Achieving the highest levels of IT security with HP OpenVMS

Table of contents

invent

Introduction

The litany of threats in today's online world – viruses, worms, hacking, slamming, spamming, phishing, spyware – reads like the inventory of a mad scientist's laboratory combined with the to-do list of a terror cell. Delivering complete security coverage across an enterprise's IT infrastructure in the face of these threats is a fundamental component of overall enterprise business continuity.

HP designs its products, services, and solutions to be secure in operation and deployment to meet this rapid growth in the rate of security incidents; an ever-increasing sophistication of attack; government response through regulation; and changes in IT infrastructure to accommodate changing business objectives.

An important product contributing to the HP security framework is a general-purpose, commercial operating system for those with exceptional security needs – the HP OpenVMS operating system. OpenVMS has years of proven performance, high availability, and the impeccable security credentials that are the subject of this white paper. It was one of the first commercial operating systems to achieve a US Department of Defense C2 security rating and all new releases comply with these rigorous standards.

OpenVMS continues to evolve with industry-standard security technology enabling secure interoperation in heterogeneous environments. And it runs on the HP Integrity server platform as well as HP AlphaServer systems. OpenVMS is an ideal operating system for today because security was designed in from the beginning.

This white paper presents an overview of OpenVMS security and its role in enterprise business continuity.

The security problem

Information security breaches have made IT security one of the most important concerns for corporate and government IT environments. Security incidents reported to the CERT Coordination Center (CERT/CC) computer emergency readiness team rose 2,099 percent from 1998 through 2002 – an average annual compounded rate of 116%.

During 2003 alone, there were 137,529 incidents, up from 82,094 in 2002. Most of these incidents stem from software vulnerabilities. Such vulnerabilities can affect critical infrastructure, as well as commerce. Although new vulnerabilities increased only 5% in 2003, the vulnerabilities discovered were, and continue to be, more severe, more sophisticated and much easier to exploit.

Financial losses from unauthorized access to data and theft of proprietary information went up slightly in 2004 from 2003. In a survey conducted by the Computer Security Institute, 639 respondents reported that the average loss from unauthorized data access grew to $303,234 in 2004 from $51,545 in 2003. Also, average losses from information theft rose to $355,552 from $168,529. Total losses for those two categories were about $62 million. However, while corporate and institutional computer break-ins increased, average financial losses in other categories decreased.[1]

According to the 2005 CSI/FBI Computer Crime and Security Survey, virus attacks continue to be the source of the greatest financial losses. The survey determined that unauthorized access "showed a dramatic cost increase and replaced denial of service as the second most significant contributor to computer crime losses during the past year." Ironically, the survey also found that the percentage of organizations reporting computer intrusions to law enforcement has continued its multi-year decline because of "the concern for negative publicity."

Governments are well aware of the increasing threat to commerce and have enacted or are preparing legislation to require business attention to information security issues. The Sarbanes-Oxley legislation demands greater IT security of US corporations. In the healthcare industry HIPAA carries strict requirements and stringent penalties. And the EU has privacy laws that are among the most rigorous in the world.

With the flood of threats that occur on networks today that spread at computational speed, enterprises face a rapidly changing environment that demands an intense, proactive stance for dealing with information security. But are they serious about it? In the 2004 E-Crime Watch survey, Bob Bragdon, publisher of CSO magazine, writes: "The increase in e-crime over the past year again demonstrates the need for corporate, government and non-governmental organizations to develop coordinated efforts between their IT and security departments to maximize defense and minimize e-crime impact. There is a lot of security spending going on, but not much planning. It's essential for chief security officers and information technology pros to find the most manageable, responsive and cost-effective way to stop e-crime from occurring."

Achieving security

Achieving 100% impenetrable IT security is possible! To reach that goal, though, requires unplugging all IT components from the power grid, the network, and all peripherals. It is also necessary to lock all storage devices such as disks, tapes, flash cards, and so forth behind closed vault doors. This is, clearly, an unacceptable state for IT environments that are meant to add value to any enterprise's operations.

