The Impact of the DoD Mobile Code Policy on Advanced Distributed Learning, Web-based Distance Learning and other Educational Missions

Institute for Information Technology Applications and Advanced Distributed Learning CoLaboratory, Alexandria Test Report

Dr. Margaret E. Halloran, IITA; Dr. Jerry West, ADL CoLaboratory; Maj Gina Briggs, US Air Force Reserves; LtCol Moses Kamai, OASD (SO/LIC); Ms. Karen Keefer, ADL CoLaboratory; CMDR Jim Nugent, US Navy; Ms. Leslie McDade Morrison, DoD Chancellor's Office; Mr. Marty Salyars, Army Management Staff College; Mr. Neal Ziring, National Security Agency, and Ms. Susan Zuckerman, MITRE Corporation

30 August 2001

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 AUG 2001		**00-00-2001 to 00-00-2001**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Impact of the DoD Mobile Code Policy on Advanced Distributed Learning, Web-based Distance Learning and other Educational Missions	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Information Technology Applications,HQ USAFA/DFPS,2354 Fairchild Drive ,USAF Academy,CO,80840-6258**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**48**	

Executive Summary

Mobile code is software that downloads via the Internet and runs on users' workstations without the users' knowledge. Mobile code can be both potentially beneficial and harmful to systems and networks in the Department of Defense (DoD). The DoD Memorandum, dated 7 November 2000, *Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems,* establishes DoD-wide policy on the use of mobile code in DoD information systems and computers. The memorandum, also referred to as *the DoD Mobile Code Policy*, or just *the Policy*, defines mobile code and mobile code technologies as follows:

> **Mobile code** is defined (for the purposes of the Policy) as software obtained from systems outside the enclave boundary, transferred across a network, downloaded and executed on a local system (e.g., a computer with a Web browser) without explicit installation or execution by the recipient. **Mobile code technologies** are software technologies that provide the mechanisms for the production and use of mobile code (e.g., Sun Microsystems' Java and JavaScript; Microsoft Corporation's VBScript and ActiveX).

Many of the interactive components of web-based distance learning and Advanced Distributed Learning (ADL) are programmed using mobile code and mobile code technologies. In addition, distance learning and ADL often requires access to materials outside of the enclave as defined by the DoD Mobile Code Policy, as the course content or assignments of this instruction requires users to access web sites that are not developed and/or maintained by personnel within the DoD. For these reasons, ADL and web-based distance learning programs may be more sensitive to the DoD Mobile Code Policy than other base operations and a thorough test of the effect of the implementation of the DoD Mobile Code Policy is warranted.

In August, 2000 the Institute for Information Technology Applications (IITA) located at the US Air Force Academy conducted a series of Mobile Code Policy implementation tests that were deemed preliminary in nature and therefore limited in scope. Implementation guidelines were not available to test the policy in full; Active X was the only Category 1 code tested and there was no differentiation between signed and unsigned Active X code. In addition, due to the low rate of actual errors encountered, the 'surf team' became habituated to the procedure and it was difficult for them to keep on task. Therefore, not all pages in a URL were examined and some problems may have gone undetected.

Since August 2000, some of the configuration guidelines supplied by MITRE have been revised, and further guidelines were developed. Therefore, a more in-depth study of the Policy was warranted. In order to properly identify problems that are a result of the mobile code configurations, the Policy needed to be tested in a real-world environment per the baseline implementation guidelines (Configuration Guidance Volume 1). An automated web-crawler was used to reduce "surfer burnout" so that a more thorough

examination of the web sites were conducted. In addition, since more web sites supplied by the DoD educational community had problems than those sampled at random in the August 2000 testes, it needs to be determined whether that was a sampling anomaly or a reflection of the technology used by the educational community.

Requests for information on the types and frequencies of mobile code usage in the development of DoD web-enabled courseware were sent to points of contact at 51 DoD Academic agencies and 13 Learning Management System vendors. Eighteen surveys were returned, and only one-third of the respondents indicated that they used Category 1 mobile codes and only 27.8% of the respondents indicated that they used Category 2 mobile codes. None of the respondents indicated that they were using Windows Scripting Host or Unix Shell Scripting. Of the courseware contracted by the DoD, all of it would be permissible within the scope of the policy if it was signed with a DoD certificate or if it executed actions pre-installed on the browsers.

The gap analysis performed between the Mobile Code Policy and the Configuration Guidance supplied by MITRE indicates that the guidelines can be recommended as sufficient measures to comply with the Mobile Code Policy. The one area that could be improved upon is the time it takes to configure each workstation.

During our tests it took an average of 1 hour and 15 minutes to do the first workstation and an average of 40 minutes after the sequence had been repeated several times. In addition, during the evaluations the team had to learn the meaning of the additional warning prompt sequences that would appear on the screen. Therefore, we recommend that a streamlined method for configuring the workstations be written, which includes information for the user on the prompts that they might expect to see while accessing their online courses or supplemental material.

The web crawler examined a total of 2,203 host servers and 671,716 URL's. Of these, 204 host servers (4363 URL's) contained Active X and 430 host servers (12,804 URL's) contained Java applets. Due to practical time constraints it was not possible for the evaluation team to view all of the URL's that were identified by the web crawler as containing mobile code. The evaluation team examined 128 host servers, representing 3227 URL's that contained Active X. They also examined a minimum of one instance of every type of Active X program, identified by a unique code known as the Class ID. The evaluation team also examined 276 host servers, representing 10,522 URL's that contained Java applets. Of all the hosts and URL's examined by the web crawler and the human examination team, only 3 hosts contained content that could not be viewed due to the implementation of the Mobile Code Policy.

During this study, most of the Category 1 mobile code encountered executed functions that are pre-installed with the browser (e.g. Shockwave Flash) or was signed by a US certificate signing authority and most of the Category 2 mobile code did not operate outside of the sandbox on the client workstation; therefore both of these were not impacted by the Policy. Furthermore, during this study we found only three impediments attributable to the policy after approximately 192 man-hours engaged in a targeted search

from a list of URL's known to contain mobile code whereas most users would encounter mobile code or mobile code technologies only a few times if at all while taking an online course or doing research using supplemental course materials.

Therefore, if the Mobile Code Policy is implemented as recommended by the Configuration Guidelines supplied by MITRE, we expect the impact to the learner, ADL programs and web-based distance learning to be minimal.

