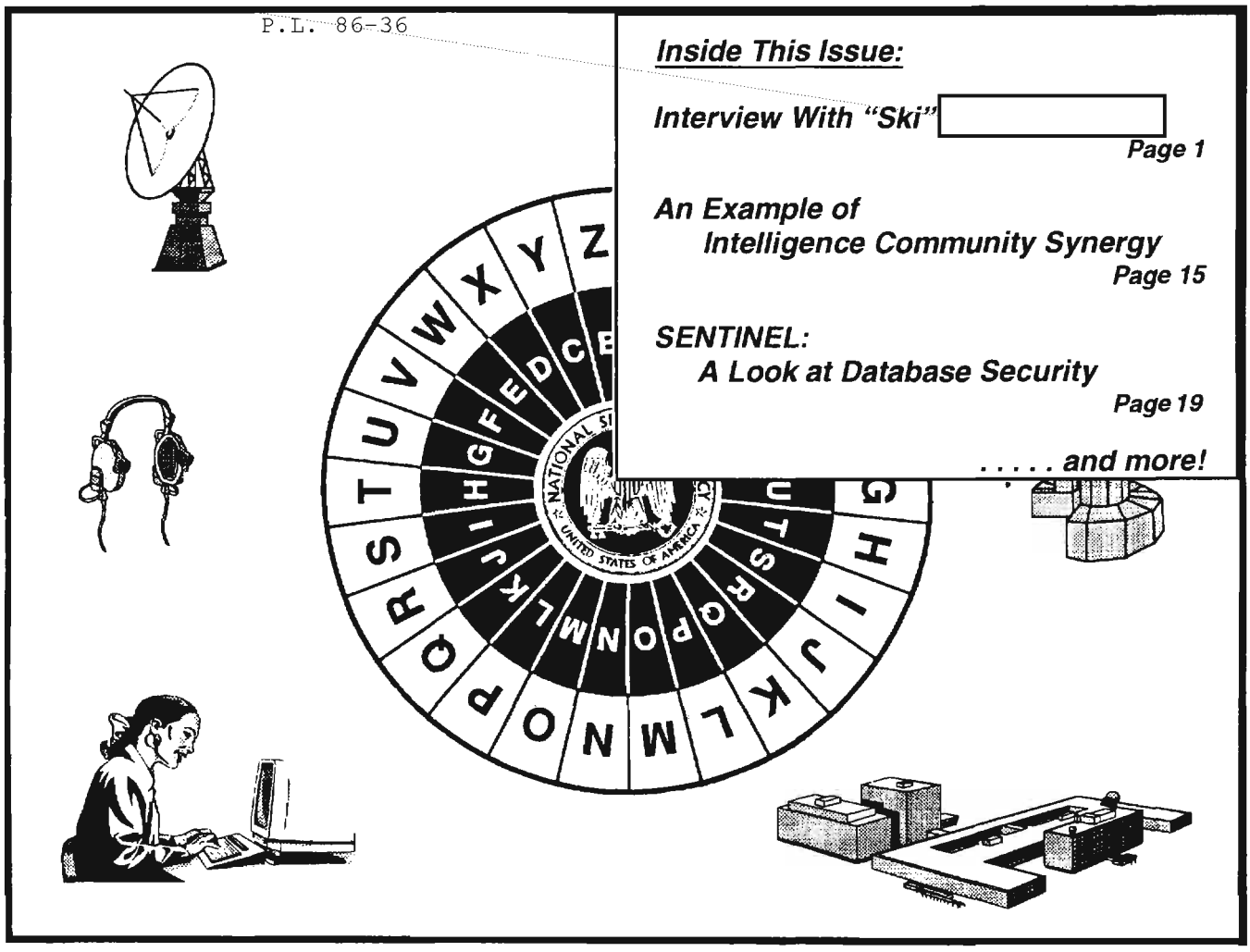
NATIONAL SECURITY AGENCY

CRYPTOLOG

The Journal of Technical Health

Vol. XXIII, No. 2 SUMMER 1997



Inside This Issue:

CRYPTOLOG

Summer 1997
Vol. XXIII, No. 2

Published by P02, Operations Directorate Intelligence Staff

To submit articles and letters, please see last page.

