CGA DIRT

Damage Information Reporting Tool
Database Security Whitepaper

DIRT Development Team

For CGA Data Committee

Revision	Comments	Date	Author
1.0	Created document	05/01/2004	DJH
1.1	Updated network diagram	05/13/2004	DJH/RTG
1.2	Final edits/photos	05/13/2004	DJH/RTG/JDM

Table of Contents

INTRODUCTION 3
PROJECT STATUS 3
REFERENCES AND REFERENCE DOCUMENTS 3
PROJECT OVERVIEW 3
DESCRIPTION 3
SECURITY ASPECTS 5
GENERAL SECURITY 5
POLICY 6
PHYSICAL SECURITY 6
NETWORK SECURITY 6
PLATFORM SECURITY 7
APPLICATION SECURITY 8
DATABASE SECURITY 9
CRYPTOGRAPHY 9
CONCLUSION 10

Introduction

Project Status

Phase: Production Pilot	**Category:** Data collection and reporting tool
Product Name: CGA Damage Information Reporting Tool (DIRT)	**Development Sponsorship:** Common Ground Alliance Data Reporting Committee
Document Contributors: D. J. Hagberg, DIRT Developer Rudy Gonzales, DIRT Developer J. D. Maniscalco, UNCC Executive Director	

References and Reference Documents

Reference Doc/sites	Version	Location
Defense in Depth	n/a	NSA Website http://www.nsa.gov/snac/
Oracle Technical Library	n/a	Oracle Website http://otn.oracle.com/
SANS Institute policy recommendataions	n/a	SANS Website http://www.sans.org/

Project Overview

Description

The goal of the Common Ground Alliance (CGA) Damage Information Reporting Tool (DIRT) is to provide a North America-wide collection point for the reporting of underground damages. The tool is designed for use by both small and large companies to enter one or many damage reports in a secure fashion with the following goals:

- Web-based access to the application from any modern OS and web browser.
- Secure, verified registration of new users.
- Submission of single damage reports through a simple, intuitive web form.
- Submission of multiple damage reports through a file upload process that can scale to support thousands of records at a time.
- Limited access and time window for editing of submitted damage reports.
- Detailed reporting capabilities for submitting companies for their own data.
- Summary reporting capabilities across all data.
- User and Company management

The DIRT tool itself is run and hosted in a secure data center at the Utility Notification Center of Colorado (UNCC), Golden, Colorado on secured servers in a multi-tiered secured network. This document provides a high-level overview of the security aspects of the DIRT application and its hosted environment.

UNCC Data Center Network & Server Racks

UNCC Firewall, Network, and Voice Services

Security Aspects

Based on general security frameworks from the US National Security Agency (NSA) and SANS (SysAdmin, Audit, Network, Security) Institute, the security of the Damage Information Reporting Tool environment, application, and data will be discussed according to several aspects:

General Security: the basic approach to security followed during application development, testing, and production.

Policy: the "people" part of the security equation, setting rules around process, permissions, etc. to be followed by administrators and users.

Physical Security: controlling access to systems where the application and data reside. Network Security: design and implementation of the secured, tiered network, and access controls.

Network Security: the network architecture, firewalls, subnets, and rules for data flow restrict remote access to the servers and possible flow between application tiers.

Platform Security: the security of the host(s) and platform where the application runs, including OS, application language, and application server environment.

Application Security: policies within the application itself to enforce roles, privileges, and actions.

Database Security: restrictions and controls implemented at the database level, including permissions, backup & archiving, and auditing strategies.

Cryptography: when and where encryption technologies are used in relation to the DIRT application and its environment.

General Security

The DIRT development and implementation team has maintained a focus around data and environmental security as a major component of the application. The general approach has been one of "defense in depth" as advocated by security standards from the NSA, the SANS Institute, and the Internet Engineering Task Force as well as vendor guidelines from Oracle and RedHat.

Each of the aspects discussed below is not, in itself, enough to protect the application and data from compromise. But all combined together form a fortress strong enough to defend against all but the most determined attacker.

Policy

The general people-oriented policies around the DIRT application involve restrictions and agreements, including contractual agreements, around access to the environment, systems, application, and data for DIRT.

The DIRT application, environment, and data are hosted for CGA by UNCC with agreements in place on usage, access, and responsibilities. UNCC is obligated and committed to allowing only authorized personnel access to the physical location and systems where the DIRT application and data are hosted.

Only a restricted number of people have low-level access to the DIRT data and then, only for purposes of backup for data- and disaster recovery, fault analysis, and development of new features. This includes the DIRT development team at this time.

No other access to the systems and data are allowed except through the DIRT application itself.

Physical Security

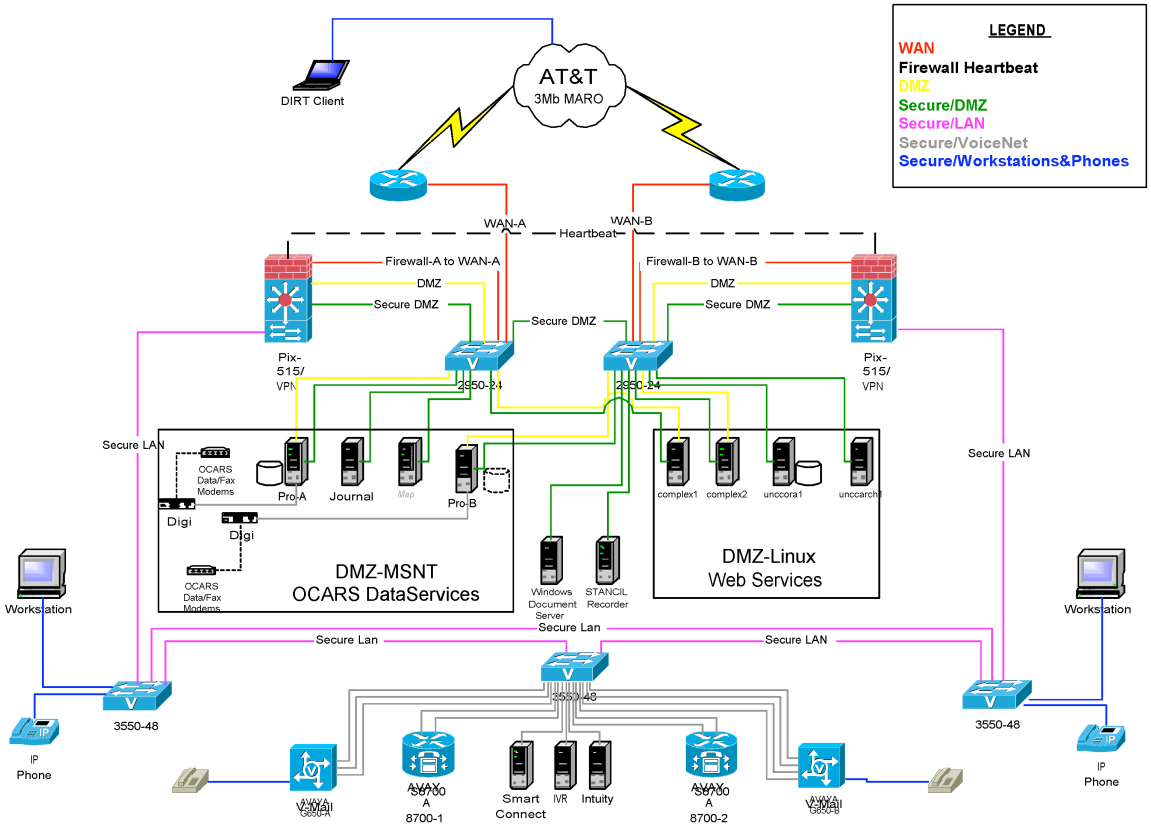
UNCC's data center in Golden Colorado resides in a secured facility with limited access to operational areas for staff members and their accompanied guests only. The data center where the DIRT application is hosted is protected by restricted, logged electronic card key access.

Only a limited number of network operations staff and the DIRT development team are allowed access to this area. Other parties such as equipment vendors are only allowed in the data center if monitored by the operations staff.

Off hours, the building is protected by an individually-keyed alarm system. This system monitors all potential building access points and notifies Golden police in the event of motion inside the facility or unexpected entry.

Network Security

Following best practices for network design, the UNCC data center network is based on SANS, CISCO, and NSA recommendations with a multi-layered network design that provides a high-level of security. This ensures that all connectivity to and from the Internet is restricted, logged, and separated from backend services of the UNCC call center and administrative LANs. Users and owners of the DIRT data collection and reporting tool are advised that there are individuals in the world's computing environment who seek to invade or "hack" into secure computer systems as a hobby, for profit, or who are seeking to inflict damage on computer systems for malicious reasons. Specialists who maintain the DIRT System have designed a system which can resist most all attacks by hackers; however, there is no guarantee that highly skilled and determined hackers will not access the DIRT System. In the event of a security breach, the system will be shut down and users will be notified immediately, followed by a detailed investigation into any data or application issues.



As you can see from the above diagram, the first defense against penetration from the Internet are the redundant Cisco PIX firewalls. Next, the hardened internet-facing servers: complex1.uncc.org and complex2.uncc.org provide the email, web, and application server portions of the DIRT application.

The “Secure LAN” segment is a separate physical network with its own firewall protection. The Oracle database server, unccora1 is connected here, separate from both the Internet-facing servers and the rest of the UNCC LAN. In addition, the backup server is connected in this same secured area, ensuring that backups are protected by the same rules as the database itself. Network access to the Oracle server is restricted to only authorized and authenticated connections from the DIRT application running on complex1 and complex2.

UNCC’s LAN for the call center, administrative personnel, and normal operations data exists behind yet another layer of firewall protection with restricted access to and from the Internet. None of the LAN hosts are permitted access to the Oracle database server or backup/archive server at this time. UNCC’s voice over IP (VOIP) network is the final network segment, where only voice traffic is allowed and is not permitted to connect to the Secure LAN or Internet-facing portions of the network, via firewall rules.