Table of Contents

Page number

Executive Summary……ii

1. Introduction 3
- 1.1Background 3
  - 1.1.1 DoD Mobile Code Policy 3
  - 1.1.2 Potential impact of the policy on distance learning and ADL initiatives 4
  - 1.1.3 Previous tests conducted to evaluate the impact of the Policy on education 4
  - 1.1.4 Why further tests were needed 5
- 1.2 Purpose 5
- 1.3 Points of Contact 6

2 Study Overview and Methodology 6
- 2.1 Determining the impact of the policy 6
- 2.2 Goals of this Study 7
- 2.3 Gap Analysis 8
- 2.4 Documenting the frequency with which mobile code is used in web-enabled courseware programming 8
- 2.5 Courseware Evaluation Test Methodology 8
  - 2.5.1 Scenarios to be tested 8
  - 2.5.2 Limitations of the test 8
  - 2.5.3 Courseware sample 9
  - 2.5.4 Types of files to test 9
  - 2.5.5 Use of automated web crawler to do preliminary examination of web sites 10
  - 2.5.6 Computer configurations 10
  - 2.5.7 Procedure for manually checking courseware 13
  - 2.5.8 Measures of problem severity 13
  - 2.5.9 Problem diagnostic 13
  - 2.5.10 Data analysis 14

3 Results and Analysis 14
- 3.1 Gap Analysis 14
- 3.2 Use of Mobile Code by DoD educational agencies 15
- 3.3 Web-based courseware evaluations 15
  - 3.3.1 Mobile code policy implementation problems 16
  - 3.3.2 Category 1 Mobile Code 17
  - 3.3.3 Category Two Mobile Code 17
  - 3.3.4 Browser specific problems 17
  - 3.3.5 Guardnet problems 18

4 Interpretation and conclusion 19

5 Acknowledgements 20

Appendices
Appendix A – Mobile Code Policy 21
Appendix B – Questionnaire on Mobile Code usage by DoD 22
Appendix C – Data collection forms 24
Appendix D – GAP Analysis 25
Appendix E – Sample output from web crawler 40
Appendix F – Compiled problem log 42

1 Introduction

1.1 Background

1.1.1 DoD Mobile Code Policy

The DoD Memorandum, dated 7 November 2000, *Policy Guidance for Use of Mobile Code Technologies in Department of Defense (DoD) Information Systems*, establishes DoD-wide policy on the use of mobile code in DoD information systems and computers. The memorandum, also referred to as *the DoD Mobile Code Policy*, or just *the Policy*, defines mobile code and mobile code technologies as follows:

> **Mobile code** is defined (for the purposes of the Policy) as software obtained from systems outside the enclave boundary, transferred across a network, downloaded and executed on a local system (e.g., a computer with a Web browser) without explicit installation or execution by the recipient. **Mobile code technologies** are software technologies that provide the mechanisms for the production and use of mobile code (e.g., Sun Microsystems' Java and JavaScript; Microsoft Corporation's VBScript and ActiveX).

The DoD Mobile Code Policy only applies to mobile code obtained from sources outside the user's own enclave. The Policy does not apply to use of mobile code downloaded from within the confines of an enclave or preinstalled on a user workstation. An enclave is defined as *an information system environment that is end-to-end under the control of a single authority and has a uniform security policy, including personnel and physical security*. Enclaves can be specific to an organization (e.g., base, post, camp, or station) or a mission (e.g., Global Command and Control System (GCCS)) and may also contain multiple networks. They may be logical, such as an operational area network (OAN), or be based on physical location and proximity. As a standard, the enclave typically starts and ends at the premise router. For the purposes of the Policy, component domains with assured security boundaries can be treated as a single enclave.

In summary, the Mobile Code Policy defines three categories of mobile code technologies:

- Category 1 technologies pose a severe threat to DoD operations. The high risk associated with the use of Category 1 technologies outweighs almost all possible benefits. However, the implementations of some mobile code technologies differentiate between signed and unsigned mobile code, and these implementations can be configured to allow the execution of signed mobile code while simultaneously blocking the execution of unsigned mobile code. Risk is reduced when Category 1 mobile code is signed.
- Category 2 technologies pose a moderate threat to DoD information systems. The use of Category 2 technologies, when combined with prudent countermeasures against malicious use, can afford benefits that outweigh their risks.

- Category 3 technologies pose limited risk to DoD systems. When combined with vigilance comparable to that required to keep any software system configured to resist known exploits, the use of Category 3 technologies affords benefits that outweigh the risks.

The full policy is reproduced in Appendix A. In addition to the policy itself, a companion document, the *Configuration Guidance for Client Workstations, Applications, and Firewalls To Implement the DoD Memorandum on Use of Mobile Code* addresses specific implementation instructions for common platforms and software packages. It is commonly referred to as the Mobile Code Configuration Guidance or Implementation Guidance.

1.1.2 Potential impact of the policy on distance learning and ADL initiatives

Distance-learning (DL) is any formal approach to learning in which the majority of the instruction occurs while the educator and learner are at a distance from each other. Although several forms of distance learning have existed for many years, including print-based correspondence courses and video-based training, the internet has drastically increased the use of distance learning and often increased the quality of the instruction. In recent years, the Air Force, Army, Navy and Marines have all begun significant DL initiatives and the Office of the Under Secretary of Defense for Personnel and Readiness has produced the Department of Defense Strategic Plan for Advanced Distributed Learning (ADL). This document sets forth a strategy for providing instruction across the DoD to maintain military readiness in the information age. Such instruction must be distributed (structured without the physical presence of an instructor), available to learners on demand, and use appropriate technologies and media (e.g. CD ROM, world wide web).

One reason use of the world wide web can increase the quality of distance learning instruction is that it affords an element of interactivity that can not be duplicated in print-based instruction. Many of these interactive components are programmed using mobile code and mobile code technologies. Distance learning and ADL often requires access to materials outside of the enclave as defined by the DoD Mobile Code Policy. Often, the course content or assignments of this instruction requires users to access web sites that are not developed and/or maintained by personnel within the DoD. For example, the Air Force Language Link Russian Maintenance course uses Russian journalism sites to provide the Russian linguist students real-world examples in their reading and listening skills lessons. Instructors at many resident programs including the United States Air Force Academy often use non-DoD web resources for teaching and research. For these reasons, distance-learning programs may be more sensitive to the DoD Mobile Code Policy than other base operations and a thorough test of the effect of the implementation of the DoD Mobile Code Policy is warranted.

1.1.3 Previous tests conducted to evaluate the impact of the policy on education

On 30 July to 2 August, 2000 the Air Force's Institute for Information Technology Applications (IITA) located at the US Air Force Academy examined 224 unique URL's

for a total of 1181 web pages with 23 different types of mobile and non-mobile code files. The URL's consisted of courseware produced by the DoD, university (.edu) web sites, commercial courseware and other web sites. A total of 12 problems attributable to the mobile code configuration were documented, or 5.3% of all URL's. Of the 40 sites recommended by the DoD educational community, 9 (22%) had problems attributable to the mobile code configuration; 6 were not usable when viewed with Internet Explorer and 3 were not usable when viewed with Netscape.

