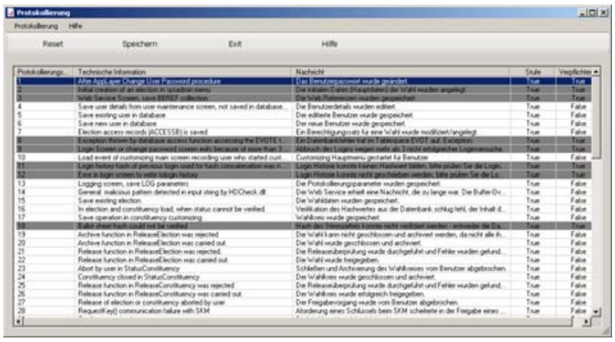
“Logging” vs. Audit System

Conventional e-voting or other security-related systems offer classical logging, whether in files or in a (maybe encrypted) database table. This however does not enable fast, real-time search and auditing capabilities as they are needed in an election environment.

EVOTE LGG offers a comprehensive auditing system that is structured as a multi-dimensional data warehouse to enable fast and to-the-point access to the relevant facts needed in an audit situation.

Benefits

Customisability: LGG can be adapted to your needs by offering a large number of possible logging points and enabling administrators to choose which points to enable. Some sensitive logging events however may not be deselected.



Protokollierungs...	Technische Information	Nachricht	Stufe	Verpflichtet
1	After AppLayer Change User Password procedure	Das Benutzerpasswort wurde geändert	True	True
2	Initial creation of an election in quadrant menu	Die initialen Daten (Hauptdaten) der Wahl wurden angelegt	True	True
3	Web Service Screen, save BBREF collection	Die Web Referenzen wurden gespeichert	True	True
4	Save user details from user maintenance screen, not saved in database...	Die Benutzerdetails wurden editiert.	True	False
5	Save existing user in database	Der editierte Benutzer wurde gespeichert	True	False
6	Save new user in database	Der neue Benutzer wurde gespeichert	True	False
7	Election access records (ACCESSB) is saved	Ein Berechtigungssatz für eine Wahl wurde modifiziert/angelegt	True	False
8	Exception thrown by database access function accessing the EVOTE I...	Ein Datenbankfehler trat im Tablespace EVOT auf: Exception	True	True
9	Login Screen or change password screen exits because of more than 3 ...	Abbruch des Logins wegen mehr als 3 nicht erfolgreicher Loginversuche	True	True
10	Load event of customizing main screen recording user who started cust...	Customizing Hauptmenü gestartet für Benutzer	True	False
11	Login history hash of previous login used for hash concatenation was in...	Login Historie konnte keinen Hashwert bilden, bitte prüfen Sie die Login...	True	True
12	Error in login screen to write tologin history	Login Historie konnte nicht geschrieben werden, bitte prüfen Sie die Lo...	True	True
13	Logging screen, save LOG parameters	Die Protokollierungsparameter wurden gespeichert.	True	False
14	General: malicious pattern detected in input string by HDCheck.dll	Der Web Service erhielt eine Nachricht, die zu lange war. Die Buffer-Ov...	True	False
15	Save existing election.	Die Wahldaten wurden gespeichert.	True	False
16	In election and constituency load, when status cannot be verified.	Verifikation des Hashwertes aus der Datenbank schlug fehl, der Inhalt d...	True	False
17	Save operation in constituency customizing	Wahlkreis wurde gespeichert.	True	False
18	Ballot sheet hash could not be verified	Hash des Stimmzettels konnte nicht verifiziert werden - entweder die Da...	True	True
19	Archive function in ReleaseElection was rejected	Die Wahl kann nicht geschlossen und archiviert werden, da nicht alle ih...	True	False
20	Archive function in ReleaseElection was carried out.	Die Wahl wurde geschlossen und archiviert.	True	False
21	Release function in ReleaseElection was rejected.	Die Releaseüberprüfung wurde durchgeführt und Fehler wurden gefund...	True	False
22	Release function in ReleaseElection was carried out.	Die Wahl wurde freigegeben.	True	False
23	Abort by user in StatusConstituency	Schließen und Archivierung des Wahlkreises vom Benutzer abgebrochen	True	False
24	Constituency closed in StatusConstituency	Der Wahlkreis wurde geschlossen und archiviert.	True	False
25	Release function in ReleaseConstituency was rejected	Die Releaseüberprüfung wurde durchgeführt und Fehler wurden gefund...	True	False
26	Release function in ReleaseConstituency was carried out.	Der Wahlkreis wurde erfolgreich freigegeben.	True	False
27	Release of election or constituency aborted by user	Der Freigabevorgang wurde vom Benutzer abgebrochen.	True	False
28	RequestKey() communication failure with SKM	Anforderung eines Schlüssels beim SKM scheiterte in der Freigabe eines ...	True	False

Encryption and Data Integrity: All logging entries are of course encrypted, in addition, the integrity of each log record and of the log as a whole is maintained by checking values (SHA-1 hash) which are checked when the log is accessed.

