U.S. NAVAL INSTITUTE

Published on U.S. Naval Institute (http://www.usni.org)

Proceedings Magazine - March 2015 Vol. 141/3/1,345

Professional Notes

The New Paradigm for Cyber Security

By Captain Mark S. O’Hare, U.S. Navy (Retired), and Alfred R. Berkeley III

Traditional “network-centric” cyber defenses intend to prevent a thief from reaching data, while new “data-centric” cyber defenses assume the thief will reach it. The new defenses make information hard to find and impossible to read. The difference between the old and new approaches is profound. By changing the balance of power between predator and prey, it introduces a new price-performance curve for cyber security.

The intelligence community is moving some of its processing to commercially provided “cloud” computing. The first part of its rationale was that data-centric cyber security would make the cloud implementations safe. While the media picked up on the outsourcing policy conflict, it failed to address the technologies that make the move safe—it missed the shift from network-centric to data-centric technologies.

“Data-centric” Cyber Security

Conventional wisdom says data-centric security is “encrypted storage.” Too simple, this definition misses the mark. Data- centric cyber security is much more than encrypted storage or encrypted transmission, and it is fundamentally different from what we have all been taught: It is a new paradigm.

At the core of data-centric cyber security, “cryptographic splitting” combines the functions of encryption, authentication, random bit splitting, communities of interest, fault tolerance, and key management into a single pass-through function. Data is fundamentally transformed into secure, fault-tolerant, and verifiable portions, with reduced key management overhead.

Data-centric cyber security is arriving now for several reasons. First, the failure of traditional methods has focused attention on the need for new methods. Second, entrepreneurs saw the need and invented the new technology. Third and more fundamentally, the computational power required to make data-centric cyber security functional, reliable, convenient, and cost effective has arrived in the form of more powerful microprocessors.

State-of-the-Art Capabilities

These capabilities are the current state-of-the-art for data-centric cyber security:

Encryption, a fundamental capability, is necessary but not sufficient to define the data-centric paradigm. Data-centric cyber security uses any encryption that the user wants to use.

Bit-splitting is the “secret sauce” of the new technology. Technically, it is cryptographic splitting or robust computational secret sharing (RCSS) in a multifactor implementation. RCSS is a relatively new branch on the computer science tree. Bit-splitting takes cipher text and decomposes it bit by bit. It prepares each bit for reassembly and then for physical dispersal. If you have the keys, reassembly is easy; if not, it is overwhelmingly complex.

Physical dispersal places the bits in a user-defined number (“N”) of physical locations, or “shares.” Information- dispersal algorithms are not new, but using them to distribute randomly selected data at the bit level is. The physical separation can be on a combination of local and remote locations.

Redundancy is provided by adding bits to enable “M” of the “N” shares to rebuild lost or damaged shares. Think of redundant array of inexpensive disks storage. The user can specify what “M” is. (“M” is less than or equal to “N.”) The redundancy inherent in cryptographic splitting eliminates the need for copies of copies so prevalent in most data centers today.

High availability is all about “up time” as a percentage of “total time.” Having data accessible from multiple dispersed physical locations and requiring less than the total number of shares to restore the data improves the odds of remaining up if one or several locations are unavailable. “M” of “N” provides high availability.

Disaster recovery is the ability to recover from a disaster, man-made or natural. Again, being able to operate from many locations without interruption improves the odds of recovering from a disaster. “M” of “N” provides disaster recovery.

Imperviousness to brute force decryption is a result of the predator not knowing how many shares it needs to recover before starting to break the system. “M” of “N” provides imperviousness to brute force decryption. No complete file exists unless shares are recombined under system control.

Imperviousness to distributed denial of service attacks is a useful byproduct of physically distributed shares and the ability to operate with only “M” of “N” shares available. Locations under attack can be ignored while the business can keep operating out of other physically separated locations.

Authentication is provided to ensure that the data in any share have not been corrupted or tampered. It is about authenticating data, not users. Authentication is performed either on the presplit encrypted data or the individual data shares to detect data corruption due to hardware failure or targeted attacks.