However, each of the 9 sites could be viewed using the alternate browser. For example, if a site could not be viewed with Netscape, it could be viewed with Internet Explorer and the reverse was also true. The ability or inability to access information due to the mobile code policy implementation configurations was uniform across all browser and operating system versions; Internet Explorer 5.0 produced the same results as Internet Explorer version 5.5. In addition, we did not find any problems accessing non-mobile code resources on the test computers using the configuration guidelines supplied by MITRE.

Unfortunately, the tests performed were preliminary in nature and therefore limited in scope. Implementation guidelines were not available to test the policy in full. Active X was the only Category 1 code tested and there was no differentiation between signed and unsigned Active X code. In addition, due to the low rate of actual errors encountered, the 'surf team' became habituated to the procedure and it was difficult for them to keep on task. Therefore, not all pages in a URL were examined and some problems may have gone undetected.

1.1.4 Why further tests were needed

Some of the configuration guidelines supplied by MITRE for the August tests have been revised, and further guidelines have been developed. Therefore, another test of the Policy was warranted. In order to properly identify problems that are a result of the mobile code configurations, the Policy needs to be tested in a real-world environment per the baseline implementation guidelines (Configuration Guidance Volume 1). Measures need to be taken to reduce "surfer burnout" so that a more thorough examination of the web sites can be conducted. In addition, since more web sites supplied by the DoD educational community had problems than those sampled at random, it needs to be determined whether that was a sampling anomaly or a reflection of the technology used by the educational community.

1.2 Purpose

This document is a report on the impact of the DoD Mobile Code Policy on ADL, distance learning, and residential DoD education, using the implementation guidance supplied by MITRE. This report will be distributed to the Mobile Code Working Group to review and forward to the MCEB Information Assurance Panel for use when the policy comes under review in November, 2001.

1.3 Points of Contact

IITA, the ADL CoLaboratory in Alexandria, Virginia and the Total Forces Advanced Distributed Learning Action Team (TFADLAT) Working Group on Mobile Code Issues have produced this study jointly. Primary points of contact for this study are:

Margaret E. (Peg) Halloran, Ph.D.
Director of Educational Technology
Institute for Information Technology Applications
2354 Fairchild Dr. Suite 4K25
US Air Force Academy, CO 80840
Phone: (719) 333-8325 DSN 333-8325
FAX: (719) 333-4355 DSN 333-4255
peg.halloran@usafa.af.mil

Jerry L. West, D.Sc.
Technical Director
Advanced Distributed Learning Co-Laboratory
1901 N. Beauregard St. Suite 106
Alexandria, VA 22311
bus. (703) 575-4346
fax (703) 575-4370
west@adlnet.org

2 Study Overview and Methodology

The Institute for Information Technology Applications (IITA) and the Advanced Distributed Learning CoLaboratory (ADL CoLab) conducted a study of the impact of implementing the DoD Mobile Code Policy on DoD educational missions including distance learning and ADL. The study consisted of three components including a gap analysis of the policy and the configuration guidelines supplied by MITRE, circulating a questionnaire to query developers on the use of mobile code and performing a set of evaluations on existing courseware at the ADL CoLab from 18 to 22 June 2001.

2.1 Determining the impact of the policy

The impact of the policy was determined by the probability of a learner accessing an educationally relevant site that contains mobile code coupled with the probability of the material not being useable due to implementation of the mobile code policy.

Simply stated, the impact was calculated as:

Impact = P(educationally relevant content with mobile code) x P(content not usable due to mobile code configuration).

Many things determine each of these probabilities. For example, the probability of a learner accessing a site with mobile code will be dependent upon the frequency

educational materials that contain mobile code are assigned to the learner. The probability that the presence of mobile code on the site deems the material unusable, will depend on whether the mobile code is signed, whether it comes from a trusted source, whether the mobile code is superfluous to the content of the course, and whether the web site has been dual-programmed to use different codes by different browsers.

Therefore, to properly gauge the impact of this policy on the distance learning (or other educational) community, course resources were pulled from a sample of relevant courseware and learning materials and tested in a real-world scenario. If the materials could not be accessed, the reasons were documented as to the cause (not signed, not viewable with Netscape, could not download viewer etc.) so that problems can be properly identified and recommendations for the minimization of the impact of the policy could be made, when possible.

Not all problems accessing educational courseware web sites are due to the mobile code client configurations. Problems with adequate bandwidth, proxy filters etc. may also interrupt the ability of the learner to access educational resources. These problems should not be confounded within the impact of the mobile policy itself, but were documented as part of the diagnostic procedure for mobile code policy implementation issues.

2.2 Goals of this Study

IITA and the ADL CoLab implemented the policy on workstations behind a firewall supplied by DISA and configured to generic DoD specifications at the ADL CoLab to assess the impact of the DoD Mobile Code Policy on distance learning and ADL using a variety of real-world scenarios. In addition a gap analysis was conducted to determine if the configuration guidelines can be used to implement the policy, and a questionnaire was circulated to query developers on the use of mobile code in developing software. The goals of the study in order of priority were to:

1. Analyze the impact of implementing the Mobile Code policy on ADL, web-based distance learning, and resident DoD educational missions.
2. Test the effectiveness of the June 2001 version of the Mobile Code Configuration Guidance in blocking or inhibiting malicious mobile code.
3. Identify potential gaps between the Mobile Code Configuration Guidance and the requirements of the Mobile Code Policy
4. Identify possible improvements to the Mobile Code Configuration Guidance that may be used to meet the intent of the Mobile Code Policy while minimizing impact on operations.
5. Document other network configuration impediments to ADL, distance learning and education that are discovered as a result of these tests.
6. Estimate the frequency with which a DoD learner accesses courseware or other educational materials, which contain mobile code programming essential to the content of the course.

2.3 Gap Analysis

Mr. Marty Salyars of the Army Management Staff College conducted a GAP Analysis study between the Policy and the Configuration Guidance. This analysis was conducted in two phases. Phase one was the configuration guideline interpretation of the policy, and phase two was the configuration guideline implementation of the policy. The analysis for both phases was based on 1) reviewing the policy and configuration guideline, 2) interviewing an Information Management Officer, programmer, system administrator, and webmaster, and 3) completing the step by step configuration procedures using Windows 95 with Netscape, IE 4.0, Windows 98SE with Netscape, IE 5.0, and NT 4.0 with Netscape, and IE 5.5.

