



# The Financial Benefits of Mandatory Access Control Security

November 2007



## Executive Summary

The emergence of and growing dependency upon a global digital economy, that is central to transforming the delivery of services and related business processes in both the public and private sectors, is increasingly accompanied by serious threats posed by cyber crime.

Unauthorized access, viruses and spyware, and theft of critical and/or proprietary personal information is a threat faced by organizations of all types around the world, and especially by governments and financial institutions. The consequences for organizations affected by cyber crimes can include public embarrassment and a loss of confidence by clients, the potentially high cost of responding to the loss of proprietary data, as well as civil and sometimes criminal liabilities for regulatory violations.

Traditional methods of security, such as firewalls and electronic access controls, offer diminished effectiveness as organizations and systems resources become increasingly linked to provide high value services that cross traditional security boundaries. Shared-services environments are another growing area in which malicious intrusion has the potential for wide-spread damaging consequences.

In response to a challenge from the UK Cabinet Office, and in partnership with them and with Tresys Technology, an undertaking was made to provide a security model that can be tailored to meet exact, in-depth security requirements. Security breaches can be contained such that a breach in one area does not imply breaches elsewhere. This model is referred to as Mandatory Access Control (MAC) security.

Simply put, the primary and unique capability of MAC is the confinement that it provides. MAC security is designed to prohibit the escalation of unwarranted access privileges that are so common in software attacks today. MAC adds multi-layered access restrictions that are not subject to the discretion of users or administrators. MAC limits access to resources according to policies defined by the organization's security officer. Once installed and configured, the enforced MAC security rules remain constant.

The current standard infrastructure security model is referred to as Discretionary Access Control (DAC) security. DAC security restricts access to system resources based on user identity and the privilege assigned to each class of user. Under DAC, users 'own' system resources and grant access to them to other users at their (the 'owning' user's) discretion. Every program or system function that is invoked by that user runs with their privileges, including mail clients, web browsers, and any programs downloaded from the Internet.

MAC is an exciting innovation in security compared to the standard DAC model. With MAC, applications, not users, are assigned privileges and access. Users cannot change this permission.

But beyond the functional and assurance advantages of MAC security, is there financial value to be gained from implementing MAC security? To answer this question, IBM<sup>®</sup>, Tresys Technology, and Belmin Group Ltd performed an assessment and found that there is a potentially compelling financial benefit to be realized.

The results and details of this assessment are discussed in the pages that follow...

# Assessment Methodology

To assess the potential financial benefits of implementing a MAC security model vs. a DAC security model, we first defined a simple and hypothetical web-based transactional environment supporting a total of 250,000 external and internal registered users, with 20,000,000 transactions (writes to the database) per year.

MAC security is currently implemented on the Linux® platform and enabled through SELinux (Security Enhanced Linux), which is a flexible MAC technology included in the mainline Linux 2.6 kernel and fully supported by Red Hat from their Enterprise Linux version 4 and 5. SELinux is developed and maintained by the Open Source community, a community to which IBM makes a significant contribution of technical skill and code.

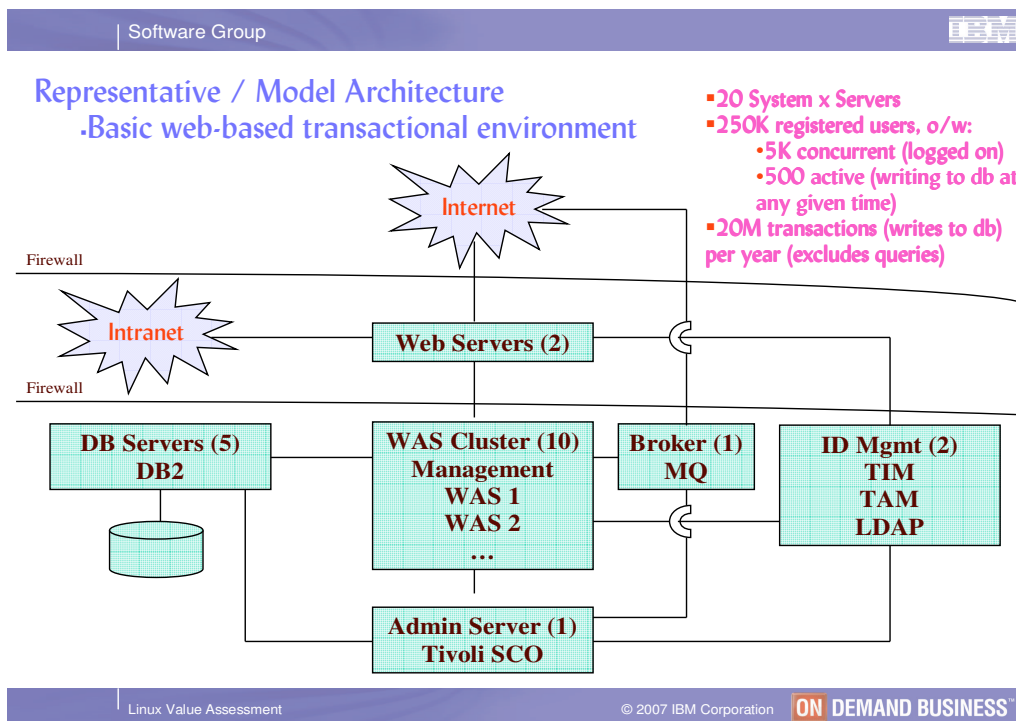
The same system environment of IBM WebSphere® software and IBM DB2® data servers running on Linux, together with IBM Tivoli® software, was used for both the MAC and DAC scenarios.

The financial assessment of the MAC and DAC scenarios includes the estimated up-front and on-going costs, over a three-year horizon, for three main areas of system infrastructure security:

- Security compliance and acceptance
- Security management (e.g. managing policies, monitoring, etc.)
- Vulnerabilities and critical security breaches

In addition, the incremental license and maintenance costs for Tresys Technology's Razor and Brickwall products, used to implement and manage the MAC security, are included.

The figure below shows the architecture of the simple, hypothetical web-based transactional environment used in this assessment:



# I. Security Compliance and Acceptance

Costs in this area were developed by first identifying the major tasks involved in the initial security compliance effort, and the efforts to re-comply with security requirements over the three-year period, of the system platform based on the model architecture.

The events that drive the need to re-comply (e.g. operating system patching), and their frequency, were also estimated. Assumptions regarding mitigation of these events under the MAC approach were based on analysis of CERT® Program Linux-based vulnerability reports for 2007 (through Sept 4, 2007) to determine the type of vulnerability and whether SELinux could be used to mitigate the vulnerability.

The full time equivalent (FTE) people resources to perform these major tasks were estimated under the MAC approach and under a standard DAC approach, and an estimated fully burdened rate of \$355/day was then applied to the FTE resource to determine the associated costs.

Among the major tasks included in the initial compliance effort are:

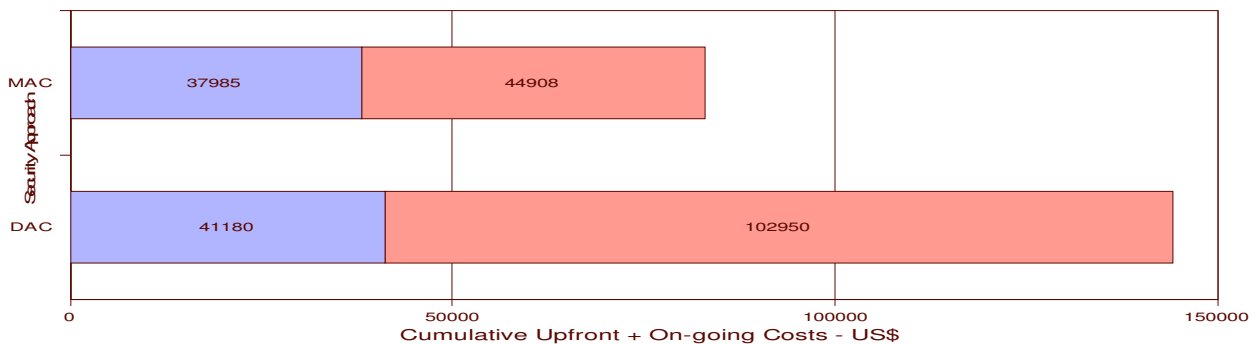
- Planning
  - System planning
  - System audit
  - System (hardware and software) and application installation
- Installation
  - System hardening
  - Functional and security testing
  - Analysis and problem resolution

The events that drive the need to re-comply include:

- Operating system patching (12/year)
- Application patching (4/year)
- Middleware patching (2/year)
- Critical / emergency patching (2/year)
- System upgrades (1 every 24 months)

## How MAC security helps:

- Mitigation of events that drive the need to re-comply (53% of CERT reported remotely exploitable vulnerabilities in daemon processes were mitigated by SELinux)
- Less time required for system hardening (policies, provided by Tresys Razor, can be applied which significantly reduce the need for script development, runs, healthchecks, etc.)



Note: These costs reflect FTE resource costs as described above and exclude license and maintenance costs for Tresys Technology's Razor and Brickwall products. Those license and maintenance costs are included in the graph on page 8.

## II. Security Management

Costs in this area were developed based on published security survey data and on analyst data<sup>1</sup> regarding the amount of time spent on activities such as patch management and security management in Linux environments. The analyst data was based on a survey that included over 200 respondents with Linux deployments, across a range of industries and enterprise sizes (from <20 servers to > 1000 servers), of the time they spend per server per week on these management tasks.

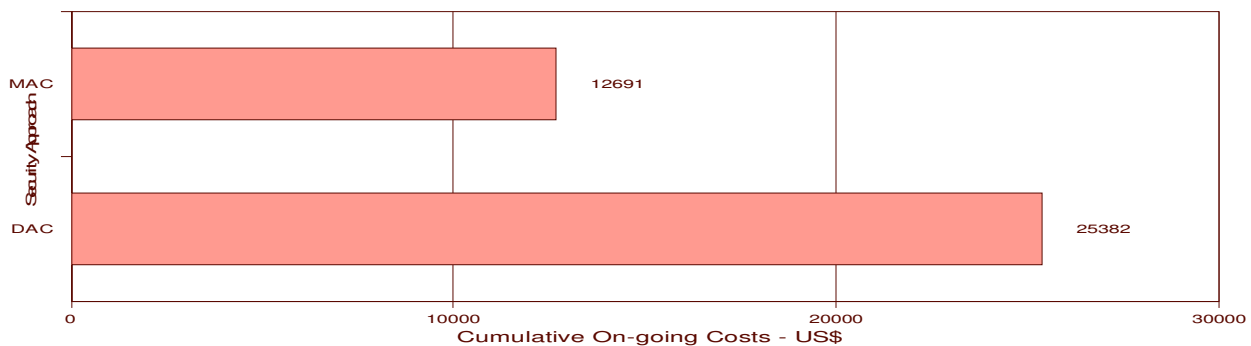
Security management tasks include:

- Policy management
- Security monitoring
- Spyware and virus management
- Security patching

The estimated time spent per server per week was converted to FTE people resource and an estimated fully burdened rate of \$355/day was applied to determine the associated costs per server. This value was then multiplied by the number of servers (20) in the hypothetical environment. An assumption regarding the mitigation of the estimated time spent performing these tasks under MAC security was based on the tasks included and estimates of the proportional amount of the time spent on those tasks.

### How MAC security helps:

- Less time required for policy management and security monitoring (once installed and configured, MAC security rules remain constant... even as additional resources are brought online, and the accuracy of security logs under MAC is reliable)



### III. Vulnerabilities and Critical Security Breach

Costs in this area were developed by first estimating the probability of experiencing the theft of proprietary data during the three-year assessment horizon. This estimate was based on the results of the 2007 E-Crime Watch survey<sup>2</sup> as released by CSO magazine and conducted with the U. S. Secret Service, Carnegie Mellon University Software Engineering Institute's CERT<sup>®</sup> Program, and Microsoft Corp. This survey covered the 12 month period from July 2006 – June 2007. Approximately 32% of all respondents experienced an e-crime during this period, with almost 13% of all respondents having experienced a theft of proprietary data including customer records, financial records, etc.

The major administrative tasks involved in handling an e-crime were identified, as well as the estimated FTE people resource to perform these tasks under the MAC approach and under the DAC approach. An assumption regarding the mitigation of the estimated time spent performing these tasks under MAC security was based on an assessment of tasks which would directly benefit from MAC functionality. An estimated fully burdened rate of \$355/day was then applied to the FTE resource to determine the associated costs under MAC and DAC security.

The cost involved in responding to a theft of proprietary data was developed based on an estimate of the number of individual records potentially compromised by a single theft multiplied by the cost per record to execute a proper breach response plan, then factored by the estimated probability of experiencing such a theft (10%) during the three-year assessment horizon. An assumption regarding the confinement and containment of the breach under MAC was based on the attacker being restricted, even in the event a 'zero-day' vulnerability, to only those resources permitted within the SELinux MAC policy. The estimate of individual records is based on a published report<sup>3</sup> of 250 data breaches last year, compromising the personal information of nearly 55 million people (an average of 220,000 per breach). The cost per individual record (\$12) used in this assessment is based on an actual case involving a U.S. financial services company. Both Forrester Research and Jonathan Penn have estimated the cost at \$15 per record.

Among the major administrative tasks included in the handling of an e-crime are:

- System take down / isolation
- Forensics – discovery of all resources affected
- Emergency fix / patch
- Monitoring for further attacks
- Functional testing
- System re-start / go-live
- Confirmation of system hardening
- Security testing
- Analysis and problem resolution

The activities and actions executed in a breach response plan include:

- External notifications to potentially affected persons, other interested parties, and as may be required by law
- Dedicated call centre and/or other arrangements to assist breach victims and answer queries
- Placement of fraud alerts on individual credit files at appropriate credit reporting agencies
- Offering of appropriate identify theft products

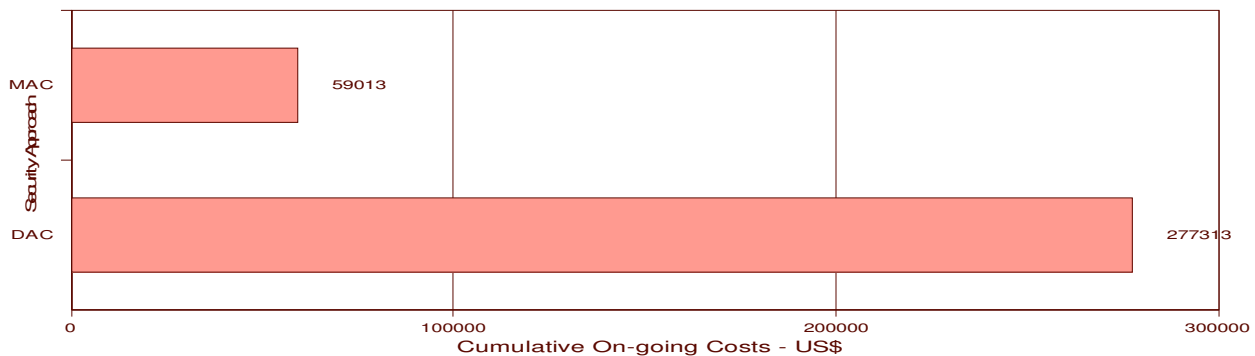
Note: Additional actions that may be required for some breaches, such as credit card replacement, are excluded from this analysis.

Additional factors used to estimate the cost of a critical security breach include:

- 1 critical security breach during the three-year assessment horizon
- 220,000 individual records affected if a critical breach occurs and personal proprietary data is compromised
- \$12 cost per individual record for the execution of a breach response plan
- 10% probability that the critical breach will result in the compromise of personal proprietary data and a breach response plan is required and executed
- The compromise of personal proprietary data is 80% confined / contained through the restrictions to system resources that are imposed on attackers through SELinux MAC policies

#### How MAC security helps:

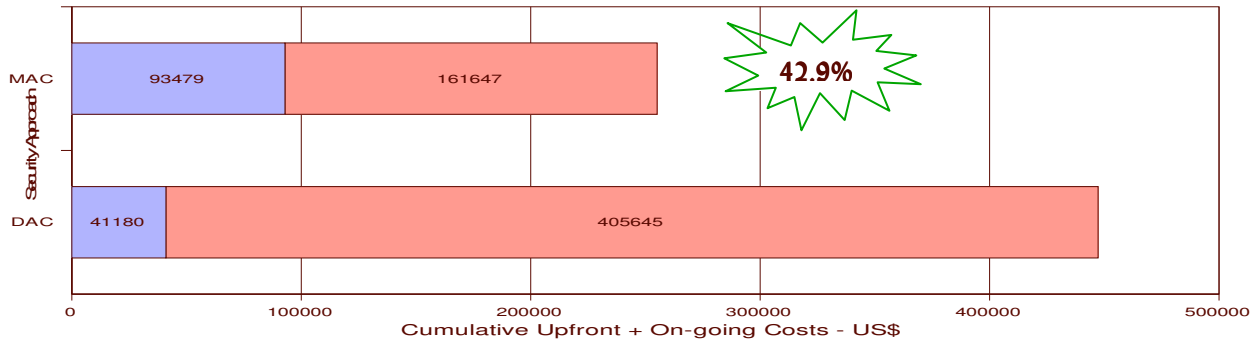
- Less time required for the forensics work to determine the system resources affected by a critical security breach
  - Reliability of security logs (virtually incorruptible by the attack) allows checks of system resources to be targeted at only the subset of resources affected
- Access to system resources is confined and contained by the SELinux MAC policies such that the resource restrictions imposed by the policies are virtually unbreakable by the vulnerable application or by the attacker
  - The benefits of this confinement and containment are easily multiplied when implemented in hosted / shared-services environments
  - This applies even in the event of 'zero-day' attacks



## Summary and Conclusions

Beyond the functional and assurance advantages of enhanced IT security, there is a potentially compelling financial benefit to be realized from the implementation of MAC security.

Over a three-year horizon, this assessment found that implementation of MAC security can provide financial savings of up to 43% in upfront plus on-going costs when compared to DAC security (excluding the potential revenue impact of unplanned downtime). The figure below shows the upfront costs and the on-going costs:



MAC security, as enabled by SELinux and currently implemented for IBM WebSphere and IBM DB2 by Tresys Technology's Razor and Brickwall products, is a unique and powerful capability that is widely available in a mainstream operating system for the first time ever – 'MAC for the masses'.

"We consider Mandatory Access Control to be a key enabling technology to aid government and businesses alike, in being confident they can deliver more services, more quickly and with better function, without compromising security."

-- Dr. Steve Marsh, Intelligence and Security Advisor, UK Cabinet Office

"SELinux is the culmination of over 35 years of operating system security research. For the first time we have MAC security available in a mainstream operating system in a form that is flexible enough to meet a wide range of security challenges."

-- Frank Mayer, Chief Technology Officer, Tresys Technology  
Co-author, [SELinux by Example](#)

Belmin Group Ltd is a leader in using MAC security to help drive high-value transformation of business processes and delivery of services for clients. Belmin Group's ARIES (automated reconciliation & invoicing) application replaces existing manual methods of invoice processing to reduce costs and increase efficiency.

"Security is paramount to Belmin and its users, who comprise many UK public sector organizations, including 94 NHS Trusts and a major UK Central Government Department. Belmin solutions currently process some £920 million per annum of sensitive UK public sector purchasing expenditure. The beauty of the SELinux implementation from our perspective as a solutions developer, was that when we enabled the extra security layer, nobody was aware that it was even running... To be able to apply such granularity of control without any detriment to service delivery is both progressive and compelling."

-- Richard Stoneman, Marketing Manager, Belmin Group Ltd

Notes: For more information regarding MAC and DAC security, please refer to the white paper “Enabling Government and Business Transformation with Mandatory Access Control Security,” jointly authored by IBM, Tresys Technologies, Belmin Group Ltd, and CSIA (Central Sponsor for Information Assurance), dated December 2006 and as may be updated from time to time.

IBM system servers, IBM WebSphere products, IBM DB2 products, IBM Tivoli products, and SELinux are available from and/or through IBM, and from partners where applicable. Tresys Technology’s Razor and Brickwall products are available from Tresys Technology ([www.tresys.com](http://www.tresys.com)).

<sup>1</sup> “Get the Truth on Linux Management,” Enterprise Management Associates (February 2006)

<sup>2</sup> Data is sourced / originates from CSO magazine, U.S. Secret Service, CERT® Program, Microsoft Corp.

<sup>3</sup> Chronology of Data Breaches published by PrivacyRights.org.