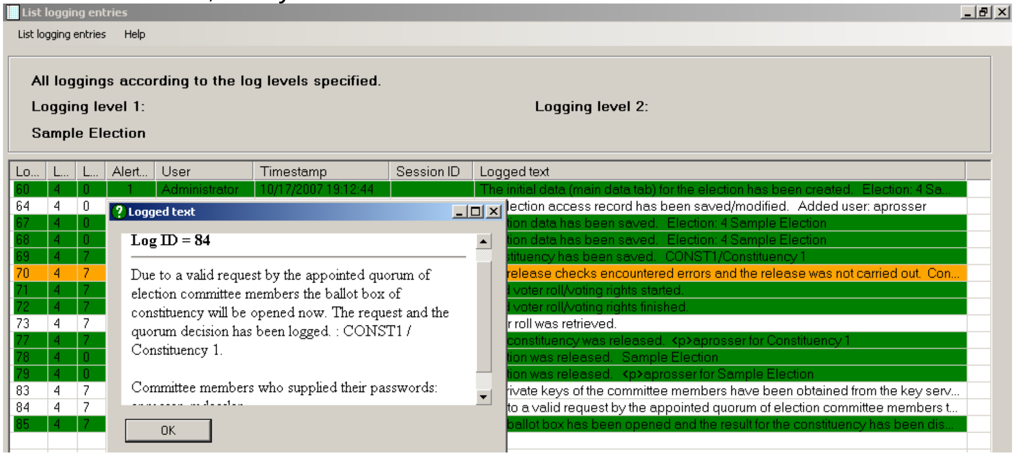
Multi-dimensional Structure: The log entries are stored in a multi-dimensional cube structure, which enables fast and specific search capabilities, e.g.: “all log entries for a certain constituency”, “all log entries for a certain voter”, “all system alarms”.

Complete Auditability: EVOTE offers a large number of standard reports that enable audits over the entire life cycle of an election. In addition, customer-specific reports may be added at any time due to the flexible structure of the logging system. All EVOTE components including VRL and SKM use the logging and auditing system, hence providing a seamless and comprehensive audit trail.

Integration in Access Concept: LGG seamlessly integrates into a role-based access concept ensuring that users can only access information where they are authorized to do so.

Re-use: LGG is a .net dll assembly with defined and documented interfaces as well as standard reports that may be used by any other application that can access .net assemblies. LGG also works with its own separate database, which makes it easily separable from EVOTE.

Since some dimensions of the LGG data warehouse structure can be redefined, the system may adapt to a wide variety of applications and also integrate in their respective access concept.



All loggings according to the log levels specified.

Logging level 1:

Logging level 2:

Sample Election

Lo...	L...	L...	Alert...	User	Timestamp	Session ID	Logged text
60	4	0	1	Administrator	10/17/2007 19:12:44		The initial data (main data tab) for the election has been created. Election: 4 Sa...
64	4	0					lection access record has been saved/modified. Added user: aprosser
67	4	0					tion data has been saved. Election: 4 Sample Election
68	4	0					tion data has been saved. Election: 4 Sample Election
69	4	7					stituency has been saved. CONST1/Constituency 1
70	4	7					release checks encountered errors and the release was not carried out. Con...
71	4	7					l voter roll/voting rights started.
72	4	7					l voter roll/voting rights finished.
73	4	7					r roll was retrieved.
77	4	7					constituency was released. <p>aprosser for Constituency 1
78	4	0					tion was released. Sample Election
79	4	0					tion was released. <p>aprosser for Sample Election
83	4	7					rivate keys of the committee members have been obtained from the key serv...
84	4	7					to a valid request by the appointed quorum of election committee members t...
85	4	7					ballot box has been opened and the result for the constituency has been dis...

Log ID = 84

Due to a valid request by the appointed quorum of election committee members the ballot box of constituency will be opened now. The request and the quorum decision has been logged. : CONST1 / Constituency 1.

Committee members who supplied their passwords:

Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at

Intrusion Detection Cockpit (IDC)

The cockpit enables system administration staff to constantly monitor EVOTE activity, particularly during an ongoing election. All voting sessions are tracked by LGG and each request from a voting client is checked for

- ☞ Consistency with the voting process;
- ☞ Timeouts;
- ☞ Malicious content

and a large number of other potentially malicious activities. Also the data integrity of the EVOTE database is consistently checked. Any suspicious activity causes an alarm in the Logging and Audit System LGG.