A more realistic goal is to make penetrating an IT environment as difficult as possible so that the probability of successful penetration is as low as possible. In addition, because 100% protection is not realistic, the second goal is to ensure that, if there is a breach, the offender can be rapidly identified and the nature of the intrusion fully documented. This needs to be accomplished at a cost that is tolerable based on the risk one is willing to accept. Steven W. Foster, Chief Security Officer of the Aegis Group and retired FBI agent, calls it achieving "optimal cost-effective risk mitigation."

[1] http://www.csoonline.com/metrics/view.cfm?id=834

From the outset, information security has to be placed within the context of the enterprise's total business continuity program and policies, including the physical environment, access, personnel, data security, contingency plans, drills or exercises, and so on. Yet all the IT security in the world won't do much good if an intruder can stroll unheeded into the computer room or extract a key password from a naïve employee through a bit of clever "social engineering." A strong analogy can be made between IT security and physical security. In its most extreme implementation, physical security consists of many layers, tests, confirmations, and keys. The chart below depicts a physical security approach with a number of components to protect the vital assets:

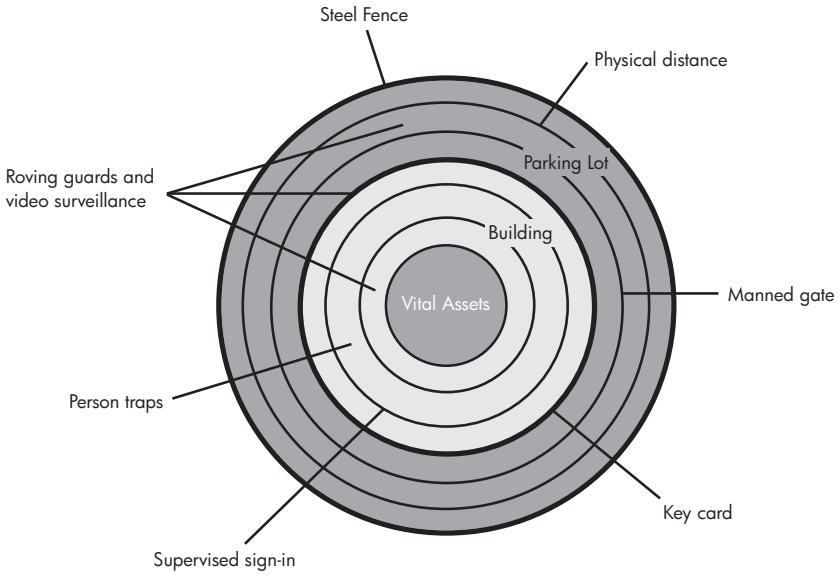
- The entire facility campus may be surrounded by a strong fence (first layer of protection to block intrusion).
- The parking lot is some distance from the facility (next layer providing a level of difficulty in getting quickly to the facility).
- Entry to the parking lot is protected by a manned gate (identification and verification prior to entry; also recording of who enters and when).
- Front door requires use of a key card (physical block and further record of who is where and when).
- Front desk requires sign-in and an access badge may limit areas to which the visitor has authorized access. An internal key card may also provide such limits (physical barrier and continuous privilege visibility).
- A person trap monitored by video may be employed in one or more locations to slow the progress of access and ensure the ability to stop an intrusion on checking.
- Roving security guards periodically challenge and check visitors for authorization.
- Strategically placed video surveillance throughout the facility and campus monitors and documents occupancy.

As depicted in the diagram there are multiple layers, a variety of checks, documentation points, and ways to limit access to specific areas. Each, though, carries some probability, however small, of being breached.

Because they are sequential and because each one is independent of the others, the probability of an intruder making it through all of these rings is exceedingly low. Should an intruder succeed in accessing a prohibited location there is still ample documentation of who was where and when. Therefore, even if the worst happens, the probability of quickly knowing of the breach, identifying the intruder, and taking remedial action is extremely high.

