ITANIUM® SOLUTIONS ALLIANCE

Case Study

Eliminating Malware Vulnerabilities

Intel® Itanium® 2 Processor
Network Servers
Streamlined Operating System
Enhanced Security

SECURE64

"Secure64 has drawn from its intimate knowledge of the Itanium architecture to develop software technology that provides unheard of levels of security for the enterprise with significant performance improvement."

Kirk Skaugen
VP, Digital Enterprise Group, GM, Server Platforms Group, Intel Corporation.

SourceT* is a micro operating system designed from the ground up for unprecedented levels of security and performance.

As the master of system resources, the operating system has the greatest responsibility for achieving security. It controls the resources of the computer – memory, CPU, I/O devices – and has an obligation to protect the system from unauthorized access. To help the operating system thwart attacks, IT professionals apply security patches on a regular basis and create more layers of defense by adding security appliances to the network.

But constantly plugging security holes consumes an ever-increasing share of IT time and budget. These 'solutions' are often just temporary fixes, susceptible to new attacks of escalating sophistication. IT departments face the unending task of preventing the loss of vital business assets.

Contributing to security woes is the ever-increasing size – millions of lines of code - of today's general-purpose operating systems (Linux*, Windows*, and Unix*). "They are developed, tested and maintained by huge teams of programmers, none of whom can possibly understand the entirety of the code base or all the interactions among code modules," says Bill Worley, CTO of Secure64. An alternative approach is to install a very small footprint operating system, optimized for performance and security, on the most vulnerable systems on the network.

IT departments place a high priority on protecting servers located at the edge of the network that are connected to the outside world, thus most vulnerable to attack. Such is the case for Domain Name System (DNS) servers that translate domain names to IP addresses. "If DNS servers go down, the Web goes down, email goes down and entire businesses go down," says Steve Goodbarn, CEO of Secure64.

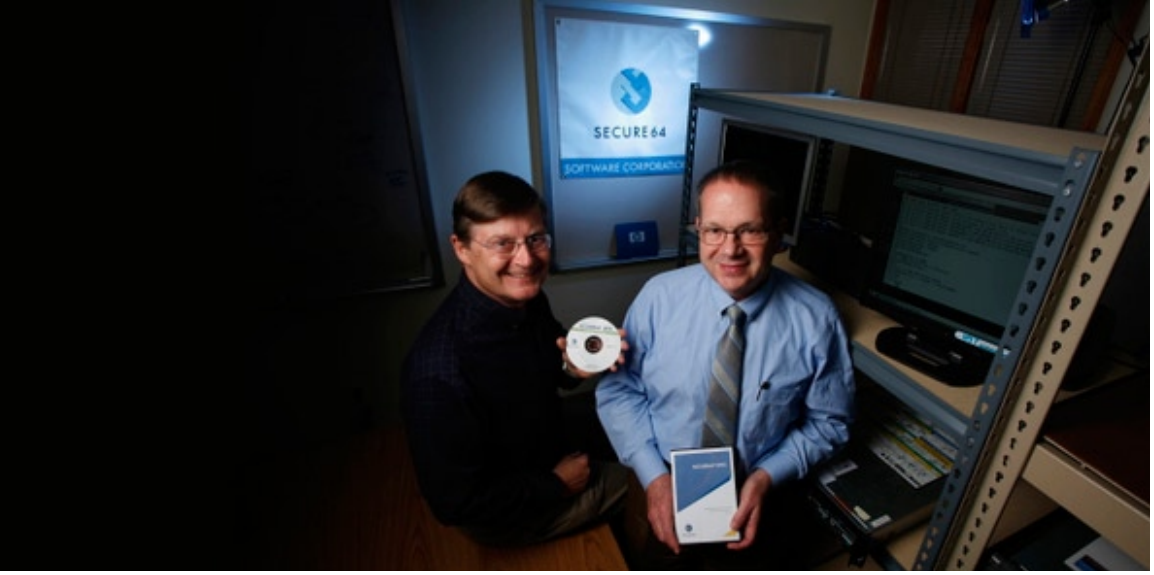
Understanding the benefits from running a streamlined operating system on systems prone to attack, Secure64 sought to develop a platform addressing both security and performance.

Challenge

- Minimize operating system footprint. Keep the size of code with greatest system authority (highest privilege level) to an absolute minimum, thus reducing the amount of attack-susceptible code.
- Protect the software. Prevent malware from accessing applications and data.

Solution

- Enforce six essential security properties. Develop operating system that optimizes security and performance.
- Address security issues at the lowest system level. Employ the hardware security features of the Intel® Itanium® 2 processor.



Designing a System Invulnerable to Attack

Developing a system that can adequately defend itself against malware begins with an understanding of the root causes of vulnerabilities in today's operating systems. This analysis helps solve security issues at the lowest system level possible, where it's typically less expensive and more effective. For example, it's better to protect memory regions at the CPU level than at the board, application software or system levels.

There are four generic security challenges to solve. First, the highest software privilege level (PL.0) must be highly secure. The code running in PL.0 should be very small and access to code executing in PL.0 should be reliably restricted. Second, memory must be protected from unauthorized access, preferably enforced through hardware-based mechanisms. Third, I/O stacks require safeguarding, especially in light of networking protocols that were not designed to withstand misuse. Last, system administrators must be sufficiently authenticated.

