Encrypted Systems for Database Security

Anonymous

Xtern Work Sample Assessment

Security

October 19

2021

Encrypted Systems for Database Security

Data Privacy

A crucial consideration when accounting for encrypted database records is the comparability of information. If an encrypted record were a string of individually encrypted field values, it would be possible to compare encrypted values within some field i, and determine all records with identical values in that field. If the deciphered value were known for some record (say the record about the attacker), then all other records with similar encrypted values could be compromised. (Davida, George I, et al.)

Publicly visible information within a database fails to benefit from encryption systems, as repeated encryption/decryption even with bearer token authentication results in unnecessary compute and cost additional compute time. Therefore, fields such as the Username can be stored in plaintext effectively.

On the other front; password security for example is a well-researched domain with little room for further improvement. To that effect, I propose the use of salting with SHA-256 to encrypt passwords - mitigating rainbow tables and ensuring minimal informational compromise in the event the relevant database is breached. Information such as Phone Numbers, Billing and Email Addresses could use a novel implementation of Homomorphic Encryption. Research papers such as Faster CryptoNets discuss extensively the use of said homomorphic encryption. It allows for systems to run compute on data while maintaining it's state of encryption. This can allow for a single pipeline system wherein any attackers breaking the database cannot access decrypted information. Encryption systems for the same can be extensively hardened, beyond what is computationally reasonable due to the fact that if operations can be performed on encrypted data directly, it need not ever utilize decryption.

Finally, private user information unrelated to user confirmation can be encrypted and stored locally, further leveraging custom-implement hardware such as the Titan Security Chip on Google Pixel devices.

Implementing & Assessing Application Security

The OWASP Top 10 Vulnerability List presents an extensive report of vulnerabilities prevalent in systems today. Several of these vulnerabilities and common oversights continue to apply to native systems.

Logging is a useful tool crucial to providing insight during development. However, insecure logging (where logs carry forward onto production) represent a crucial source of additional information that can expose protocols and functions used through the runtime of the application which could lead to the carried compromise of the system.

Retaining past CVEs also result in a vast array of compromises to the target systems. Due to the extensive nature with which CVEs are reported, it is often trivial to replicate and exploit systems based on pre-provisioned CVEs. Therefore, keeping dependencies and source packages updated, alongside ensuring the presence of updated security patches does well to cut down on potential vulnerabilities within the system.

Effective methods of determining system security, alongside top-down approaches also include public bug bounty hunts and red-team/blue-team pentesting challenges within the corporate staff.

Monitoring Application Operational Security

Systems incorporating tools for networking are a common target of realtime attacks. For the hypothetical application, the amount of communication between servers has a direct impact between the amount of damage such an attack can do. While presumably, communications between said systems are expected to be relatively lower in this example, it is entirely possible to result in some loss of capital using script-kiddie techniques by any misguided cracker.

Here, monitoring tools provide extensive sets of information to both identify, prevent and analyse effectively attacks to the target system. Presented below is an informative table depicting crucial tools and their impact on operational security, in addition to the native solutions provided by the relevant cloud provider:

Tool	Applications
Security Onion NIDS Dashboard	Network Intrusion Detection alerts
Arkime	Examining Network Traffic, Looking at emails, Extracting Pcaps
Security Onion Sysmon Dashboard	Windows File creation/modification , Windows Registry Key creation/modification, Windows Network communication events, Windows Process creation/injection
Autopsy, Velociraptor	Disk analysis, Search Filesystems, Examine files, Recover deleted files
Kolide	Live host interogation
Volatility	Examining process/DLL information, Examining active network, connections, Extracting in memory malware