

Integrated Adaptive Resilient Asymmetric Data Security

CHALLENGE

Many common applications must access sensitive data. Compromising sensitive data can cause major damage, so protecting data confidentiality is essential. Integrity is also important because computed results must be trusted to be correct and untampered. Combining integrity with data confidentiality protection can introduce additional challenges.

CURRENT PRACTICE

Existing techniques cannot adequately protect data confidentiality, even prevalent approaches such as isolation, hardening of software and hardware, and active monitoring have their associated risks. It is unrealistic to eliminate every software and hardware bug for all reasonably complex real world systems, even with the best possible engineering practices. Many applications are performance-driven and often use cutting edge hardware and software components. Thus, we can expect many software and hardware bugs and security vulnerabilities that can be exploited by an adversary. Once an attacker breaks into a system, some aspects of confidentiality and integrity are immediately compromised.

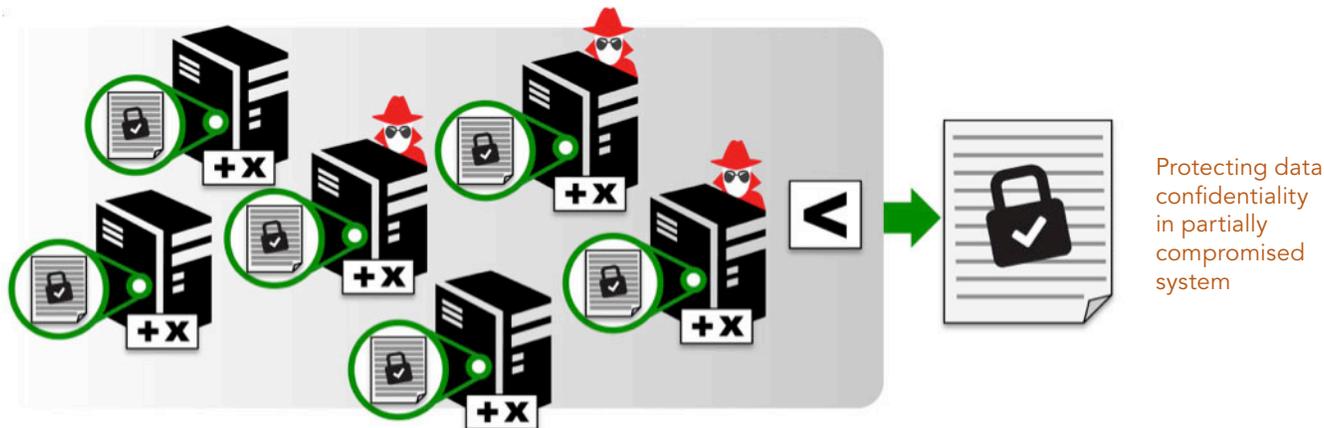
APPROACH

The goal of this project is to develop technologies that can provide provable secure resilient data confidentiality, as well as integrity. By provable secure, we mean that we can withstand any kind of security attacks, no

A general practical method to protect data confidentiality even when parts of systems are compromised



matter the amount of resources that attackers may have. That is, the attacker's only option is to guess at confidential information with the given amount of resources. To achieve provable data confidentiality for common applications, first we must extend computation over encrypted data to allow both data query and data processing operations. One obstacle is that it is theoretically impossible for one homomorphic encryption scheme to allow both range queries and



additions, or both range queries and multiplications, and still be able to withstand chosen text attacks. To overcome this obstacle, we developed a scheme to enable data to be transformed into different encryption forms in distributed environments when different data operations are needed. Second, our system must adapt to the changing threat levels. We develop techniques to enable partially compromised systems to dynamically reconfigure to tolerate increasing numbers of compromised machines.

IMPACT

We are developing a technique that can protect data confidentiality and integrity, as well as availability, even when parts of a distributed system are hijacked. Our technique does not require knowledge of specific exploits and is applicable to a wide range of both known and unknown exploits, including zero day exploits.

Contact

Jian Yin

Principal Investigator
(509) 371-6398
jian.yin@pnnl.gov



Pacific Northwest
NATIONAL LABORATORY

*Proudly Operated by **Battelle** Since 1965*