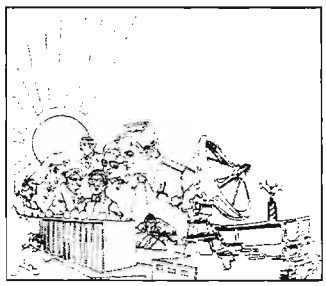


Table of Contents

P.L. 86-36

EO 1.4.(c)
P.L. 86-36

SENTINEL: A Look at Database Security ~~(FOUO)~~

by [redacted]

P.L. 86-36

(U) The need to store data classified at many different levels in one database prompted the creation of the SENTINEL database security filter. Managers, analysts and collectors at NSA need to make decisions based on data from many different sources and classification levels. With shrinking budgets and personnel cuts, individuals are expected to manage more information and make broader decisions than in the past.

Approaches to security (U)

(U) The most secure solution to the database security issue is to start at the ground level. Acquire a secure operating system, such as Trusted Solaris, as the foundation. Next place a secure relational database management system on top of this to form a completely secure system. Unfortunately, this solution is more expensive, harder to use, and more difficult to administer than a traditional operating system and database management system. In addition to cost and usability, this solution requires you to supply all the users of your system with the same configuration, which incurs further cost.

(U) Another solution, and the one taken by SENTINEL, is to take a traditional operating system such as SunOS, Solaris, or AIX and use a traditional database management system such as SYBASE. This solution is not as secure as the one mentioned above but fits into the existing computer architecture, which does not include trusted operating systems and database management systems. SENTINEL was created to prevent accidental data disclosure but not a malicious attack.

What is SENTINEL? (U)

(U) SENTINEL is a security filter for SYBASE databases which provides multi-level security down to the row level. SYBASE alone provides security at the table level, but this is not good enough for SENTINEL's users, who demand finer granularity down to the row level. For those not familiar with relational database management systems, the composition of today's relational database management systems consist of application databases at the top. Databases are composed of tables and tables are composed of rows. SENTINEL insures a user will only see the rows of data for which he/she is cleared to access.

(U) The SENTINEL security filter is an integral part of project PLUS. PLUS has 1600 users worldwide located at the CSGs, RSOCs, field sites, other Key Components and DO. PLUS gives users feedback about SIGINT production as a whole and where they fit into the SIGINT production system. SENTINEL is used in [redacted] and a Second Party project called [redacted].

(U) SENTINEL has been certified by J06 at the C2 level for in-house use. The C2 criteria can be found in the Orange Book. For the full criteria, go to **http://nectarine.q.nsa/REGS/rainbow/**

orange on the NSA network. For those not familiar with the Orange Book criteria, D is the lowest or least secure level and A is the highest or most secure level with C and B in between.

How it works (U)

(U) SENTINEL is a SYBASE Open Server application program that runs between the user application, or client, and the backend SYBASE server program. It acts like a watchdog in front of the user's application database preventing unauthorized access to data. SENTINEL intercepts each Structured Query Language (SQL) request sent to the SYBASE server, modifies the request by adding the appropriate security information and forwards the modified request to the SYBASE server for processing. Once SYBASE receives this modified SQL request, it processes the request and sends the results back through SENTINEL, in pass through mode, to the user process. Pass through mode means the data is unaltered.

(U) The SENTINEL database is used to store all the pertinent security information about users, what databases they have access to and the clearance level of the databases. Storing the user classification in a separate location from the data classification is a characteristic of secure systems. Again, consult the Orange Book for more information. The SENTINEL database can be updated manually or automatically. An example of the automatic mode can be found in Project PLUS which has written a program to query the SPECLR clearance database nightly and transfer that information to the SENTINEL database. In this mode, SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next.

