The Poly^2 Network Architecture

March 16, 2004

What is Poly^2?

The Poly^2 project is an advanced research project in security architecture. It will provide secure, highly reliable network services through the use of multiple, independent systems (poly-computer) and multiple networks (poly-network). The implementation of the platform is based on sound design principles. Poly^2 addresses security issues, high availability, and scalability for critical network services.

Motivation

The highly publicized attacks involving Internet worms such as "Sapphire" and "CodeRed" illustrate serious design flaws and vulnerabilities in the implementation of server technologies. A single server machine often provides many network services simultaneously thus increasing the likelihood that a weakness in the design or implementation of a single service can be used by an attacker to commandeer the entire machine. These machines often have multiple command shells, interpreters, and compilers in addition to the code needed for the machine's primary server function. Attackers exploit the presence of these tools to infiltrate a machine, create new attack tools, propagate attacks, and conceal their activities. Our objective is to apply well-understood information security design principles to create a new distributed server architecture that is highly resistant to attack.

Design Principles

The Poly^2 network was designed with the following ideas in mind:

- Modularity

  Systems inside Poly^2 are interchangeable and independent. Any system in the infrastructure can be removed, replaced, or provisioned as needed.

- Fault Tolerance

  A failure in one component will not cause the rest of the system to fail. Multiple instances of a service can run on different hardware nodes.

- Scalability

  Adding capacity to the system is addressed with the addition of relatively inexpensive hardware.

- Service Isolation

  Each service resides on a singular, independent hardware node. Information flow is restricted to reduce the impact of attacks from compromised nodes.

- Least Privilege

  Systems and services have only the privilege needed for their function, and no more.

- Economy of Mechanism

  Since hardware nodes do not host multiple, unnecessary services, the supporting O/S and network implementations can be simplified.

- Defense in Depth

The protection mechanisms are layered to prevent a single successful attack leading to compromise of the entire system.

Implementation

This architecture is built using inexpensive commodity hardware, multiple network components,highly specialized and optimized O/S kernels, and application-specific software libraries in order to provide a given machine with only the resources necessary to provide a given network service. Additional machines providing other services are then linked using a novel communications infrastructure with additional management and intrusion detection capabilities. The aggregate design provides a myriad of traditional services to the Internet community while minimizing the ability of an attacker to take control of a given machine. Further, the modular nature of the design allows for rapid deployment of new Internet services, fault tolerance, and ease of administration. In addition to enhanced security and reliability, we believe that we will also see significant performance improvements in applications due to the fact that individual machines will be be tailored to a specific service.

More Information

Email: cerias-proj-poly2@cerias.purdue.edu
Web: http://www.cerias.purdue.edu/homes/poly2/