Now, making the leap from the physical to the virtual world, one can see that this is how OpenVMS security has worked from the first day it was offered.

Rings of physical security



OpenVMS – secure by design

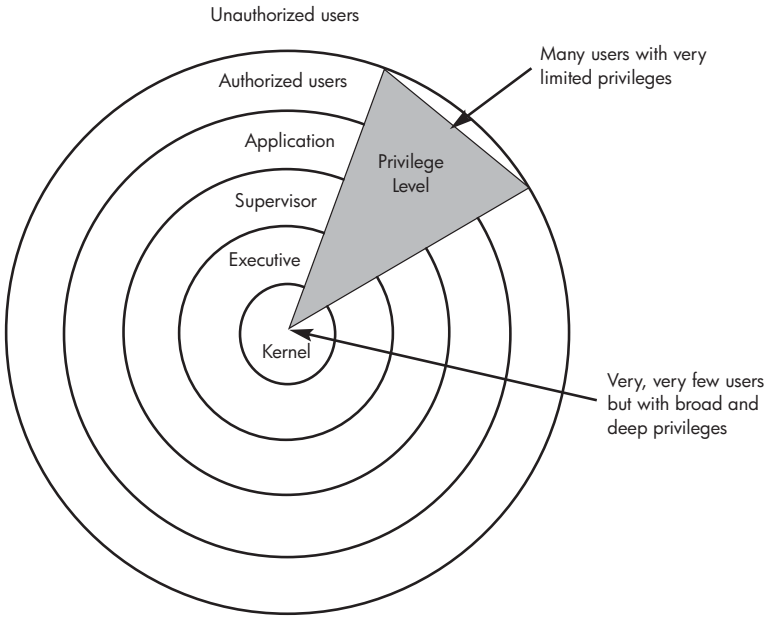
Security, at its core, is all about protecting data and transactions from unauthorized access and ensuring that data is available when businesses need it.

OpenVMS ships with an out-of-the-box default security architecture that provides "Rings of Protection" (chart shown) so that users and applications are granted the least amount of privilege needed to accomplish their tasks. In addition to the rings that are analogous to physical security as noted above, OpenVMS adds yet another dimension of locally exclusive access. A user, process, or device may have access to a particular layer for a specific purpose and still be excluded from access to all other levels for which privileges have not been granted. This provides even stronger assurance against such actions as back-door unauthorized access.

The system itself performs privileged tasks on behalf of a user or application without needing to grant the user that privilege. This design protects OpenVMS from viruses and similar attacks. Data protection extends across the whole system implementation from memory to disk storage to processor to I/O so that a flexible but secure system can be configured to meet the needs of any enterprise.

OpenVMS rings of protection

- Multiple layers – single domain
- Each layer requires its own privileges
- A breach in any one layer does not compromise any other layer



Installing OpenVMS without making any security parameter changes results in a secure environment with no default passwords or accounts with known passwords created. One of the first things that OpenVMS requests on installation is the identification of the installer and setting primary security parameters for the installer. If this is not done OpenVMS may be installed but no one and nothing at all will have access to it with the result that the installation will have to begin anew. This default was designed-in specifically to ensure that definitive security precautions are instituted from the very beginning of use.

The resulting system with established rings of security and the ability to monitor and identify users, even those with the most privileges, provides for an implementation of security policy that can be followed directly from the first moment of installation.

OpenVMS provides exceptional data confidentiality (protecting data from unauthorized access) with encryption tools and a default protection scheme that is secure and flexible.

OpenVMS has had security designed in – not bolted on – since it was first developed. At the core of the operating system is a security model that ensures that every single transaction on an OpenVMS system is audited and access is granted or denied by the security model.