Spotlight: Secure64 Software Corporation

- Founded in 2002 to provide network and server applications capable of assuring high levels of security and performance.
- In March 2007, Secure64 DNS™ server software was launched for use on HP Integrity rx2660 servers. The software runs on Secure64's SourceT micro operating system.

Plugging Security Holes

Secure64 developed the SourceT micro operating system to specifically address critical problems currently plaguing many network servers. The operating system, in conjunction with security features of the Intel Itanium 2 processor, satisfies six essential characteristics required to ensure the integrity, availability and data confidentiality of a software system.

1. SourceT implements a fully authenticated boot process that ensures the integrity and authenticity of the operating system and application images. Whenever the hardware is powered on, the cryptography features of the SourceT micro OS help verify that critical system software has not been compromised.

2. SourceT provides a secured runtime environment that fully protects memory from access by unauthorized code. This feature can prohibit any code, rogue or otherwise, from reading or writing executable images. Using the memory compartmentalization and protection key features of the Intel Itanium 2 processor, Secure64 is able to protect memory, prevent code execution on stacks, protect critical stack control flow information and isolate memory allocation bookkeeping.

3. SourceT protects the highest privilege level by executing a minimal amount of protected code (less than 10K lines).

"The execution environment includes compartmentalized memory which provides a new level of protection for crypto keys, policy control data, and other types of information requiring the highest security."

Bill Worley
CTO
Secure64

"The rx2660 was designed to bring the power, reliability and availability of mission-critical computing to a broader range of enterprise customers and the Secure64 DNS server application advances these benefits."

Michelle Weiss,
VP of Marketing
Business Critical Systems
Hewlett-Packard

4. SourceT keeps critical information confidential and uncontaminated through its file system using encryption. It encrypts and provides integrity checks for critical, non-public information using secure symmetric keys.

5. SourceT maintains availability during network attacks through its self-protecting I/O stack. All defensive measures are integrated in Secure64 software, without reliance on external protection schemes that could themselves introduce vulnerabilities.

6. SourceT is designed for multi-factor authentication and limited user authorization categories to prevent unauthorized system access.

Summary and Metrics

The performance and security efficacy of the SourceT micro operating system was evaluated during laboratory testing.

To evaluate performance, a test DNS application running on SourceT processed 102,000 queries/second, while the same application running on Linux responded to 50,000 queries/second. The raw performance of the SourceT micro operating system was more than two times better than the similar test on Linux.

In a separate test on a different hardware configuration, security efficacy was evaluated by simulating a DNS application under a network flood attack - an attacker sending a high volume of packets to a target to consume all of its available bandwidth.

- While under a 200,000 packet/second UDP[i] reflected[ii] flood attack, SourceT replied to 96,000 queries per second (0% degradation).

  By comparison, the same DNS application running on Linux on the same hardware was able to respond to 5 queries per second (99.99% degradation). SourceT was 20,000 times better for UDP-based attacks.

- While under a TCP SYN flood[iii] of 40,000 packets/second, SourceT replied to 95,000 queries per second (1% degradation).

  By comparison, the same DNS application running on Linux on the same hardware was able to respond to 5,000 queries per second (90% degradation). SourceT was 20 times better for TCP SYN-based attacks.

The impressive denial-of-service security results can be attributed to the SourceT micro operating system architecture, which builds TCP and UDP attack protection into the I/O stack, allowing applications to continue to function properly even while under a large network attack.

Key Hardware Solutions

- HP Integrity rx2660 Server
- Intel Itanium 2 processors with enhanced security features:
  - Memory compartments with protection keys to restrict access rights to memory pages
  - Independent page-level read, write and execute privileges
  - Separate RSE[iv] and conventional stacks
  - No code execution from the stack

Key Software Solutions

- SourceT micro operating system
  - Less than 10K lines of code running at PL.0
  - Asynchronous, non-blocking I/O stack
  - Built-in denial-of-service protection
  - Fully authenticated boot process

At the Intel Itanium 2 processor launch, Secure64 also demonstrated the ability of SourceT to protect memory partitions. A virus was allowed to execute under both SourceT and Linux operating systems. While it was able to find a cryptography key stored in memory and use it to decrypt secure data - credit card information - on the Linux platform, the virus was unable to access the cryptography key on the SourceT platform.

i User Datagram Protocol (UDP) is one of the core protocols of the Internet.

ii A reflected flood attack involves sending forged requests to a very large number of computers that will reply to the requests which are transmitted to the target.

iii A SYN flood is a form of denial-of-service attack in which an attacker sends a succession of SYN (synchronization) requests to a target's system.

iv The Register Stack Engine performs functions on conventional stacks, such as freeing registers for the current stack.

Benefits of Using Itanium® 2-based Solutions

The Itanium 2 architecture is the only commercially available microprocessor architecture offering the hardware security features required to create a genuinely secure, high performance system. These features include:

- Memory compartments and protection IDs
- Independent read, write and execute privileges on a per page basis
- Separate conventional and Register Stack Engine (RSE) stacks
- No code execution from stacks
- Parallel instruction processing

These features, combined with the unique architecture and capabilities of the SourceT micro operating system create an environment offering breakthrough levels of security and performance for mission-critical enterprise applications.

ITANIUM® SOLUTIONS ALLIANCE