Furthermore, (innocent) system malfunctions (e.g. a database problem) cause alarms in the Cockpit. alerting administration staff immediately. The principles are:

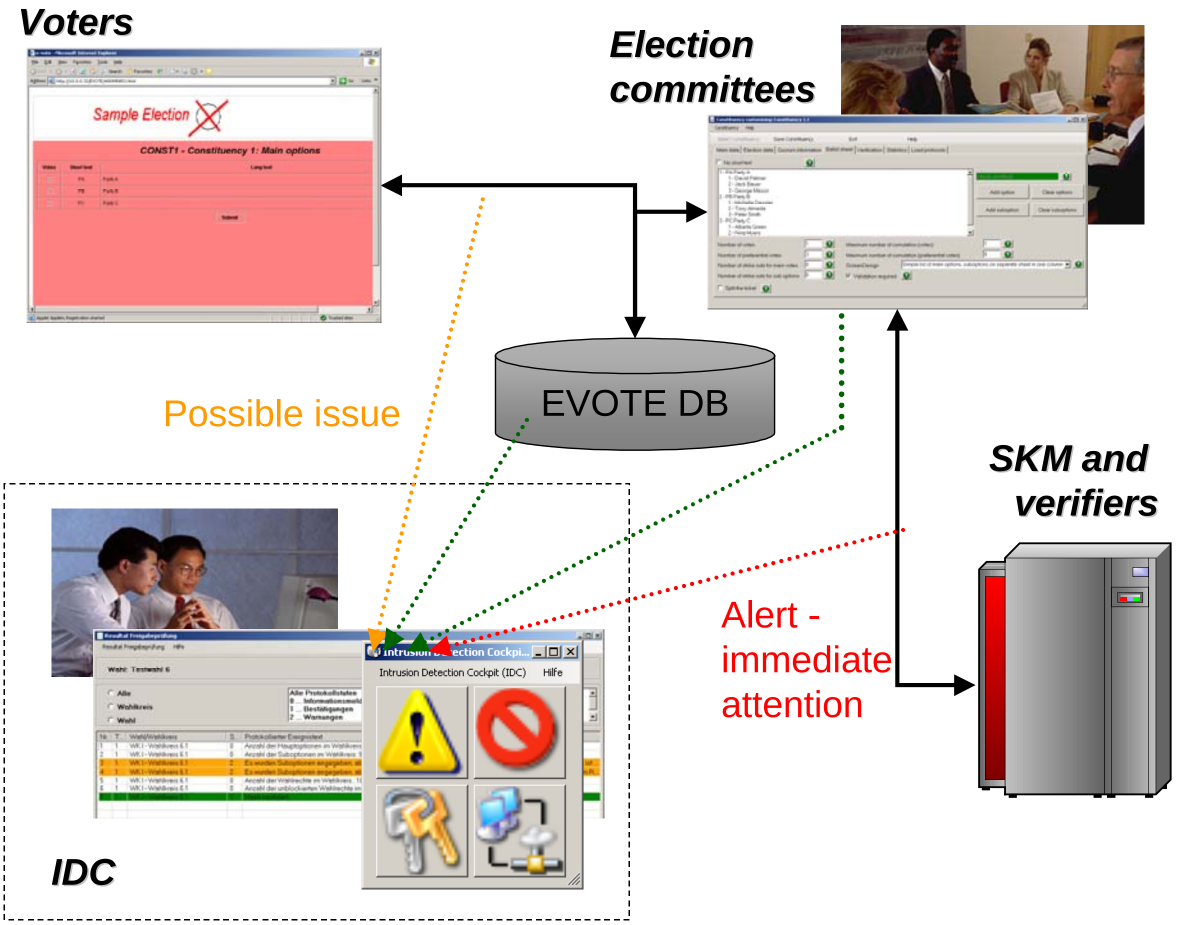
- ☞ Constant monitoring of all components;
- ☞ Process oriented threat pattern recognition;
- ☞ Automatic threat classification;
- ☞ Additional information for locating the issue;
- ☞ Immediate administrator notification.

System activities are not just scanned “as such”, but assessed in a process context, where previous communications from the same communication partner are taken into account in the analysis. Thereby **also complex threat patters can be recognized**.

With its high level of **automated surveillance and threat classification** the Intrusion Detection Cockpit is designed to assist system administrators in monitoring EVOTE. Administration thereby maintains a high-level and comprehensive “big picture” overview of system activity during an election.

At the same time, administrators may “drill down” into each alert and obtain more detailed information on the nature and source of the alert enabling them to effectively respond to the issue.

The IDC covers all application components of EVOTE and ideally supplements an infrastructure-based intrusion detection system.


Voters
Sample Election
CONST1 - Constituency 1: Main options
Election committees
EVOTE DB
Possible issue
SKM and verifiers
Alert - immediate attention
Intrusion Detection Cockpit (IDC)
Hilfe
IDC

Contact: Hierodiction Software GmbH, Rabengasse 6, A-2230 Gänserndorf. http://www.hierodiction.at