Prices for Tresys Technology’s Razor and Brickwall products are based on U.S. pricing, available upon request from Tresys Technology, and exclude applicable taxes. Prices subject to change.

The preceding report examines certain factors relevant to the cost and financial considerations of alternative forms of IT infrastructure security. It is only an estimate for information purposes only and relies on certain assumptions. It is not a statement of capacity, performance, suitability, or results. Actual cost and financial effects of implementation of either form of security will vary based on many factors. This is an estimate only and IBM does not guarantee its accuracy.

The information in this document concerning non-IBM products and/or services was provided by the suppliers of those products and/or services. IBM has not tested such products and/or services and cannot confirm the accuracy of the performance, compatibility or any other claims related to non-IBM products and/or services. Questions about the capabilities of non-IBM products and/or services should be addressed to the suppliers of those products and/or services.

IBM provides this report “as is” with no representations or warranties. IN NO EVENT WILL IBM BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL, OR OTHER CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS REPORT, INCLUDING WITHOUT LIMITATION, ANY LOST PROFITS OR SAVINGS EVEN IF IBM IS ADVISED OF THEIR POSSIBILITY.

IBM, the IBM logo, WebSphere, DB2, Tivoli, and System x are registered trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

© International Business Machines Corporation 2007

# Acknowledgements

(in alphabetical order)

## **Gordon Everett, Technical Director, Belmin Group Ltd**

Gordon has 25 years of experience in developing and maintaining application software running remotely, or as a locally hosted service. This includes his current work, with implementation, compliance, upgrades and maintenance, for Belmin's ARIES application, in use by the UK NHS, to ensure that system integrity and security is maintained whenever changes are made to the application, operating system or third party software.

## **Fred Logan, WW Program Director, Open Source and Linux, IBM Software Group**

Fred is a senior consulting sales specialist in IBM's Open Source and Linux software business. He works closely with governments around the world to help them understand and benefit from IBM and Linux open standards software and technology. Fred's previous roles in IBM have been focused on managing regional sales execution in Europe and North America.

## **Frank Mayer, Co-Founder, President, and Chief Technology Officer, Tresys Technology**

Frank has 23 years of experience in the research, design, and development of computer and network security technologies. Under his leadership, Tresys has become one of the industry's most trusted providers of high-end information security technology and engineering services. He is the chief architect of Tresys' extensive involvement in Security Enhanced Linux (SELinux), initiating numerous SELinux open source projects and products, and co-author of the definitive book on SELinux.

## **Ruby Qurashi, European Services Manager, Tresys Technology**

Ruby has over 17 years of experience across the areas of Internet security, go-to-market consultancy, technical sales, and marketing. Prior to coming to Tresys Technology, she held a variety of positions including VP Product Management for Security Solutions for MCI (now Verizon Business), and she helped launch two digital certificate vendors (Xcert International and E-Certify Corporation) into the enterprise marketplace.

## **Ian Robertson PhD, CEng, Sr Mng Consultant – Security & Privacy Practice, IBM Global Business Services**

Ian's key expertise and experience are in business process and IT architecture as a means of implementing secure applications that comply with standards for identity management and access control.

## **Spencer Shimko, Lead Security Architect, Tresys Technology**

Spencer develops security architectures for commercial, enterprise-level SELinux products with a focus on ease-of-use. He has also developed cross-domain solutions based on SELinux technology for use in multi-level security environments.

## **Graham White, Sr IT Specialist, Emerging Technology Services, IBM Software Group**

Graham works from the IBM lab in Hursley/UK, where he has garnered deep Linux skills in various areas for almost 8 years. One of Graham's major focus areas is to develop, set up, and proof security concepts of IBM Middleware on Linux as well as security concepts of the Linux operating system in general for IBM Business Partners and customers.

## **Hollis Wieruscheske, Sr Program Manager, WW Linux Business Development, IBM Software Group**

Hollis developed the methodology and process for the Linux Value Assessment (LVA), which is used in a consultative sales process to demonstrate to customers the potential financial benefits and value proposition of an IBM/Linux/open standards-based solution vs. other alternatives. Previously, he designed and implemented IBM's first-ever software volume licensing and subscription offering. He also held multiple financial management positions, including full IBM division-level responsibility.