

option



retu



vote



tab



Secure Oracle9*i*AS Gets Their E-VOTE

Security features in Oracle9*i*AS make online voting a success.

By David A. Kelly

There's no telling how Al Capone, the infamous Chicago gangster who advised his corrupt followers to "vote early and vote often," would have reacted to recent elections in St. Albans, U.K., but we can only guess it wouldn't have been favorably.

By using an electronic voting (e-voting) system based on Oracle9*i* Application Server (Oracle9*i*AS), he certainly would have been able to vote early—any time from Thursday night through Saturday. In fact, he could easily have voted from a computer or cell phone, if he had one. However, thanks to some clever application design and security features built into Oracle9*i*AS, he would certainly have had a problem voting often.



Situated to the north of London, St. Albans has a population of just under 130,000. The city was home to a successful online voting initiative last year.

"We made sure that when users voted, it couldn't be changed, and they couldn't vote again," says David Litchfield, cofounder of Next Generation Software (NGSSoftware), an internationally recognized security consulting firm. "We really tried to subvert the system and found there are easier ways to break a voting system than by hacking into the internet-based application."

Who can forget the recent back-to-back election fiascos in Florida? If nothing else, those elections showed how important each vote was and highlighted how problematic traditional and even new electronic voting machines can be. Since then, a variety of local, state, and national governments have started re-evaluating their voting processes and technologies in hopes of increasing voter participation, speeding election results, and replacing outmoded voting machines. And Oracle9iAS, with its robust security architecture and resilience, has emerged as a key enabling technology for new e-voting solutions.

"E-voting systems have to demonstrate reliability and availability," says Christopher Baum, vice president, Gartner, Inc., a Connecticut-based research and advisory firm. "People have to believe in the system and that the voting is secure." With security requirements that stretch from the application design to deployment to management and monitoring, St. Albans' e-voting application is a composite of many of the challenges facing businesses as they attempt to develop secure applications. It also provides an example of how to combine Oracle9iAS and Java-based applications to create a mission-critical system that gets the job done. Organizations considering (or using) Oracle9iAS as a platform for deploying business applications can learn from the lessons the Oracle team faced while implementing the St. Albans e-voting application.

ST. ALBANS' ELECTRONIC VOTE

The St. Albans District Council, in St. Albans, U.K., is a regional government trying to modernize its elections through the use of e-voting. In May 2002's local elections, St. Albans piloted an e-voting system that included multiple voting channels—every-

thing from kiosks to telephones to the internet. "The goal of this pilot was to introduce new technologies to simplify the electoral procedure. We believe the success of the St. Albans campaign will no doubt be part of the foundation of future voting methods used worldwide," says Mike Lovelady, the Returning Officer (voting supervisor) for St. Albans.

Used in two of St. Albans' voting wards with a total of 10,000 eligible residents, the e-voting system was codeveloped by Oracle and British Telecommunications Plc. It was the first fully electronic election in the U.K., with no in-person paper-based

voting allowed. Voters were issued a polling card and personal identification number (PIN) that was delivered by the postal service, and a voting identification number (VIN) that was hand-delivered separately by an election official. Voters were then able to use these in any of the following voting channels to cast their vote:

- **Internet.** By using their VIN and PIN numbers and a standard internet connection, citizens could vote by computer from anywhere in the world.
- **Kiosk.** E-voting kiosks were set up at multiple, standard polling places for registered voters to cast their vote. An experimental kiosk was also set up in a large supermarket.
- **Interactive Voice Recognition (IVR).** Citizens could use normal or mobile phones to connect to an IVR system that would record votes.
- **Postal.** Votes could also be cast using the U.K.'s standard postal methods, where an election worker would then use an electronic terminal to enter citizens' votes.

The e-voting application included a common layer across these different channels for voting procedures and channel connection. It also provided a secure option for the presiding officer at a polling station to use to search for a voter by name. If voters did not have their VIN/PIN, the presiding officer could check other identification and enable them to vote via the name search function. "The system was designed not to allow people to vote twice," says John Abel, principal consultant, Oracle U.K. "If they had already voted via the internet and then went to a polling station to try to vote, it would inform the voter that they had already voted."