OpenVMS provides a rich set of tools to control user access to system-controlled data structures and devices that store information. OpenVMS employs a reference monitor concept that mediates all access attempts between subjects (such as user processes) and security-relevant system objects (such as files). OpenVMS also provides a system security audit log file that records the results of all object access attempts. The audit log can also be used to capture information regarding a wide variety of other security-relevant events.

The OpenVMS security architecture and model apply equally to a single system in a computer lab or to an entire OpenVMS Disaster Tolerant cluster spread over hundreds of miles. In any case, each access will be audited and validated.

Password policy

User account information, privileges, and quotas associated with each user account are maintained in the system user authorization file (SYSUAF) under the control of the system manager. Each user account is assigned a user name, password, and unique user identification code (UIC). To log in and gain access to the system, the user must supply a valid user name and password. The password is encoded and does not appear on terminal displays. Users can change their password voluntarily, or the system manager can specify how frequently passwords change, along with minimum password length, and the use of randomly generated passwords.

For additional security, OpenVMS supports a dictionary to prohibit the use of actual words and a password reuse check to ensure that passwords are both unique and not reused for a specified length of time or a specified number of changes.

Security auditing

Auditing is the act of recording security-relevant activities as they occur on the system and the subsequent review/ analysis of the auditing log containing those activities.

This auditing information can be directed to security operator terminals (alarms) or to the system security audit log file (audits). Each audit record contains the date and time of the event, the identity of the associated user process, and additional information specific to each event. Successful and unsuccessful events alike can be recorded in the audit log file. Ironically, unsuccessful events are often more useful in revealing possible security concerns than monitoring successful access.

OpenVMS provides security auditing for events ranging from login failures and break-in attempts to abuse of individual privileges to system parameter changes.

Granularity of privilege

Every security-relevant system object is labeled with the UIC of its owner along with a simple protection mask. The system manager can, additionally, protect system objects with access control lists (ACLs) that allow access to be granted or denied to a list of individual users, groups, or identifiers. ACLs can also be used to audit access attempts to critical system objects and alert the system administrator when someone is attempting to gain illicit access to information.

Protecting information and communications

OpenVMS provides optional security solutions to protect information and communications with other systems within the infrastructure.

OpenSSL (Secure Socket Layer)

SSL (Secure Socket Layer) for OpenVMS is a version of the Open Group standard OpenSSL implementation. It provides encryption libraries and tools for OpenVMS and expands the existing 32-bit OpenSSL API library to include a 64-bit OpenSSL API library for development of secure TCP/IP connections.

Common Data Security Architecture (CDSA)

CDSA is a set of application programming interfaces that are used to encrypt data, store security certificates, and ensure the use of trust policies. It provides a platform-independent stable programming interface that developers can use to access operating system security services. It has become an Open Group standard for secure computing. OpenVMS is now building on this structure to deliver authenticated and validated software kit checking that will ship in the next release of OpenVMS, version 8.3.

CDSA is one of several security components on OpenVMS helping to ensure the integrity of applications. Because it is supported on different platforms it is especially useful in large multivendor environments.

Kerberos

Kerberos for OpenVMS, based on MIT Kerberos V5, is a network authentication protocol designed to provide strong authentication for client/server applications using secret-key cryptography.

Kerberos is available on OpenVMS and ships with the operating system. Kerberos V5 enables OpenVMS applications to accept Kerberos Tickets providing secure authenticated connections between OpenVMS and UNIX® or Windows® platforms with a single password. TCP/IP services for OpenVMS V5.3 accepts Kerberos authentication for Telnet and other services.

Per-thread security profiles

Per-thread security permits each thread of execution within a multi-threaded process to have an individual security profile. Per-thread security ensures that this security information is handled properly. Each user thread in a process has a fully separate security profile. When the user thread is scheduled, the security profile for that thread is automatically switched as well.

