Sirius – Built to resist attack

How Sirius is built makes it highly resistant to hacking attacks. Sirius is regularly penetration tested to ensure security by “ethical hackers”. What are these attacks and how does Sirius defend against them?

Brute force password attack

This is where a hacker simply tries millions of usernames and passwords. This is how **iCloud** was compromised and images of celebrities stolen. Sirius defends against this by locking out any account that has a small number of failed login attempts in a row.

Stolen Database

Let’s say a hacker succeeds in stealing a Sirius database with user credentials in it. Could they use the information to get into the online system?

Sirius defends against this by avoiding storing passwords at all. Sirius stores a cryptographic hash of the password. This hash is *salted* to prevent the use of *rainbow tables*. A rainbow table is a huge database of precomputed hashes for millions of passwords that a hacker can simply look up to determine what the password is. By adding a random string of characters (the *salt*) to the beginning of the password and then calculating the hash, the size of the rainbow table necessary is rendered too enormous to be of practical value.

Key Logging or Network Traffic Interception (Man in the Middle)

This is where a hacker installs software on a user’s PC to record keystrokes or views the data transmitted between the user’s browser the online server by monitoring the traffic. In both cases the hacker can look through the recorded text to find a regularly repeated string of characters. This could be a username and the current password. Sirius uses the concept of a **Memorable Word**. The user is asked for two or three characters from the Memorable Word. The whole word is never typed in. This makes determining the Memorable Word much more difficult.

SQL Injection

This is being reported as the attack used to steal information from **TalkTalk**. This consists of a hacker manipulating the user interface to add their own database queries to the ones being legitimately used by the application.

Sirius defends against SQL Injection attacks in a number of ways:

- Avoids dynamic SQL strings so there’s never any possibility of a database query being amended.
- Sirius exclusively uses Stored Procedures to query the database

- User inputs are scanned for SQL scripting commands

- Lowest possible access privileges for the Windows Domain account that queries the SQL database. The user account only has rights to execute the Stored Procedures it needs – access to other database structures are disallowed.

The above denies attackers the ability to steal data online even if they have managed to obtain user credentials.

URL Manipulation

This is where a hacker who has legitimate credentials to log on to the system changes parameter values in the browser's URL string in an attempt to access information not properly available to them. Sirius defends against this through *user session validation*. When a user logs on a **Session** is established unique to them and the instance of them logging on. Each time the user requests information the user's Session is checked for validity and their application rights determined. In this way Sirius based applications can ensure only data a user has rights to is displayed to them.