When it was all said and done, the election was a success, with more than 3,000 voters casting votes through the various channels. A large percentage—23.9 percent and 28.1 percent of voters in the two respective wards—used the new internet option, while 17.6 percent and 27.7 percent respectively used the automated phone voting. In addition, tallying the results was much quicker than conventional methods. "St. Albans

ROB MATHESON/CORBIS

Using Oracle9iAS Release 2 and Oracle9i Database Release 1, the Oracle and British Telecom team was able to create a completely secure application to support all voting channels.



recorded the fastest-ever count, in less than six minutes, on the evening of May 2, 2002. It was actually a record for the U.K.," says Tonia Perry, an account manager with Oracle U.K. (Another fast vote count of a much different magnitude happened recently in Brazil. After 91 million people voted in October's presidential elections, the Brazilian Electoral Justice using an Oracle database was able to count 99 percent of the votes in just under 5 hours.)

While there was no increase in overall voter turnout in St. Albans, the pilot e-vote achieved success by simplifying the electoral processes, broadening the ways in which citizens could vote, and demonstrating that e-voting can be used for real elections.

SYSTEM AND SECURITY REQUIREMENTS

Developing a solution for St. Albans required the team to address a number of design issues that many companies face when creating mission-critical applications, including:

- **Security.** Understandably, security was one of the key design criteria for the system. Consideration had to be given to everything from complete system security down to the security of votes and how they were stored within the database.

- **Accountability.** The application had to be auditable and contain mechanisms for verifying the votes as they were cast and ensuring there was no tampering or changing once they were cast.
- **Flexibility.** The system had to support multiple channels of voting and provide completely isolated databases for each of two wards.
- **High availability and resilience.** Since there were no paper-based backup alternatives planned, the system had to work, and it had to be available during the multiday voting period.
- **Multilanguage support.** The St. Albans wards where e-voting was used have a high percentage of citizens who speak Bengali; the system was required to support both English and Bengali.

ORACLE'S ROLE

"Since this was a public election, we had very high requirements for security and reliability, which are two incredibly

strong characteristics of the Oracle9i Application Server," says Abel. Using Oracle9iAS Release 2 and Oracle9i Database Release 1, the Oracle and British Telecom team was able to create a completely secure application to support all voting channels. Their system included two application servers and two database servers, one acting as the active database server and the other in passive mode running Oracle Data Guard.

Since the team needed to create an application that could interact with multiple types of front ends (everything from telephony to kiosks) and support multiple languages, a Java-based application running on an application server was a perfect fit. Oracle9iAS, with its wide range of J2EE capabilities, integrated support for the Oracle database, and Web services support, was their choice. "Oracle9iAS Release 2 provided the security and reliability using new J2EE security and high-availability features that we needed," says Abel. "In addition, using OC4J [Oracle9iAS Containers for J2EE] meant the application was J2EE-compliant and generated non-vendor-specific code, keeping it in line with Oracle's commitment to open standards and portable code."

By building the application using Oracle9iAS, the team was able to take advantage of several built-in security and system capabilities, including:

- **J2EE support.** Oracle9iAS provides built-in support for J2EE 1.3 APIs, as well as Web services and XML. Since the e-voting application was written in Java, J2EE support was a critical feature. It had a JSP front-end/GUI that was connected to a servlet running under OC4J. The team used secure JDBC database connections so all the PL/SQL was wrapped and encrypted.
- **OC4J.** Providing complete support for Enterprise JavaBeans (EJB) 2.0, Servlets 2.3, JavaServer Pages (JSP) 1.2, JCA 1.0, and Java Authentication and Authorization Service (JAAS) 1.0, the team used OC4J in a variety of ways. For example, Java servlets managed the secure connections to voters and validated the VIN and PIN numbers.
- **SSL.** Secure Sockets Layer (SSL) provides an encrypted link between the Web servers and clients. Oracle9iAS's enhanced Apache-based Web server has SSL built in, along with single sign-on, PL/SQL, Perl, CGI, and more. The team used SSL to make sure that connections between voting locations, internet

// Oracle did a great job. The application did everything it needed to and nothing more. The application design looked very good."

—David Litchfield, security expert and cofounder of Next Generation Software

users, and the telephony systems were secure.

■ **Wallet manager.** The application made use of Oracle9iAS's wallet manager, which allows applications to access private keys and certificates stored in an Oracle wallet to protect the identities of clients or servers over SSL. "Starting with the release of Oracle9i Advanced Security, we now support industry-standard Public Key Certificate Standard [PKCS] #12 wallet formats [Oracle Wallet Manager] where certificate and private keys are stored," says Kristy Browder Edwards, principal product manager, Oracle Server Technologies. "You can now store those wallets in an LDAP directory, so if you're traveling you can log onto a machine wherever you are around the world, download your wallet with your personal credentials in it, and then use that to authenticate to an Oracle database and other applications." The St. Albans application used the wallet to store the certificate used for SSL, as well as reference the wallet file in the HTTP configuration file. "In Oracle9iAS, we do not use `open_ssl / mod_ssl` anymore, but instead it is replaced with `mod_oss1`, which looks up certificates in the wallet," says Abel.

■ **Auditing features.** "Not only is auditing important, but auditing in a multitier system is particularly difficult," says John Heimann, director, Oracle Security Product Management. "Suppose you have a system in which a user signs on to the application server and then causes the application server to retrieve or update some data within a database. If there is no mechanism for correlating events in the database with the application server, then it's difficult to know whether users are violating the security policy. There are mechanisms in Oracle9iAS and Oracle9i Database to support multitier auditing."

Oracle9i contains a rich auditing facility that enables businesses to audit database activity by statement, object, user, column, and a variety of other aspects. The St. Albans team constantly monitored the

opmn.log, OC4J log, and HTTP log files. The audit logs were monitored manually, since the data volumes were low. The application included authentication audits for the VIN and PIN validation, multitier audit logs for post-audit validation, Oracle internal audit validation of all Data Manipulation Language (DML) operations, and post clear-down audit tasks.

■ **Authentication.** Oracle9iAS includes the JAAS that provides additional functionality to authenticate users and enforce access control. However, since the St. Albans system was designed for a single election, the team decided to create and use a custom user manager to authenticate each user, instead of JAAS. The user manager was set up in the WEB.XML for secure URLs (i.e., voting), so if someone tried to jump directly to the secure page (i.e., tried to vote), the controller servlet would check the cookie and allow access only if the cookie was set with a correct session ID.

■ **Encryption.** The team extended the security encryption capabilities of the application server to use random number generators to generate session keys for each piece of traffic sent across the network. Encryption was also used to generate the PINs and VINs and keep the votes safe. When the application servers were installed, the team generated the encryption/decryption code and installed encryption software in the database as "wrapped" code (obfuscated). Once the PINs and VINs were generated, the decryption software was removed from the machine, stored in a safe location, and reinstalled only when the votes needed to be tallied at the end of the election.

Selective encryption of especially sensitive stored data, such as credit card numbers and salary information, can protect such information from attacks outside the database, says Ken Jacobs, author of *Oracle Magazine's* Dr. DBA column. "Highly granular server-enforced access control is really becoming critical for hosted applications for e-commerce, where millions of users access the system

David Litchfield's recommendations for making your system and applications secure:

- Look at what handlers (such as Perl and CGI) are enabled, and make sure to remove any that aren't needed. Make sure to check all the configuration files.
- Make sure both database and application servers have the latest system patches.
- Examine the code closely anywhere that user input is required.
- Verify the permissions on files, and make sure that users can run only the queries they need to and nothing more.
- Make sure to harden each server individually. If hackers get control of the application server, they'll have access to the database server only if you've let them in by not hardening it enough.
- Where possible, set any permission for database connections as low as possible. For example, make sure users can't insert or update but can only select tables.
- Remove any unused database logins.
- Eliminate obvious passwords.
- Keep the application as simple as possible.

or several companies share a single physical database.”

In addition, some Oracle9i Database capabilities proved critical to maintaining the security of the application and record of votes. For example, the team used the virtual private database (VPD) option to create individual databases for each local authority. This enabled them to have a single physical database for easier manageability and backup, with virtually partitioned databases accessible only to the local authorities.

HACKING INTO THE ELECTION SYSTEM

Once the architecture was set up, it was run through numerous in-house and outside audits, starting with an architectural audit that served as the foundation for the overall security policy. This was followed by penetration testing by NGSSoftware, headed by internationally known security experts the Litchfield brothers.

“Being unbreakable was the single most important criterion in this project,” says Perry.