2.4 Documenting the frequency with which mobile code is used in web-enabled courseware programming

Questionnaires were distributed to learning management system courseware vendors and academic departments from the service academies, professional military education schools, training commands, and other educational missions to query them on the types of programming languages that they use to develop courseware (Appendix B).

2.5 Courseware Evaluation Test Methodology

2.5.1 Scenarios to be tested:

The tests were performed in the ADL CoLab and used two separate networks. The setup was designed to duplicate real-world scenarios encountered by DoD employees, including the use of course material (e.g. Air Force Language Link software) that requires users to access non-DoD web sites. The scenarios tested were as follows:

1. Course content hosted on a DoD server and accessed by a DoD system/client across an enclave.
2. Course content hosted on DoD server, accessed by a DoD system/client through a commercial ISP.
3. Course content hosted on a non-DoD server (e.g. University course offering) and accessed by a DoD client.

2.5.2 Limitations of the Test

However, the results of the tests are limited in the following ways:

1. Only guidance for PC based machines is available, therefore Unix Shell Scripts were not tested.
2. For Category 2 Mobile Code, Public Key Certificate over a Secure Socket Layer was the only “trusted source” or “assured channel” deemed acceptable for data collection purposes during this test.
3. There are currently no DoD approved PKI code signing certificates, therefore commercial certificates will be used for testing.
4. SIPRNET connected workstations were not tested.
5. Emerging technologies policy were not tested.
6. PerfectScript, LotusScript were not tested.

2.5.3 Courseware sample:

To obtain an adequate and valid sample for testing, personnel within the DoD educational community were emailed and asked to submit URL's for courseware with interactive or multimedia components that are required or recommended as part of the curriculum. The URL's included DoD courseware, civilian academic courses and commercial courseware sites. Participants included academic departments from the service academies, professional military education schools, training commands, and other educational missions.

2.5.4 Types of files to test

It is important to determine if reconfiguring the client workstations per the Configuration Guidelines will have any carryover effect and unintentionally block other types of files. Therefore the ability to access files with mobile code and files without mobile code will be checked. Files with the following types of code were accessed during this test:

Mobile codes

Category 1:

- Active X (signed and unsigned)
- Windows scripting host
- DOS batch scripts

Category 2:

- Java applets and other Java mobile code
- VBA
- Postscript

Category 3:

- Javascript (embedded and stand alone)
- VBScript (embedded and stand alone)
- PDF
- Shockwave/Flash

Non-mobile codes

- HTML
- XML
- non mobile Java code
- SMIL
- Quicktime
- VRML
- Real media including Real Player and Real Audio
- .avi
- Authorware w/Attain Objects
- midi
- .mp3
- .bat
- Office files that do not contain mobile code applications
  - Word, PowerPoint, Excel
- Active Server Pages
- Learning and course management systems

2.5.5 Use of automated web crawler to do preliminary examination of web sites
To reduce the habituation of human testers, an automated web crawler was used to search the contributed URL's for mobile code and interactive courseware components. Human observers reviewed those sites that contain mobile code according to the procedures outlined in section 2.5.7 below.

2.5.6 Computer configurations:
Two separate networks and test scenarios were used, a DoD simulated test bed and the National Guard's Guardnet. A diagram of the testbed configurations is found in Figure 1. All courseware was tested with both scenarios. The following systematic approach was used to set up each test and control workstation in both the simulated test bed and Guardnet prior to testing courseware:
1. Cookies, caches and histories were deleted from the browser.
2. Registry files were saved.
3. The ability of mobile code to pass through the firewall was verified by accessing a test website (http://users.erols.com/ziring/mctest) with known mobile code applications on each test workstation and control.
4. Test and control workstations were configured as outlined below:

A. DoD test network:

Test configuration – Test workstations were configured per June 2001 Configuration Guidance sections 2-4 (Table 1). Firewalls were supplied by DISA and configured to a standard DoD configuration allowing mobile code to pass through the firewall. Client test workstations included Windows '98 and NT operating systems, and the two latest versions of Netscape and Internet Explorer.

Workstation #1

Windows 98, Internet Explorer 5.5, Netscape 4.7

Workstation #2

Windows NT, Internet Explorer 5.0, Netscape 4.6

Workstation #3

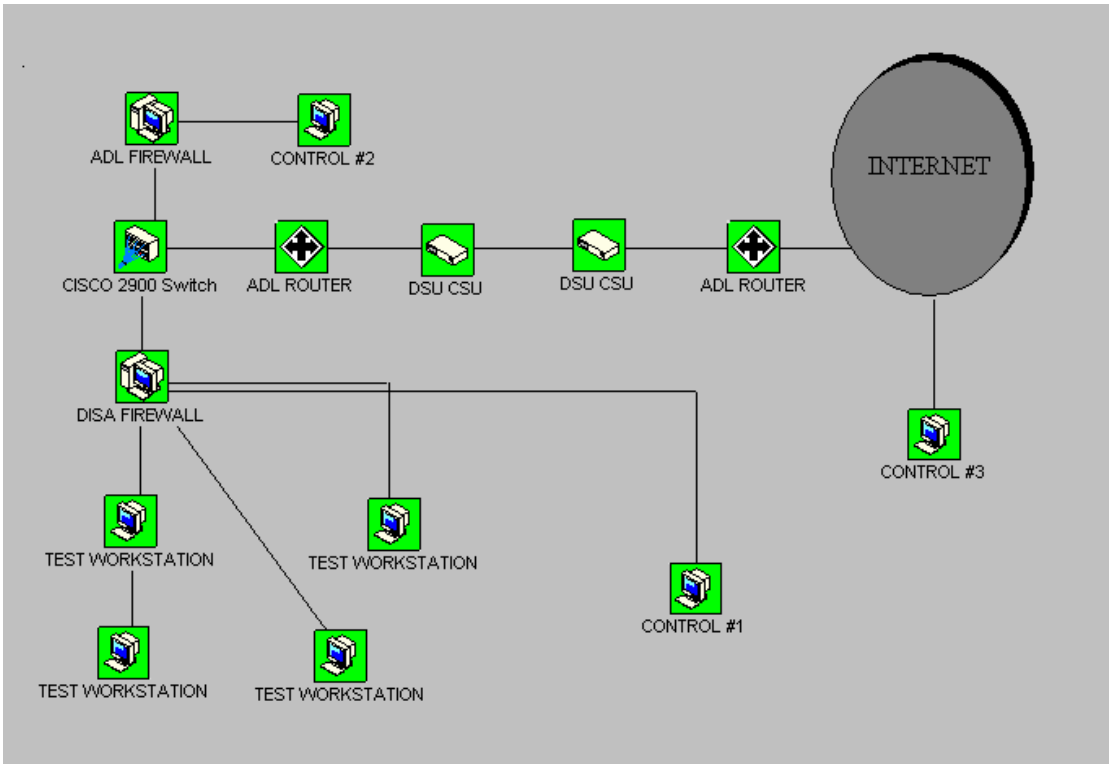
Windows NT, Internet Explorer 5.5, Netscape 4.7

Workstation #4

Windows NT, Internet Explorer 5.5, Netscape 4.6

Control #1 – This control was configured to default browser specifications to allow mobile code and located behind the firewall supplied by DISA. This control was used to determine whether inability to access a specific resource was due to a proxy, firewall, or other factor intrinsic to network, rather than the mobile code configuration. This control was confgured with Windows NT, and had Internet Explorer 5.5 and Nestscape 4.7.

Figure 1: Diagram of the ADL CoLab testbed configuration.



Control #2 – This control was configured per June 2001 Configuration Guidance sections 2-4, but was located outside the firewall supplied by DISA. It was located behind a separate firewall, which did not filter any content or mobile code. If the DISA firewall or other base configuration factors (e.g. bandwidth issues) were blocking access to a site, this configuration could check to see if access to the information was also blocked due to mobile code. This control was configured with Windows NT, Internet Explorer 5.5 and Netscape 4.7.

Control #3 – This control was configured to default browser specifications to allow mobile code and was connected to the internet via a commercial internet provider service (erols.net). This control was used to validate remote server accessibility independent of any problem with proxy or firewall configurations. This control had Windows 98, Internet Explorer 5.0, and Netscape 4.6.

B. National Guard Guardnet test network:

Test configuration – Test workstations were configured per June 2001 Configuration Guidance sections 2-4 (Table 1). Firewalls were supplied by Guardnet and allowed mobile code to pass through. Client test workstations included standard Guarndnet software of Windows ’95 and Internet Explorer 4.0 only.

Control #1 – This control was configured to default browser specifications to allow mobile code and located behind the Guardnet firewall and accessed through a NIPRENET connection. This control was used to determine whether inability to access a specific resource was due to a proxy, firewall, or other factor intrinsic to network, rather than the mobile code configuration. This control included standard Guarndnet software of Windows '95 and Internet Explorer 4.72 only.

Controls #2 and #3 – these were the same as for the DoD testbed.

5. Control and test workstation configurations were verified using the test website with known mobile code applications.

Table 1: Mobile Code Configuration Guidelines used in these tests. (Numbers are cross-referenced to sections within the configuration guidelines)

Workstation Configuration Guidance for Category 1 Mobile Code Technologies
2.1.1 ActiveX Controls and Netscape Communicator
2.1.2.2 ActiveX Controls and Microsoft Internet Explorer 5.x
2.2.1 WSH and Windows
2.2.2 WSH and Netscape Communicator
2.3.1 MS-DOS Batch Script Files and Windows
2.3.2 MS-DOS Batch Script Files and Netscape

Workstation Configuration Guidance for Countermeasures for Mobile Code in Email Messages and Attachments
3.3 Email and Netscape Communicator 4.0
3.4 Email and Microsoft Outlook Express
3.5 Email and Microsoft Outlook 98
3.6.2 Disable Mobile Code in IE 5.x
3.9 Enable User Prompts Prior To Opening Email Attachments
3.9.1 Enabling Prompts Via Windows File Types
3.9.2 Enabling Prompts Via Netscape Communicator 4.0 File Types

Workstation Configuration Guidance for Using Category 2 Mobile Code Technologies
4.1.1 Java Applets and Netscape Communicator 4.0
4.1.2.2 Java Applets and Microsoft Internet Explorer
4.2.1 VBA and Microsoft Office 97
4.2.2 VBA and Microsoft Office 2000
4.5 Configuration Guidance for Using PostScript
4.5.1 Enable Warnings before Opening PostScript Files in Windows
4.5.2 Remove PostScript File Type Recognition From Netscape Communicator
4.5.3 Enable the Safer Mode in Ghostscript and GSView

2.5.7 Procedure for manually checking courseware:

Seven observers manually checked courseware web pages 19-22 June 2001 that had been identified by the web crawler as containing mobile code. Included in this group were representatives from the ADL Co-Lab, Navy, Air Force, MITRE and National Security Agency (NSA). Each observer was assigned a specific set of hosts and was instructed to sample a representative number of URL's from each host. Some hosts only had a few URL's with mobile code so all were examined for that host, but for those hosts that had hundreds of URL's the evaluators were instructed to only sample every tenth page or pages that contained unique code. Observers were also given a list with the Active X class ID's so that they could determine whether the same programming was being used repeatedly. Unfortunately, this information was not available for the pages with Java.

Pages were observed in Internet Explorer 4.0, 5.0 and 5.5 and Netscape 4.6 and 4.7. Any pages that appeared to be missing information or that were behaving differently in Netscape and IE were logged on a data collection form (See Appendix C), along with the nature of the problem and the severity. Sites with problems were then checked with the control workstations to determine it the error was due to a mobile code configuration or other anomaly. Problems were reviewed by the test director using a decision matrix (Table 2) and further diagnosed and verified by a representative from MITRE and/or NSA.

Some sites had certificates that needed to be approved by the Chief Information Officer (CIO). Ms.Susan Zuckerman and Mr. Neal Ziring acted as the CIO for the purposes of this study. The criteria used were that the certificate had to be issued by a United States company (e.g. Verisign, Excert, Entrust) and be hosted on a server within the United States.

2.5.8 Measures of problem severity

The observers were instructed to rate the severity of the problems they encountered with their inability to access information. The rating scale is:

A. Severe - document could not be viewed, information could not be accessed

B. Moderate – caused a negative change in the way content relevant information was displayed

C. Minor – fixable or work-around by user, cosmetic change in display of content relevant information

2.5.9 Problem diagnostics

To isolate and diagnose any problems in viewing courseware that may be a result of the test configuration, any courseware that appeared to have a problem with the way information was displayed was checked with a series of control computers. A decision matrix (Table 2) was used to assess the outcome of accessing the course materials with the test and control computers.

Table 2: Decision matrix used to determine if problem was due to mobile code configuration.

		Controls			
Obs.	Test	#1	#2	#3	Decision
1.	0	0	0	0	remote server problem–recheck later
2.	0	+	0	+	mobile code configuration problem
3.	0	0	+	+	firewall, proxies etc problem
4.	0	+	+	0	anomaly – recheck problem

0 = not able to access resource, + = able to access resource

Test: Mobile code configuration behind DoD or Guardnet firewall
Control #1: Normal configuration behind DoD or Guardnet firewall
Control #2: Mobile code configuration outside DoD firewall
Control #3: Normal configuration outside DoD firewall

2.5.10 Data analysis

The total number of hosts and pages examined by the web crawler and the number of hosts and pages that contained mobile code were approximated from the crawler log reports. Due to a batching of the hosts in input files into the crawler, a small fraction (<1%) of the hosts were represented twice. The number of hosts with problems were taken from the log reports. The problems were then categorized as to whether they were due to mobile code configuration, network/firewall issues, programming error or another anomaly.