Key management is substantially automated, and most keys are encrypted, split, and dispersed. It's not new, but splitting keys at the bit level and dispersing the bits randomly is. The vast majority of keys are handled inside the dispersed shares. A smaller number of keys are managed externally, providing a simplified multi-tier key management model.

Communities of interest are an important capability. Multi-level security for coalition forces is a typical community-of- interest implementation. While communities of interest are not new, using cryptography instead of physically separate networks to isolate them is. This would prevent the "Snowden effect."

Nuclear controls are mimicked if the system is programmed to require two or more authorized users to initiate actions simultaneously.

Mandatory shares can be implemented, which provide for one or more designated data shares that must be present for the data to be recombined.

Cloaking is the ability to make the Internet beyond the data-centric software vanish to probing hackers. This is a powerful capability that has won industry prizes.

Rebuilding lost or damaged shares without decrypting the remaining shares is a powerful capability, and it is available in state-of-the-art commercial offerings. Cryptographic splitting provides the ability to rebuild lost or damaged shares without un-encrypting as a byproduct.

File-level security allows single documents to be accessible to specific communities of interest. A single file might be available to one person, or many files to many people, or anything in between.

Divisions of labor can be configured, for example, so that administrators can maintain data but not read it. The cost savings are significant, as are the improvements in security.

Cryptographically separate networks will allow running the Non-Secure Internet Protocol Routing Network, the Secret Internet Protocol Routing Network, and the Joint Worldwide Intelligence Communications Network on a single physical network.

Man-in-the-middle attacks can be thwarted because the network packets can be cryptographically split into shares that can be encrypted with keys that have been established using certificates issued by separate certificate authorities. This creates a "distributed trust model" that provides cryptographic separation within a single communication link. Since bit- split data is cryptographically split and is never whole, a hijacked channel will yield no meaningful or intelligible data to the thief.

Implementing this data-centric paradigm in secure virtual machines can avoid any use of shared memory. Since that is the playground of choice for cyber mischief, many threats are avoided.

Digital rights management can be enhanced using cryptographic splitting to provide improved file-level security and communities of interest.

The new paradigm meets the relevant requirements of the Federal Information Security Management Act and a series of other hurdles, and can be useful to U.S. government departments and agencies.

'Significant Asymmetries'

The net effect of cryptographic splitting is to keep the data unintelligible when it is at rest (in storage) and in motion (in transmission). Since data are in storage for most of their lives, in transmission for a tiny percentage of their lives, and in process (in the microprocessor) for only a tiny portion of their life cycles, these data-centric approaches to security make the data hard to find and even harder to read if found. Time-wise, this new approach protects most data 99.99999 percent of their lives.

The technology has a number of Federal Information Processing Standard 140-2, Common Criteria, and Evaluation Assurance Level 4-plus certifications. Because the approach is so radically different, it has been tested quite a bit by people who know what they are doing; the encryption works.

We are looking at a new price-performance curve for cyber security. Like many new technology curves, this one offers better performance at lower all-in costs. It is likely to create unexpected collateral damage to older technologies and their vendors. The described capabilities improve cyber security a lot, but they are not all we need. They help with data at rest and data in motion, but they do not protect data in the microprocessor. Furthermore, while they authenticate data, they do not authenticate users. Strong policy and provisioning will also always be needed in any good security solution.

The new data-centric paradigm creates significant asymmetries between friend and foe. Authenticated friends have the keys, while the foe has an enormous computing load to find and intercept even a single share, thus rendering any intercepted data meaningless.

Kevin McLaughlin, "Amazon Wins $600 Million CIA Cloud Deal As IBM Withdraws Protest," CRN, 30 October 2013, www.crn.com/news/cloud/240163382/amazon-wins-600-million-cia-cloud-deal-... [12] .
Mihir Bellare, Phillip Rogaway, "Robust Computational Secret Sharing and a Unified Account of Classical Secret- Sharing Goals," 14 August 2007, https://eprint.iacr.org/2006/449.pdf [13].

Captain O'Hare graduated from the U.S. Naval Academy in 1976. He is a former program executive officer of aircraft carriers, and currently the CEO of Security First Corp.

Mr. Berkeley is the former vice chair and acting chair of the President's National Infrastructure Advisory Council. He is also the former president of the NASDAQ stock market and is currently the director of Security First Corp.