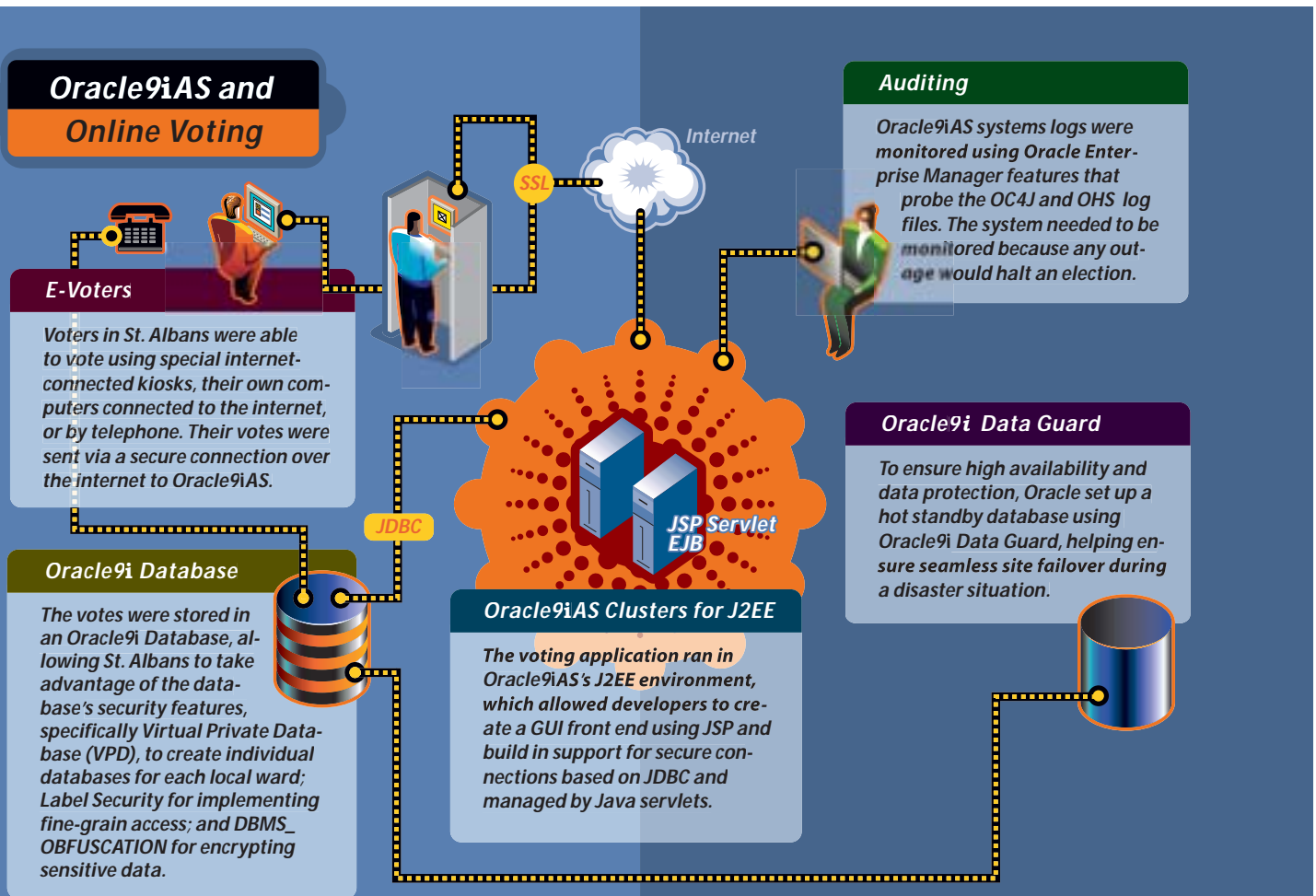
“From the government perspective, if we had been hacked in May and any of the results corrupted, destroyed, or tampered with in any manner, it would have completely stopped any further e-voting activities, because it would have undermined public confidence.”

The Litchfield team of four “white hat hackers” was brought in to do both black-box and white-box penetration tests.

A black-box penetration test is essentially a “hacker’s-eye view” of an application or system. Given no more information about an application or system architecture than the IP address, the Litchfield team attempted to break into the St. Albans e-voting system. The Litchfields did find some issues with the application server, which the e-voting development team quickly resolved. “The Oracle response was great. They had a working patch in a couple of hours,” says David Litchfield. “Once we applied it, we couldn’t do anything—absolutely nothing—to the system.”

The team also found minor issues with the Perl handler and CGI handler. Removing the Perl and CGI handlers and patching the previous bug removed the application server vulnerabilities.

Next they turned their attention to the “white box” tests, where they were provided information on the application, source code, network diagrams, and access to the application to explore and identify any additional vulnerabilities. During the white-box tests, they found a number of small issues such as incorrect permission settings and a host computer (a Sun Solaris running the Oracle database) that had been left unhardened. They went on to look for coding problems in the JSP. “One of the things to check during a white-box test is to look at any place in the code where there’s opportunity for user input or the places where you can run commands,” says Litchfield. “Those will basically define what can be done by an attacker.” For





During the live voting period, there were no system outages or issues and no successful penetrations or hacks.

Identifying Users at Work

In addition to helping municipalities and organizations develop user identification processes (and providing the technology to make those processes work), Oracle has a long history of providing identity-management technology for use inside companies.

Identity management is the process for securely managing the complete lifecycle for network and user entities in an organization. It most commonly refers to the management of an organization's application users, where steps in the security lifecycle include account creation, suspension, privilege modification, and account deletion. The network entities managed may also include devices, processes, applications, Web services, or anything else that needs to interact in a networked environment.

The next release of Oracle's application server, Oracle9iAS Release 2 version 9.0.4, will contain enhanced features for managing users. Called Oracle Identity Management, this functionality is an aggregation of directory, security, and user management tools that Oracle products rely on for distributed security. Oracle9iAS is the primary vehicle for Oracle Identity Management, however these features will also ship as part of the infrastructure with other Oracle products including the Oracle9i Database and Oracle9i Collaboration Suite. Oracle Identity Management includes:

- Oracle Internet Directory (OID): A scalable, robust LDAP V3-compliant directory service implemented on the Oracle9i Database.
- Oracle Directory Integration Service: Part of OID, which permits synchronization between OID and other directories and user repositories.
- Provisioning Integration Service: Part of OID, which provides automatic provisioning services for Oracle components and applications and, through standard interfaces, third-party applications.
- Delegated Administration Service: Part of OID, which provides trusted proxy-based administration of directory information by users and application administrators.
- Oracle9iAS Single Sign-on: Provides single sign-on access to Oracle and third-party Web applications.
- Oracle Certificate Authority: Generates and publishes X.509 V3 PKI certificates to support strong authentication methods.

example, in programs written in C, you would look for potential memory problems or buffer overflow conditions. In the case of St. Albans, the hackers did not find any coding bugs or vulnerabilities, and nothing needed to be changed.

"Oracle did a great job," says Litchfield. "The application did everything it needed to and nothing more. The application design looked very good."

The penetration team also tried a number of attacks against the application and application logic—everything from trying to vote twice to making sure that once a person voted, his or her vote could not be changed. For example, the votes were encrypted with a one-time password specific to the user, which essentially acted like a checksum so that it would be immediately identifiable if anyone changed it. They also checked to make sure that the returning officer couldn't intervene and compromise individual votes or the election count.

In the end, all the investigation and attempted penetrations paid off. During the live voting period, there were no system outages or issues and no successful penetrations or hacks, although the St. Albans team recorded about 200 worms that attempted to get in over the five days the system was online. Overall, the system was a success.

THE FUTURE

The British government is now looking to build on the e-voting pilots that were run for the May 2002 elections by encouraging district and local governments all across the U.K. to run e-voting tests. These activities will probably include both e-voting and e-participation events (such as running referenda). If things go well, it could mean that such systems would be used for national elections later in this decade. ■

David A. Kelly is a business, technology, and travel writer who lives in West Newton, Massachusetts.

nextSTEPS

LEARN about Oracle9iAS security features

OTN's Security Technology Center offers security information about Oracle products
otn.oracle.com/deploy/security/oracle9ias

ATTEND a class on Oracle9i Application Server

Oracle University offers many Oracle9iAS Security courses
oracle.com/education/course_listings/database/index.html?oracle_oracle9ias_security.html