3 Results and Analysis

3.1 Gap Analysis

Detailed results and substantiation of findings to the mobile code working group are contained in the GAP analysis report (Appendix D). The configuration guide reasonably interprets and implements the Mobile code policy. All requirements in the policy were implemented in the configuration guide. However, the Configuration Guidance is organized according to the mobile code risk categories under the Policy. As such, configuration guidance for a single software product is spread across several sections based on risk categories. The Gap Analysis recommends that the Configuration Guidance be re-organized according to software product to simplify carrying out the configuration of the client machine in a timely manner.

A total of 20 findings were identified in the configuration guide. However, none of these findings related to a requirement in the policy that would prohibit its use by those wanting to comply with the policy. Of the 20 findings, 18 were either confusing

statements needing clarification, or suggested improvements to help the reader understand the content, one was a recommended change to the structure of the guide to enable a simple yet timely implementation of the policy, and one indicated a need for additional study to evaluate the impact of disabling ActiveX plugins in Netscape.

In conclusion, the configuration guideline can be recommended as a solution to network security managers seeking to comply with the mobile code policy.

3.2 Use of Mobile Code by DoD educational agencies

Requests for information on the types and frequencies of mobile code usage in the development of DoD web-enabled courseware was sent to points of contact at 51 DoD Academic agencies and 13 Learning Management System vendors. Eighteen surveys were returned, and of those responding only six (33.3%) indicated that they were developing any course content that had Category 1 mobile code, and of those using Category 1 mobile code, all were using Active X (Table 3). None of the respondents indicated that they were using Windows Scripting Host or Unix Shell Scripting. Only 4 (27.8%) of the respondents indicated that they were using any Category 2 or Java applets.

The most widely used types of mobile code for web-enabled courseware development are those considered to be in Category 3 - including JavaScript and some VBScript. Although the response rate to the survey was low, there is no reason to believe that the results would vary significantly from these numbers if a larger sample size participated.

Table 3: The frequency with which mobile code was reported to be used by 18 Department of Defense Academic agencies.

Mobile Code Type	% yes	% no
Active X	33.3	66.7
- signed	66.6	33.3
Java Applets	27.8	72.2
- signed	100.0	0.0
JavaScript	88.9	11.1
VBScript	11.1	88.9
MS-DOS batch	0.0	100.0
Unix Shell Scripts	0.0	100.0
Visual Basic for Applications	11.1	88.9
LotusScript	0.0	100.0
PerfectScript	0.0	100.0
Other	22.2	77.8
Downloaded Over email	5.6	94.4

3.3 Web-based courseware evaluations

There were 660 unique hosts submitted by 27 Department of Defense Academic agencies including The Naval Postgraduate School, the Air Force Institute of Technology, the U.S.

Joint Forces Command's Joint Distributed Learning Center, U.S. Army Armour School, and The Army Management Staff College. The NavyLearning.com website was also submitted and contained over 300 web sites from across the DoD. The 660 hosts were batched and submitted to the web crawler for analysis. The web crawler examined those hosts as well as sites that were embedded as links, for a total of 2,203 host servers and 671,716 URL's. Of these, 204 host servers (4363 URL's) contained Active X and 430 host servers (12,804 URL's) contained Java applets.

Due to practical time constraints it was not possible to examine all of the URL's that were identified by the web crawler as containing mobile code. The evaluation team examined 128 host servers, representing 3227 URL's that contained Active X. They also examined a minimum of one instance of every type of Active X program, identified by a unique code known as the Class ID. The evaluation team also examined 276 host servers, representing 10,522 URL's that contained Java applets. A sample of the web crawler output is included in Appendix E.

Out of the 671,716 URL's examined by the web crawler and human evaluators, only three hosts contained content that could not be viewed due to the implementation of the Mobile Code Policy. There were also 82 problems encountered on different hosts where the examiners could not access some or all of the content on a host server that were not attributable to the mobile code policy. There were 16 instances where information could only be viewed in Netscape or Internet Explorer and the other 63 perturbations were due to firewall issues, network problems, the remote server being down, and miscellaneous programming problems intrinsic to the web page (Appendix F).

3.3.1 Mobile Code Policy implementation problems

The first of three URL's that were impacted by the policy www.onr.navy.mil/sci_tech/engineering/ProgRev99/presentations/Clemson/CU2/index.html contained a PowerPoint presentation that could not be viewed. However, the method used to post the presentation is not a standard method of posting PowerPoint on a website, and 103 other URL's with PowerPoint launched by Active X controls were viewed by the examiners without a problem. The second problem encountered was with the host marines.nscs.com/feedback/reports/, which called for a snapshot viewer that was not preinstalled on the browser. This host had 16 URL's all containing the same Active X control. In addition, there was a programming error that prevented the snapshot viewer from being downloaded and the site was disabled (perhaps temporarily) in the weeks following these tests.

There was only one instance when the test Chief Information Officer did not approve a certificate. This certificate was located on a US host server, but was signed by a European certificate authority. If the certificate had been signed by an American certificate authority, it would have been accepted and not been impacted by implementation of the Policy. The CIO's did approve three other certificates all signed by US certification authorities during these tests (Table 4).

Table 4: Certificates that were encountered and accepted during the examination of 2,203 hosts subject to Chief Information Officer Approval.

Host	# URL's	Type
www.umr.edu/telinfo/newsltr.html	1	Active X
www.xtreme.learning.com/csvc/svm.asp	1	Active X
www.parallelgraphics.com	3	Active X
liftoff.msfc.nasa.gov/realtime/Jpass/20/Applet.asp	3	Active X

3.3.2 Category 1 Mobile Code

Active X was found to occur multiple times on a single URL on many of the URL's examined. A total of 10,715 separate instances of Active X were found on the sites examined by the web crawler. The majority of the Active X controls encountered during this test were pre-installed in the browser and therefore not prohibited or impacted by the implementation of the Policy.

We were able to determine the function of a Class ID of the Active X by entering it into a diagnostic computer program Mary X, which is part of the NSA SNAC Value Added Tools program set. Shockwave Flash was the most frequent application launched by an Active X control, accounting for 9803 of the observations (Table 5). The evaluation team did not report any problems viewing any of the Shockwave Flash Applications due to implementation of the mobile code policy in either the DoD testbed or the Guardnet Testbed environment. An application to launch Real Player G2 was the next most frequently used Active X control with 209 instances found and no problems were reported using this technology due to the implementation of the Policy.