External authentication

External authentication allows users to log in (or sign on) at the OpenVMS login prompt using their external user IDs and passwords. The PATHWORKS and Advanced Server for OpenVMS authentication modules are supported as external authenticators, providing NT-compatible authentication of OpenVMS users. When successfully authenticated, the external user ID is mapped to the appropriate OpenVMS user name and the correct user profile is obtained.

OpenVMS security is part of a broader IT infrastructure

Earlier, the concept of levels of security was placed in the context of a multi-tiered computing infrastructure, including the recommendation that OpenVMS be used in the layers requiring the most robust security. It is important to understand that this is not only because OpenVMS is so secure, but also because OpenVMS is designed to integrate extremely well with the entire IT infrastructure. In addition to a considerable array of e-business infrastructure technology and tools, the OpenVMS operating system can be tuned to perform well in a wide variety of environments including combinations of compute-intensive, I/O intensive, client/server, real-time, and other environments. For users who are familiar with the UNIX shell and utilities, OpenVMS is providing an Open Source port of GNU's GNV – a GNU-based, UNIX environment.[2]

The OpenVMS security model continues to evolve to interoperate seamlessly in secure heterogeneous environments by supporting industry standard technologies.

[2] For more information on e-business infrastructure tools refer to: www.hp.com/go/openvms/ebusiness

[3] Information Security Defined (HP Handbook p.16)

Government security standards

OpenVMS is committed to consistently delivering a secure base operating system. An earlier version was evaluated and certified to be compliant with the DoD 5200.28-STD Department of Defense Trusted Computer System Evaluation Criteria. Since then, each release of OpenVMS must and does successfully complete the same test suite used to validate this C2 compliance to the National Computer Security Center before it is released.

Internal malice

In an OpenVMS system, the system manager controls everything and everything that happens is logged. If a system manager becomes the criminal element, he could delete the audit log to cover his tracks, but the very fact of a deleted audit log would, therefore, implicate the system manager.

An OpenVMS system can be set up so that even the system manager function needs two passwords to log in. So, with OpenVMS, the probability of external problems is virtually zero. And if a system manager acts internally, his malfeasance would be clearly identified. So the worst case of an "inside job" could not go undetected and the "secure by design" characteristics of OpenVMS support cost-effective risk mitigation.

HP, security, and OpenVMS

The objective of information security is to protect from harm the interests of those relying on information, and the systems and communications that deliver the information. Harm results from failures of confidentiality, integrity, and availability.[3]

While emerging definitions are adding concepts such as information usefulness and possession – the latter to cope with theft, deception, and fraud – the networked economy has added the need for trust and accountability in electronic transactions. HP implements security following the three main principals of security commonly known as CIA:

Confidentiality: Information is observed by or disclosed only to those who have a right to know.

Integrity: Systems and information are protected against unauthorized modification.

Availability: Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from failures.

OpenVMS provides the technical controls to augment the administrative and physical controls that need to be in place to secure information.

Business transactions as well as information exchanges between enterprise locations or with partners need to be trusted. This is known as authenticity and non-repudiation.

When developing a security policy for any security environment, the factors of governance, identity, management, and infrastructure need to be considered and included in a security plan.

Governance

Governance is about managing the risks associated with an organization's information assets aligning IT with business needs and objectives. In many organizations, industry best practices and government regulations drive the need for governance. A governance program contains logic, business procedures, and managerial and operational processes all supported by more specific, lower-level policies for IT operations and security. As we have seen, the OpenVMS operating system is admirably suited for implementing security policies around access and identity.

Identity management

Identity management includes the set of processes, tools, and social contracts surrounding the creation, maintenance, utilization and termination of a digital identity for people or, more generally, for systems and services to enable secure access to an expanding set of systems and applications.

From a technological and IT perspective, identity management is just one aspect of managing business solutions and the overall IT stack. Identity management must be considered in an holistic way by including (among other things) the management of security, trust, and privacy along with the management of policies, requirements, and changes. All these aspects are very interrelated and affect business solutions and the IT stack at different levels of abstraction.

Proactive security management

Proactive security management is an important and complementary part of IT infrastructure management and operations. The fundamental goal of this area is to make sure the mechanisms for protection are operating appropriately – during set-up, operation and decommissioning of various IT services.

Proactive security management has the capability to protect data, applications, systems and networks in the face of changing threat environments and changing business models. Proactive security management enables the vision of the HP Adaptive Enterprise by delivering policy-driven security management across the enterprise to prevent, detect, warn, log, and heal the effects of attacks, security policy violations, and other threats. The OpenVMS rings of protection enable very fine-grained and proactive security management.

For example, the out-of-the-box security defaults in OpenVMS represent one form of proactive security management. Unless privileges are granted during installation, the OpenVMS environment will be 100% inaccessible, even to the system manager doing the installation. The privileges that are established for the system manager during the install are logged, thus ensuring an auditable security environment from the instant of installation.

Another example is the OpenVMS password policy. First, the system prohibits the use of passwords that are commonly discernable. The operating system maintains a dictionary of prohibited passwords such as real words and previously used passwords. It also identifies and rejects simplistic character strings as passwords and requires passwords to be changed periodically. Second, passwords are level-specific and grant access only to those layers for which the user has privileges. And finally, as mentioned above, a password must be established on installation.

Trusted infrastructures

Trusted infrastructures are those infrastructures deserving of confidence in their support of the critical IT applications underlying the most critical business processes. They are able to adapt and protect themselves from an ever-increasing set of threats, often propagating at computational speed.

When IT infrastructure technologies fail to keep pace with emerging threats, they become distrusted in their ability to maintain a level of service necessary to sustain the applications depended upon by both business and society. Trusted infrastructures are a key focus area for HP and a hallmark of OpenVMS capabilities (please see "The DEFCON experience – cool and unhackable" on page 11).

Managing security

Corporate governance requires that assets be managed efficiently and are available to take advantage of new business opportunities as they arise. Without security, it is clear that this cannot be guaranteed. However, a company that does not ensure that it is flexible and adaptable cannot guarantee efficiency or the ability to react to new business opportunities. A company needs to be adaptable and it needs to be secure to ensure good corporate governance. This is not a choice. The road to corporate governance and compliance with regulations requires that security governance is demonstrable and that adaptability, as defined by the HP Adaptive Enterprise framework, is a reality.

As we have seen, OpenVMS security is easily managed as part of the standard system management tools. Therefore, the benefits of the highest security and adaptability are both available at the same time.

Maintaining security in the face of change

In today's changing environment, a successful security management solution must be able to adapt in a way that is cost-effective, efficient, and speedy. In addition to responding to evolving threats as described above, the security management system should enable business model and organizational change. You can imagine how painful a security management system would be that takes a year to integrate two merging companies or doesn't allow critical information to be shared between key partners to meet orders. These types of changes have direct implications for IT infrastructures, implications that must be addressed in an efficient, timely, and secure way. Therefore, the security management solution must be able to manage the protection of IT Infrastructures before, during, and after change.

Services

Building an Adaptive Enterprise in which business and IT are synchronized to capitalize on change requires a secure IT infrastructure. With "defense in depth" security safeguards — such as those available with the OpenVMS operating system — tightly integrated into Adaptive Enterprise solutions, customers enhance their ability to address risk management, cost containment, quality of service, and overall business agility.

The professionals at HP Services are uniquely equipped to help guard against security threats and, at the same time, streamline appropriate information access. HP has more than two decades of experience as a security provider for enterprises and government bodies around the world. It can help customers meet their short-term needs as well as long-term goals — from security training to policy definition, ethical hacking to solution design, platform hardening to implementing and managing a secure global infrastructure.

HP delivers a comprehensive approach with complete lifecycle services for designing, building, integrating, managing, and evolving sound security solutions, including:

Security planning and governance: Gauges security risks, defines security policies and governance structures, and prepares personnel for security implementations.

Trustworthy infrastructure: Establishes end-to-end IT security and implements appropriate technologies including data centers, networks, productivity tools, desktops, and wireless devices.

Identity and access management: Strengthens application-level security with advanced identity provisioning and policy-based access controls.

Security management: Provides a "single pane of glass" view that helps organizations respond to events and alerts in a timely manner.

Business and commerce enabling security: Helps organizations meet industry-specific security requirements.

Security education and training: Keeps personnel current with state-of-the-art practices and technologies.
More information is available at http://h20219.www2.hp.com/services/cache/10682-0-0-225-121.html.

Conclusion

Ultimately, how do you fight computer criminals? You fight them at the system and at the application. And you fight them with the right policies, privileges, and checks and balances. And since information security is only one aspect of total business continuity, physical security down to the locks on the doors must be addressed with the same intense, holistic, and proactive approach. It is system, network, and security people with the right tools that make the difference in the battle. It is the people who deploy the security policies and, ultimately, who have to monitor systems for security and intrusions.

Confounding the situation is the opening of business and organizational boundaries. With any combination of partnerships, mergers, dynamic supply chains, online customer services, federations and changing user populations, it is very difficult to draw a line where an organization's intranet stops and the Internet begins. The concept of "inside" and "outside" no longer holds true. And, indeed, the irony of this shift is that most attacks were typically mounted from within in the past, thus providing a degree of bounding for protecting, monitoring, and remediating.

This risk has not declined but what previously were considered low-probability external risks have been growing rapidly in number, intensity, and sophistication. In short, IT environments that require elevated security capabilities need OpenVMS, whether on HP Integrity servers, AlphaServer systems, or a combination of both, now more than ever.

The DEFCON experience – cool and unhackable

DEFCON is an annual computer underground conference for hackers held in Las Vegas, Nevada. Hackers from all over the planet attend to meet others into hacking, hang out with old friends, listen to speeches or just hack on the network.

An OpenVMS team (known as the Green Team) attended DEFCON9 to demonstrate the industrial strength and competitiveness of OpenVMS as a Web and application server and for mission-critical operations directly connected to the Internet without a firewall. The team's goal was to install an OpenVMS server, running Telnet, FTP, WEB and Personal WEB services and maintain availability and integrity during attacks to any of the previously mentioned services. It also needed to prevent hackers from gaining access to unauthorized files and consequently to avoid hackers from "Capturing the Flag."

The Capture the Flag contest is designed to emulate real world Internet security scenarios. The goal is for teams to compromise other teams systems and place a file "flag" in other teams' root directories.

After about 52 hours of playing, the DEFCON judges (a.k.a. Goons) placed a note in the Scoreboard file that said that the Green Team's OpenVMS box was "Virtually Unhackable" and that hackers might want to move on to another target.

The Goons pronounced the OpenVMS system "Cool" because in addition to being unhackable it had the best web content and services on the floor. They also noted that the OpenVMS system provided continuous service of those applications during the entire event despite all the hacking attempts. Thus the OpenVMS server came away from DEFCON9 with the title of "Cool and Unhackable." (Adapted from "Virtually Unhackable" DEFCON9: Securing OpenVMS with System Detective http://www.pointsecure.com/)

Refer to the following sources for additional security information and discussion.

www.hp.com/go/openvms/security

www.hp.com/go/security

http://h20219.www2.hp.com/services/cache/10682-0-0-225-121.html

www.cert.org

www.cve.mitre.org

www.us-cert.gov

www.issa.org

www.sans.org

The Black Book on Corporate Security, Larstan Publishing, Washington DC & Philadelphia, 2005

HP Security Handbook, Hewlett-Packard Development Company, 2004

For more information

To learn more about OpenVMS security, please visit
www.hp.com/go/openvms/security

To learn more, visit **www.hp.com**.

4AA0-2896ENW 11/2005

invent