

## **Distributed Data Schemes Provide Security**

A Cyber Security Assumption Buster Workshop Series

**Assertion:** “Distributed Data Schemes Provide Security”

Distributed data architectures, such as cloud computing, offer very attractive cost savings and provide new means of large scale analysis and information sharing. There has been much discussion about securing such architectures, and it is generally felt that distribution, and the replication that is usually associated with it, provides some inherent protection; adversaries will have difficulty locating your data in the cloud, and by breaking it up and replicating different segments throughout the platform we send the adversary on a wild goose chase to find and reassemble all the relevant bits. It is also felt that cryptographic mechanisms like bound tags, encryption, and keyed access control can be used to develop distributed platforms with a high level of assurance. There are several applications of distributed architectures that offer non-sensitive services like viewing recorded TV at the airport. Applications are also offered for potentially sensitive uses like document collaboration. Yet it is unclear whether these applications can safely be extended to highly sensitive uses. Could we readily support a distributed electronic health care system that securely supports ad hoc consultations or remote surgery with full access to patient history while protecting patient privacy, for example?

To answer this question we need to take a closer look at the protection provided inherently and cryptographically. With respect to the former, we must think about how the architecture can be designed to provide secure availability to friend and not foe. We must examine the impact of the design for security, resilience, and availability and understand the trades we are implicitly making among these attributes. We must consider whether the data about data that is required by these architectures introduces a new data risk. We must think about the multiplicity of paths provide by these architectures. We must figure how to do risk analysis on a system when key information like data location is unavailable by design. With respect to the latter, we must consider the whether the key management strategy is robust enough operate in a distributed architecture. We have to think about the assurance of tag binding and access update and revocation. We must consider the vulnerabilities of the platforms that host the cryptographic mechanisms and the distribution of those functions in the architecture.

In this workshop, we will explore the implications of distributed data on security. We will consider what effect the introduction of the notion of a determined adversary has on our analysis of data security requirements. In the first session we will discuss the properties of distributed platforms that are thought to make such architectures inherently more secure. In the second, we will discuss the issue of cryptography and distributed platforms.

### **Distributed Data Questions:**

- What characteristics make distributed data environments secure?
- What is the opportunity for attack in a distributed data environment?
- Can we expect opportunities to be increased, decreased, or simply be different than similar enterprise computing models?
- How is the threat model changed in the altered environment?
- Are the technical controls for assuring integrity, availability, and confidentiality of sensitive data and computations stronger or weaker in the new environment?
- How do users with interrupted service distinguish between malicious behavior and routine maintenance?