There were no URL's found as part of this test that contained scripts that executed in Windows Scripting Host (WSH). Therefore, we were unable to determine the impact of implementing the policy on using Windows Scripting Host per se, however since WSH was not found in over 670,000 URL's, we can estimate that the impact of implementing a policy that restricts the use of this type of programming would have little to no impact on the learner.

3.3.3 Category Two Mobile Code

Of the 430 hosts and 12, 804 URL's that contained Java, 7689 of the URL's belonged to the same host and used the same program, a clock that appeared on all of the Carnegie Mellon University web pages. The evaluators did not report any problems observing any Java applets on any of the web hosts or URL's due to implementation of the Mobile Code Policy.

3.3.4 Browser specific problems

There were 16 unique instances where content could only be viewed in either Netscape or Internet Explorer. In thirteen of these occurrences the content in the URL was only observable using Internet Explorer and of these only one site contained Active X. In two instances, evaluators were able to view pages with Active X components using Netscape,

Table 5: The Class Identifications and function of the Active X components encountered during the mobile code policy implementation tests.

Class ID	Frequency	Function
D27CDB6E-AE6D-11cf-96B8-444553540000	9803	Showave Flash Object
CFCDAA03-8BE4-11CF-B84B-0020AFBBCCFA	209	Real Player G2 Control
8856F961-340A-11D0-A96B-00C04FD705A2	181	Microsoft Web Browser
86A88967-7A20-11d2-8EDA-00600818EDB1	160	
EFBD14F0-6BFB-11CF-9177-00805F8813FF	103	Microsoft PowerPoint
7A2CB982-9E7E-11D3-990D-00A0C94C695A	92	unique to one site
072D3F2E-5FB6-11d3-B461-00C04FA35A21	18	Cold Fusion Form Runtime
C9DA1E5F-3689-11D2-9DF3-00805FB1E78E	18	
70E81EBA-381E-11D2-9DF3-00805FB1E78E	17	
F0E42D60-368C-11D0-AD81-00A0C90DC8D9	17	
4B6E3013-6E45-11D0-9309-0020AFE05CC8	14	
0002E510-0000-0000-C000-000000000046	13	Microsoft Office Data Spreadsheet
F4818F4C-BEC5-11CF-83AD-00A0242FBEA6	12	
0002E530-0000-0000-C000-000000000046	11	
166B1BCA-3F9C-11CF-8075-444553540000	10	Shockwave Active X Control
8AD9C840-044E-11D1-B3E9-00805F499D93	8	JavaBeans Bridge Object
22d6f312-b0f6-11d0-94ab-0080c74c7e95	6	Windows Media Player
D7053240-CE69-11CD-A777-00DD01143C57	5	
4E330863-6A11-11D0-BFD8-006097237877	3	
0FC6BF2B-E16A-11CF-AB2E-0080AD08A326	2	
8E27C92B-1264-101C-8A2F-040224009C02	2	Calendar Control Object
1663ed61-23eb-11d2-b92f-008048fdd814	1	Allaire Homesite Script X Factory
16E349E0-702C-11CF-A3A9-00A0C9034920	1	
1A4DA620-6217-11CF-BE62-0080C72EDD2D	1	File Finder Toolbox Bitmap
2179C5D3-EBFF-11CF-B6FD-00AA00B4E220	1	Microsoft Netshow Player
31B7EB4E-8B4B-11D1-A789-00A0CC6651A8	1	
71830411-44EC-11CF-81B6-000021570103	1	
adb880a6-d8ff-11cf-9377-00aa003b7a11	1	
D702FBF4-EE60-11d0-BD5B-00A0C91F4635	1	Microsoft Forms Command Button
E33551EE-425E-427B-9FB5-631C173292D7	1	
ED0B00C0-6039-11D3-BBEC-EED8E92EDA6E	1	
F75FBEA9-0444-11D2-9C48-00A0C94C8A8A	1	
Total:	10715	

but not using Internet Explorer. Therefore, it appears that the problems the evaluators encountered in viewing content on these sites were due to programming issues specific to how browsers deal with web-programming independent of the mobile code policy implementation procedure that was followed (Table 6).

3.3.5 Guardnet problems

The Guardnet classroom test bed workstations had Microsoft Windows '95 operating system with Internet Explorer 4.0. This test bed did not have Netscape installed on the workstation. Therefore it gave us the ability to examine the impact of the Policy on a learner who does not have access to the latest technology. The content in nine URL's could not be viewed in the Guardnet classroom, but could be viewed by the other workstations in the DoD test environment. Since they could not be viewed by the control machines that did not have the configuration guideline specifications applied and the mobile code policy configured workstations, it appears that the inability of the evaluators

to access content on these machines was not a result of the Policy, but rather a function of the firewall or other network configuration.

Table 6: Hosts that had content that was viewable in either Netscape or Microsoft Internet Explorer (IE), but not both. The browser in which the content could be viewed is indicated in the last column.

Host	# URL's	Type	Browser
www.tacom.army.mil/immc/Support/construction/cegroup.htm	1	Java	Netscape
www.keesler.af.mil/cc/CCbegin.htm	2	Java	IE
marines.nscs.com/caci/index.htm	1	Java	IE
www.lackland.af.mil/344trs/svscontactsnew.htm	32	Java	IE
www.altus.af.mil/pg54/ppg54.html	1	Java	IE
www.amsc.amedd.army.mil	1	Java	IE
www.umr.edu/~ima	1	Active X	IE
www.benning.army.mil/rtb/RANGER/rangerschool.htm	1	Java	IE
www.umr.edu/~aises	1	Java	IE
192.132.84.3/vr/OPQ.htm	1	Java	IE
www.armyrotc.com/basiccamp/index.html	1	Active X	Netscape
www.segs.fit.edu/Course_Schedule/body_course_schedule.html	1	Java	IE
www.hamptonroads.com/	5	Java	IE
www.senate.gov/~kennedy	1	Active X	IE
www.senate.gov/~lincoln/html/webform.html	1	Active X	IE
www.senate.gov/~lincoln/html/webform.html	1	Active X	Netscape

4 Interpretations and Conclusion

The gap analysis performed between the Mobile Code Policy and the Configuration Guidance supplied by MITRE indicates that the guidelines can be recommended as sufficient measures to comply with the Mobile Code Policy. The one area that could be improved upon is the time it takes to configure each workstation.