(U) SENTINEL will have current security information about its users. It will know, for instance, if a user has lost the TK clearance from one day to the next

(U) SENTINEL expects a security label to be attached to every row in a database and to every database user. This label contains three components: a hierarchical component for storing clearance information such as Top Secret, Confidential, etc.; a privacy component which restricts releasability privileges; and a compartment component which stores need to know items such as TK, VRK, BYEMAN, etc. The clearance component can store 16 different combinations of mnemonics. The privacy component supports a maximum of 32 privacy labels. The compartment component supports a maximum of 1024 compartments. These components are stored as bit mapped fields where each bit or pattern of bits corresponds to a mnemonic such as TK, VRK, SECRET etc. The decision to store this information as bits was developed in the interest of space and speed. Since a bit, which can either be a 1 or a 0, is the smallest unit in a computer, it does not take up much space. Manipulation of bits in a computer is also very fast.

(U) At the heart of SENTINEL is the SQL parser. It breaks SQL statements down into separate components which are then passed to the processing module of SENTINEL. This processing module inserts limiting information, derived from the SENTINEL database, about the user into the user's SQL and then forwards the modified SQL on to the SYBASE server for processing. For instance, a user query might say something like, "I want to see all rows in the employee table." SENTINEL modifies that query to say "I want to see all rows in the employee table that are at my clearance level," or, more specifically, "I want to see all rows in the employee table that are Top Secret or below, TK and VRK." The information used to modify the query comes from the SENTINEL database.

(U) In addition to the row level security provided by SENTINEL, other security features are in place. The first restriction SENTINEL imposes is no user accounts on the backend SYBASE server. We don't want an ordinary user to bypass SENTINEL by logging on to the backend database to access information. Users log in to SENTINEL using their unsecured Agency SID and password. SENTINEL uses this account to retrieve the sid and password of the user's secured account. Using this information, a secured connection is established, the unsecured connection is terminated and

the password to the secured account is changed. This level of security differentiates between a user's access to a database in secured mode versus access to a database in an unsecured mode. Access to secured databases is granted to a user through the secured sid. Attempts to use a secured database under an unsecured SID will be prevented by the SYBASE server's database level access control mechanism.

(U) One of the main reasons SENTINEL only works with the SYBASE relational database management system is that it is the only widespread database management system at the Agency that supports bit manipulation. There are other products on the market that perform database security such as ORACLE's Row Level Security product, but this requires developers to purchase ORACLE whereas SYBASE is essentially "free" since NSA has a site license for SYBASE.

SENTINEL Operation (U)

(U) SENTINEL runs in the background, which means there is nothing to see. It has no user interface, so you will never see a SENTINEL icon on your computer screen. SENTINEL operates in two modes. In the first mode, developers can include SENTINEL library "C" language modules in their "C" programs to create their own custom applications that are secure. This is what project PLUS has done. The last method to access SENTINEL is through the use of stored procedures. Stored procedures are collections of SQL statements used to perform a task or set of tasks designated by the user. These stored procedure calls can be sent to SENTINEL through a "C" language program or an ISQL session. An ISQL session allows its user to type and send SQL without having to know a programming language such as "C". This last mode provides the greatest flexibility because it allows a user to send any allowable SQL and receive results instantly while still being assured they will receive only the data for which they are cleared. In addition to the standard SYBASE stored procedures, the SENTINEL developers have added many security specific stored procedures. These stored procedures allow the user to set and retrieve their clearance, privacy and compartment levels within allowable bounds. A user is allowed to downgrade their clearance level to give a demo, for instance, but is never allowed to raise their clearance level beyond that which is set by the SENTINEL administrator.

Conclusion (U)

P.L. 86-36

(U) The long-range goal of database security is to have a product that can access many different types of databases, not just SYBASE. This product would not greatly hinder the performance of database retrievals and updates. It would also require minimal updates to the user's application to take advantage of the security aspects. Until such an application is found, SENTINEL is here to fulfil the database security requirement.

~~(FOUO)~~ Mr. [redacted] started his Agency career twelve years ago as a computer analyst in the R directorate. Since then, he has worked in a variety of areas from contracting officer's representative (COR) to software development and system support. He currently works in E223 as the SENTINEL project leader. When the weather is nice, Mr. [redacted] can be found riding his bicycle. He would like to thank [redacted] and [redacted] for their enhancements to this article.

Kλ

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu