

# White Paper on Stealth Software Technologies



For further information, contact:

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

-Proprietary-

One of the important challenges in searching data is that users frequently want to hide search queries. User queries provide an indication of topics most users would prefer to keep private, including personal interests, hobbies, professions, research topics, opinions, and plans of action. (Note the furor generated by the recent *New York Times* articles on the publication of even a part of the AOL query log.) The problem becomes even more stark if a government user with security clearance wishes to search unclassified (or lower classification) machines, databases, or the internet. In this case, the requirement to hide the query may be legal in nature, and in the worst case scenario, revealing such a query might jeopardize national security. Thus, the need arises for the ability to execute searches without revealing the query even to machines that execute those searches.

Stealth Software Technologies, Inc. (Stealth Software) has developed novel software encryption capability for a wide range of applications that primarily target the intelligence community, law enforcement, and Department of Homeland Security (DHS), with secondary markets for the Department of Defense (DoD), the State Department, and commercial applications. Stealth Software allows one party to access and query others' databases without revealing the specific question being searched for, while at the same time protecting the searched databases from improper transfer of data out of their databases. This unique combination of capabilities is important for many applications in intelligence and law enforcement, as well as for multi-agency and coalition operations.

- For the intelligence community, Stealth Software allows users to execute classified queries on unclassified (or with a lower classification) machines without having to upload all data into a classified setting. Stealth's solution offers cost-effectiveness, efficiency, and timeliness, and provides a revolutionary capability for the intelligence community to collect data without revealing sources and methods (or anything else) about the nature of the classified query.
- If adopted by the intelligence community, the solution offered by Stealth Software would have profound effects on the ability of homeland security analysis and operations. Analysts tend to stay on the network where most of their work is conducted. Intelligence analysts typically stay on the Top Secret network. However, because of the unique and complex nature of homeland security, intelligence analysts need to be able to pull information from all levels of classification because the "tactical" information from state and local levels is typically unclassified. Currently analysts typically toggle back and forth from network to network through a switchbox. The novel solution offered by Stealth Software would allow the analysts to stay at the Top Secret network and pull information from lower classification networks without revealing the nature of the Top Secret queries to the lower classification networks. Thus, it would really increase the productivity and quality of homeland security analysts.
- A key issue for multi-agency and coalition operations is how and when to share data.

# White Paper on Stealth Software Technologies



For further information, contact:

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

*-Proprietary-*

The ability to identify the existence of key data that needs sharing, while still protecting the data owners' processes, sources and methods for release of the data, is a critically important capability for multi-agency and multi-nation operations.

Stealth's software enables classified IT network users to securely search any unclassified databases (or databases with lower classification level) without revealing the terms or results of the search to anyone other than the individual writing the query. Through the use of Stealth's Smart Public Key Encryption, search terms and results remain encrypted in an unbreakably secure fashion. Stealth software technology has numerous valuable applications centered on significantly improved information gathering and sharing among intelligence agencies. Stealth's solution can be used for:

- Improved collecting and processing of unclassified (or lower classification) data without having to upload all the unclassified data that needs to be searched into classified environment;
- For multi-agency and multi-coalition operations, checking coalition databases for individuals or events without disclosing their names to coalition members, while simultaneously controlling the amount of information shared;
- Providing real-time alerts to intelligence agencies when potential terrorists or foreign operatives attempt to enter the country, apply for a credit card, or are stopped for a traffic violation. The novel capability allows

agencies to establish these real-time alerts on hundreds of thousands of unclassified machines (for example, on every police laptop in US) without having to reveal classified triggers for alerts on the unclassified machines performing the monitoring. (For example, the triggers could be pseudonyms of terrorists or descriptions of the car they are driving, which are obtained through human intelligence and are classified, and thus cannot be released through an All-Points-Bulletin);

- Providing a service similar to Google for the intelligence community and DoD, by which Stealth's servers will continuously collect and store a portion of the web (or chat room traffic). When the intelligence community wants to search this data, they will send (encrypted) search queries to Stealth's servers; Stealth's servers will be prevented from decrypting these queries both during and after servicing the search request. Although Stealth's servers will never "understand" a given query, they will be able to process it and compute the encrypted answer. (Likewise, Stealth's servers will be unable able to decrypt the answer). Our revolutionary technology allows us to run an encrypted query against a portion of the web and compute an encrypted answer without ever getting the decryption key for either the query or the answer. It is worthwhile noting that Stealth's servers need not be located in a Sensitive Compartmented Information Facility (SCIF) because no information about a query or corresponding answer is ever revealed to Stealth's servers. This presents significant advantages to the intelligence

# White Paper on Stealth Software Technologies



For further information, contact:

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

*-Proprietary-*

community and DoD, including the ability to search portions of the web in a timely manner without revealing anything about the queries and without having to continuously import the web into a classified environment, thus providing considerable cost-savings and operational agility.

In contrast to other solutions in the marketplace, Stealth's software is real-time and is significantly more cost-effective. Stealth developed its patent-pending technology to address the need for secure search that conceals search terms. The solution works as follows:

- Step 1: Type an original query on a classified system (the "high" network) and apply our STEALTH-COMPILER to create object code that is ready to do the search. The STEALTH-COMPILER also creates a special decryption key.
- Step 2: Migrate an object code (an encrypted query) to an unclassified system (the "low" network) to potentially many locations throughout the network (such as all police laptops or an unclassified server farm that stores a portion of the web).
- Step 3: Run the object search code generated in Step 1 on the unclassified data on multiple unclassified machines processing one document/object at a time and update the encrypted storage for each document. The main novelty is that this code is a "straight-line code," which means it applies the same process to every input and appears to continuously overwrite a small encrypted buffer. However, the software actually retains (in an encrypted form) only data that

matches the conditions of the query while providing a bullet-proof guarantee that makes it impossible to tell which documents eventually satisfied the query.

- Step 4: Periodically (once per minute, hour, day, week, month, etc.) bring the small encrypted buffer that contains the encrypted answers from the low (i.e., unclassified) network to the high (i.e. classified) network.
- Step 5: Decrypt (using the key generated in Step 1) the contents on the high network, which will contain only documents that satisfy the classified query criteria.

## Important notes:

- Step 4 can be executed in a real-time by delivering (every minute) an encrypted match/no match "flag" from each unclassified machine that executes the search to classified machines. Such flag footprint is tiny (a few hundred bytes) and can be processed in real-time. Step 4 can be further "hardened" to ensure that only certain information can get flagged (for example only names from a predefined set of possible names). This capability is critical in multi-agency and DoD coalition operations, where additional assurance about release of data must be guaranteed for coalition and multi-agency operations.
- In all cases, the computer being searched must have Stealth's software loaded on it (permission to search must have been granted by the Network Administrator). Thus, the user of the computer being searched will be aware that the computer is

# White Paper on Stealth Software Technologies



For further information, contact:

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

*-Proprietary-*

being searched, but will be unable to know what terms are being searched for. Although the terms and results of the search remain secret, this is not a spyware program.

## Customer needs addressed:

### Internal Agency: High to Low Search and Data Collection

The U.S. Intelligence Community is composed of 16 major agencies comprising approximately 100,000 individuals.<sup>1</sup> The information in these agencies is controlled with varying levels of employee access to information (i.e. "Secret", "Top Secret," and Sensitive Compartmented Information (SCI) or Special Access Program (SAP) clearances levels). Data is stored on multiple networks that are physically separated from each other. As a result, users of differing clearance layers are prevented from searching different clearance levels (both lower and higher). This was originally designed to ensure that less secure, less secret, "low" networks did not have access to the more secure and more secret, "high" networks. Clearly, it is essential to prevent users with lower clearance level from accessing information of higher clearance level. However, the current practice paradoxically also prevents users with higher clearance levels from searching data of lower clearance (or even unclassified) levels; that is, a huge obstacle exists for high users who need to be able to easily search and manipulate information on low

networks. Currently, high side users are not permitted to query low networks because the nature of a query can divulge higher clearance information. In order for the users with higher clearance levels to search the low network (or even the internet) the **entire** low network must be temporarily replicated and stored on a secure high network. This method is costly, time consuming, and does not allow for real-time information access. By strongly encrypting the search terms and results using our technology, Stealth's software allows high network users to search low databases and pull the data to the high level without revealing the search terms or results to low side and without having to continuously replicate low network data on the high network.

The secure search functionality desired by the intelligence community encompasses two major needs: real-time monitoring of new information added to a low side network or database (such as news articles released throughout the course of the day), and the ability to mine an entire low database (e.g., a search of all of the incidences of the word "Hamas" in the past three years). Although these are both major pain points for the intelligence community, the two applications differ in the computing power required to carry out the secure encrypted searches.

### Inter-Agency Information Sharing:

In the post 9/11 world, one of the intelligence community's greatest problems has been data sharing between agencies. Significant data mining projects that attempted to bridge the gap between disparate government databases have

---

<sup>1</sup> John Negroponte, Director of National Intelligence, Speech, September 11, 2006

# White Paper on Stealth Software Technologies



*For further information, contact:*

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

*-Proprietary-*

been terminated due to privacy concerns. Cooperation between agencies has been hindered by laws that prevent database sharing between agencies. Furthermore, certain legal restrictions prevent high side users from allowing low side users to view search terms (e.g. high level CIA members need to search an NYPD database but do not want low-level officers to know what terms they are searching).

Stealth's software solves these problems. Unlike large-scale data mining programs which simply aggregate data and search for meaningful relationships, Stealth's software only allows users to search for specific terms (identities, bank account numbers, etc.). This mitigates privacy concerns by allowing legal processes (e.g., obtaining warrants) to be followed prior to searching because the search is targeted towards specific terms. More importantly, encrypted search and retrieval ensures that only the individual(s) writing the query sees what was searched for and what was found. To further protect privacy, the software can also be adapted to allow the unencrypted answer only to go to a trusted intermediary (such as a judge). This allows classified searches to be conducted with assurance that no information goes back to the high side without being looked at by a trusted intermediary. The advantage is that there is no trace of the nature of the query left on the low machine, thereby ensuring that sensitive data is not divulged.

Currently, conducting sensitive search of any type between agencies is impossible because it requires allowing the agency performing the search to replicate an entire database/network in a secure environment. For obvious privacy

reasons, agencies such as police departments do not allow this wholesale replication. As a result, potentially crucial criminal and national security data is not shared to the degree it should be shared.

## Inter-Governmental Information Sharing:

In addition, Stealth's software can be configured to return only an encrypted binary "found"/"not found" response. This allows an analyst at one agency to determine if a record exists in another agency's database, but forces that analyst to work through the personnel of the other agency in order to view the content of the matching record if one exists. This limited search configuration is useful for cooperation between U.S. agencies and for multi-nation operations, enabling two different countries' intelligence agencies to cooperate with much stricter control over the information being shared.

## Intelligence Agency Alert Network: Agency /Local Law Enforcement

Stealth's software is ideally suited to providing an "alarm" system that can alert high level clearance users in real-time when critical (classified) events occur. Further, it does so without necessitating that high users have unfettered access to the databases of other agencies or companies. By loading Stealth's software client onto low side police officer laptops, Stealth's software would allow agents at the FBI, CIA, and DHS to be alerted within

# White Paper on Stealth Software Technologies



For further information, contact:

- Dr. Rafail Ostrovsky      rafail@stealthsoftwareinc.com
- Dr. William Skeith      William.skeith@stealthsoftwareinc.com

-Proprietary-

seconds if a suspect's name appears on local or state law enforcement computers. For example, if a known terrorist (using either a real name or known alias) is stopped for a traffic violation, this event would appear as an alert to the intelligence analyst within seconds. Under this scenario, Stealth's software would return the cell phone or other contact information of the officer who stopped the individual in question so that the intelligence officer can follow up with the arresting officer. This same alert system can also be applied to flight manifests and border entry databases.

This alert type of search requires minimal computing power and data transfer, resulting in true real-time results. With Stealth's software, updates can be sent every few seconds to the high side with no additional hardware needed. The low network can be guaranteed that the high user is only getting an I.P. address or officer contact information, and that they are neither copying nor replicating the entire police record. Moreover, this alarm system can be easily installed on any network willing to cooperate with a federal intelligence or law enforcement agency by installing Stealth's software.

## Intelligence Agency Alert Network: Agency / Commercial Database

Similar to the FBI's desire to search law enforcement databases, intelligence agencies often need to securely search and monitor commercial databases, such as airlines and

credit card databases, without company employees (who have no security clearance) knowing the specific nature of the search. Using current methods, these searches require replicating the entire databases being searched, thus creating privacy concerns. By searching only specific terms instead of replicating entire databases, privacy-protecting controls can be easily implemented (search results can be routed directly to a judge to decide if this information violates privacy protections). In addition, Stealth's software enables the high value application of ongoing monitoring and alerts, two features that are not part of the capabilities offered by current solutions. This monitoring will be extremely useful in cases of suspected terrorists attempting to open bank accounts or purchase dangerous chemicals.

---

*To date Stealth Software has received \$150,000 in NSF SBIR grants, and an additional \$100,000 from the Office of Naval Research. In addition, depending on our achievement of certain milestones, Stealth Software may receive up to another \$1 million in grants during this upcoming year. Stealth Software developed our patent-pending technology at UCLA, and we have negotiated exclusive rights to this patent from the university. The company has developed a working prototype of our product, which is currently ready for beta testing.*