Platform Security

RedHat Enterprise Server 3.0 is the operating system for the servers where DIRT is deployed. This is a commercially-supported distribution of the Linux operating system,

designed and maintained for the purposes of enterprise deployments. The specific installation for UNCC's Internet-facing servers is a highly restricted set of components, following the SANS-recommended principle of minimal installation. All un-needed services are disabled at installation time, before the systems are even attached to the network.

UNCC's policy is to apply all security-related patches before the next business day after release from RedHat. For major maintenance updates that are not security-related, patches are applied every two months.

The servers themselves are set up with restricted logins that only occur through an encrypted Secure Shell (SSH) session. This ensures that at no time do passwords get transmitted over the network in a form that can be seen or decoded by an attacker. All file transfers and remote administrative functions occur over this connection.

The DIRT application was written in the Java programming language using the Java 2 Enterprise Edition (J2EE) framework. Both Java and J2EE have their own security aspects, namely the bytecode security verification of the Java runtime and the deep security mechanisms of the J2EE framework. The Java language and runtime system have features that prevent the most common security exploits – buffer overflows.

The J2EE security framework provides systems for both authentication of users and authorization of actions they may perform. A similar system is used to restrict actions that code running in the Java runtime may perform on the underlying system. More information is available on the subject at http://java.sun.com/security/.
UNCC uses Sun's implementation of the Java runtime environment, the Tomcat J2EE application server container, and the Apache webserver to provide the base infrastructure. All these packages are monitored on a weekly basis for security-related issues and fixes are applied before the next business day after release.

The Apache webserver uses the OpenSSL package to provide secure, encrypted, and certified web access. OpenSSL provides the encryption libraries necessary for client browsers to connect using the secure http (HTTPS) protocol. The www.damagereporting.org webserver itself has been certified by a trusted authority: Thawte, a division of Verisign. This certification is renewed on a yearly basis.

Application Security

DIRT application security is comprised of several major components: secure registration, a Role-Based Access Control (RBAC) system, and company-based data "firewalling".

The secure registration process ensures that only authorized users are allowed to register for a given company. For all new users, their identity and relationship to their company are verified by a CGA Administrator. This helps to ensure valid data submission and verification against CGA's membership list. During registration, the user password is collected and immediately encrypted using a one-way hash function. This ensures that even CGA administrators and DIRT developers cannot view or decode

user passwords. Also at this time, security questions are collected that may be used to verify the user's identity.

The DIRT Role Based Access Control system ensures that users are only permitted to perform a restricted set of operations in the system, depending on their role. A "Contributor" is only allowed to log into the system, submit damage reports and view their own reports. A "Manager" has those privileges along with the ability to and modify other contributor's damage reports for their parent company. A "Company Administrator" has the 2 prior role's privileges along with the ability to approve new contributors or managers for their company. Finally, a CGA Administrator is allowed to approve new Companies and Company Administrators, as well as report across all damage reports in the system.

Throughout the application, the basic principle is that only CGA Administrators are permitted to look across companies. If a user logs in as a Company Administrator or lower, they will only see users, damage reports, file uploads, etc. for their own company and no other.

All actions performed by a user logged in to the application are logged, with periodic log inspections and archiving. This ensures a reasonably complete audit trail of the systems and is also helpful to the DIRT development team in diagnosing unexpected behaviors of the application.

In summary, the DIRT System does allow authorized users to register and use the DIRT System according to "privileges" granted by a company or CGA member using the system. It is the responsibility of all user companies or CGA members and their Administrations to ensure that only authorized users have access to the DIRT System. Maintaining the highest levels of security requires that all Companies are diligent in supervising their authorized users.

Database Security

The back-end Oracle database that the DIRT application relies upon is run in a secured portion of the network, as documented above. Similar to the operating system hardening techniques discussed in the Platform Security section, only minimal Oracle services are enabled in this installation.

Oracle roles and permissions are used to restrict access to only the data relevant for the DIRT application to run. Standard Role and Grant mechanisms are used following Oracle best practices for security.

Oracle export files are used as the archival mechanism, preserved locally on the server for rapid recovery if needed. For archival purposes, the export files are transferred to a secure "backup" server and, periodically, to tape for secure off-site storage.

Cryptography

For the web- and Internet-facing portions of the application, the SSL v.3 and TLS v.1 protocols are supported, but only with HIGH-grade encryption (128-bit or better). For

secure shell administrative access to the hosts, version 2 of the SSH protocol is used with only 128-bit or better ciphers allowed.

For the user passwords stored in the database, a SHA-1 NIST-standard hash function is used, along with a 32-bit “salt” to ensure that even if two users choose the same password, it will not show the same hashed value in the database.

Conclusion

This document has provided an overview of the security aspects of the DIRT application. If you have any questions about the details in this document, please contact the CGA Data Reporting Committee “tech team” which includes the developers, co-chairs, and other interested parties at: cga_dr_tech@uncc.org.