A Better Software System and Infrastructure

SoftEcoSDK*: A System Foundation*

What

- Environment for Client to Server Communication within a System:
    - Infrastructure securely identifies a Client to a Server
    - Firewall embedded within each Server
    - Work organized as session with checkpoint & recovery
- Message Communication Layer
    - No talking to strangers
    - Each message travels via two different paths
    - Point to point Conversation
    - Authorized Publisher to Authorized Subscribers
- Data Content Conversion between Formats
    - Class to and from Serial, XML, etc.
    - Meta data resides in memory with each class attribute

Why

- ***Prevent Cyber crime***
- ***Survive*** most ***disasters***
- High Availability with less than 2 minutes of downtime per year
- Work tasks ***scale*** when computer added
- Significantly less ***cost*** for program development and system administration
- Programs in different software languages, OS and computer work together

Software System Infrastructure, LLC

SoftEcoSDK: *A System Foundation*

A New Approach to Improved Cyber Security and Reliability

Cyber security begins by identifying points of entry into a system. Each point of entry must detect and resist an attack. A determined attacker might find a way through or around this defense. Therefore, system actions are logged and examined to detect unusual patterns that indicate a potential breach. Complete statistics on successful attacks are not publicly available. However, it can be estimated, based on published incidents and the prevalence of identity theft, that most everyone is potentially affected many times per year.

A computer-based system is available more than 98% of the scheduled operation time. This translates to down time of about 2 hours every month. This level of service is sometimes acceptable if no competitor offers significantly better service.

The aerospace, defense, energy, telecommunication and other industries have found ways to create a system that is much more reliable. For example, a telecommunication system is down less than 2 minutes per year. These solutions tend to be industry specific, based on specialized costly hardware, and unique to a vendor.

There is a new approach to a secure and high availability cyber system. The approach follows a pattern like how an operating system provides an environment for a program on one computer. An infrastructure provides an environment to create a system from computers, a network and programs sharing work among computers.

A system of computers and programs using this infrastructure operates in the following manner. An external user accesses functionality on a system interface computer. The interface computer uses the infrastructure to access a work computer holding valuable information and performing critical operations. The infrastructure firewall protects a work computer from becoming compromised by a potentially compromised interface computer. If a work computer goes down, then in progress work is recovered by another work computer. Communication between an interface and work computer continues after a pause for work fail-over. An external user might see this pause as a onetime increase in response time.

Features of this environment include:

- An infrastructure middleware with a specialized firewall.
- A program publishing an event message to configured subscriber programs.
- A program exchanging messages with an instance of itself or a configured parent program.
- A program indicating when it is ready for operation and to be directed to become active.
- An infrastructure directing a program instance to become active as needed.
- Client to server communication through an intermediate manager that saves checkpointed recovery data.
- Recovery of in progress work as needed by an identical program instance on another computer.
- Data conversion between class instance, serial and human readable text formats.

This approach differs from using a standard network firewall between layers of computers within an organizational system. A sending computer securely and uniquely identifies itself to a specialized firewall such that a firewall can better detect and discard an unauthorized message. An intermediate client to server manager uses sender identity, passed from a firewall, to tell a server what actions that a client is permitted to request from a server.

Major advantages of this new approach include:

- Information visibility securely controlled via whitelist of published event types, publishers, and subscribers.
- Allowed actions securely controlled via whitelist of clients, servers, and allowed service requests.
- No ad-hoc configuration changes as system configuration is under configuration management.
- Test a new system version at any time as multiple versions can operate at the same time on the same hardware.

This approach improves data center or control system security and reliability at a reasonable cost. The approach also scales workload among computers. Find out more details by visiting SoftEcoSDK.com or contacting SoftEcoSDK@gmail.com.

Software System Infrastructure, LLC