During our tests it took an average of 1 hour and 15 minutes to do the first workstation and an average of 40 minutes after the sequence had been repeated several times. In addition, during the evaluations the team had to learn the meaning of the additional warning prompt sequences that would appear on the screen. Therefore, we recommend that a streamlined method for configuring the workstations be written, which includes information for the user on the prompts that they might expect to see while accessing their online courses or supplemental material.

The impact of the Mobile Code Policy on the learner is dependent upon whether the learner accesses course content with mobile code, and whether implementing the Policy interferes with their ability to access that content. In this study we found that Category 1 mobile code was found on only 9.26% of the host servers and Category 2 was found on 19.5% of host servers. In addition, only one-third of the respondents indicated that they used Category 1 mobile codes and only 27.8% of the respondents indicated that they used

Category 2 mobile codes. Of the courseware contracted by the DoD, all of it would be permissible within the scope of the policy if it was signed with a DoD certificate or if it executed actions pre-installed on the browsers.

During this study, most of the Category 1 mobile code encountered executed functions that are pre-installed with the browser (e.g. Shockwave Flash) or was signed by a US certificate signing authority. Most of the Category 2 mobile code did not operate outside of the sandbox on the client workstation, therefore both of these were not impacted by the Policy. Furthermore, during this study we found only three impediments attributable to the policy after approximately 192 man-hours engaged in a targeted search from a list of URL's known to contain mobile code. Most users would encounter mobile code or mobile code technologies only a few times if at all while taking an online course or doing research using supplemental course materials.

Therefore, if the Mobile Code Policy is implemented as recommended by the Configuration Guidelines supplied by MITRE, we expect the impact to the learner, ADL programs and web-based distance learning to be minimal.

5 Acknowledgements

The authors wish to thank Ms. Sheila Collins (IITA/USAFA) for distributing and tabulating the questionnaires, for collecting the list of URL's and for data analysis. They also wish to thank Ms. Robin Mangum (ADL Co-Lab) for technical support, DISA for supplying, installing, and configuring a typical DoD firewall, Capt Duane Hellums (AFIADL), Mr. Steve Scanlon (NAVAIR) for input on the testplan, Maj. Stephan Picard (National Guard/DTTP) for the use of the DTTP classroom and GuardNet, Mr. John McLeod and Mr. Dave Twigg (DTTP) for their technical assistance, and the ADL Co-Lab interns Chris Ruddick and Jon Huang, and IDA intern Derek Brooks for their help in data collection as part of the evaluation or "surf" team.

Appendix A – Mobile Code Policy

Appendix B – Questionnaire on Mobile Code Usage by DoD

QUESTIONS REGARDING MOBILE CODE USAGE IN TRAINING PRODUCTS AND COURSES

Does your product and/or courses use or rely on the download of any mobile code into the user/client/student workstation? For each type of mobile code, please answer yes or no. If yes, please answer the questions for that type of code.

1. ActiveX controls?

   If yes:
   A. Are the ActiveX controls digitally signed?

   B. If they are not signed, would it be possible for you to sign them?

2. Java applets?

   If yes:
   A. Are the applets digitally signed?

   B. Do the applets require privileges outside of the sandbox?

3. JavaScript scripts (or JScript scripts)?

   If yes:
   A. Are the scripts digitally signed?

   B. Do the scripts require privileges outside of the sandbox?

   C. Do any scripts execute in Windows Scripting Host?

4. VBScript scripts?

   If yes:
   A. Are the scripts digitally signed?

   B. Do any scripts execute in Windows Scripting Host?

5. MS-DOS batch scripts (.BAT files downloaded as mobile code)?

6. Unix shell scripts (downloaded as mobile code)?

7. Visual Basic for Applications macros (e.g. MS Office Word, Excel, and PowerPoint macros)?

8. LotusScript scripts [e.g. Lotus Notes macros, forms]?

9. PerfectScript scripts [e.g. WordPerfect macros] ?

10. PostScript?

11. Any other types?

12. Is mobile code downloaded or embedded into email bodies or email attachments?

Appendix C – Data collection forms

For each problem encountered viewing the web pages, fill out the data collection form with the appropriate information. Use the code A = Severe, B = Moderate, C = Minor, or 0 for no problem.

			Test Configurations					Controls			
Date	Time	URL	IE 4.0	IE 5.5	IE 5.0	Net 4.7	Net 4.6	NG #1	1	2	3

Appendix D: Gap Analysis

Mobile Code Gap Analysis Report
18 April 2001

Executive Summary

Detailed results and substantiation of findings to the mobile code working group are contained in the GAP analysis report. The configuration guide reasonably interprets and implements the Mobile code policy. All requirements in the policy were implemented in the configuration guide. However, the configuration guideline's current structure lacks the practicality of following the procedures to implement the policy in a timely manner, thus, it requires testing. Although not directly related to mobile code, recommend tests be conducted to investigate and evaluate the impact of disabling ActiveX plugins in Netscape, because an organization may require the use of the Netscape browser only, and the consequences of such an action could greatly inhibit an organizations mission.

A total of 20 gaps were identified in the configuration guide. However, none of the gaps found in the configuration guide related to a requirement in the policy that would prohibit its use by those wanting to comply with the policy. Of the 20 findings, 18 were either confusing statements needing clarification, or suggested improvements to help the reader understand the content, one was a recommended change to the structure of the guide to enable a simple yet timely implementation of the policy, and one indicated a need for additional study to evaluate the impact of disabling ActiveX plugins in Netscape.

In conclusion, the configuration guideline can be recommended as a solution to network security managers seeking to comply with the mobile code policy.

GAP ANALYSIS

GAP Analysis

1.2 Purpose. To perform a GAP analysis which will determine whether the configuration guidelines are a reasonable interpretation of the policy and can be used as a baseline configuration for the scope of a new set of tests. In addition, it determines whether the configuration guidelines can be recommended as a solution to network security managers seeking to comply with the mobile code policy, and whether the configuration guidelines implement the Mobile code policy.

1.3 GAP Analysis Conducted by: Marty Salyars, Army Management Staff College

1.4 GAP Analysis Process. The GAP Analysis was conducted in two phases. Phase one was the configuration guideline interpretation of the policy, and phase two was the

configuration guideline implementation of the policy. The analysis for both phases was based on 1) reviewing the policy and configuration guideline 2) interviewing an Information Management Officer, programmer, system administrator, and webmaster 3) completing the step by step configuration procedures using Windows 95 with Netscape, IE 4.0, Windows 98SE with Netscape, IE 5.0, and NT 4,0 with Netscape, and IE 5.5.

Configuration guidance procedures were not verified relating to Windows 2000, Qualcomm Eudora Pro email, or the Lotus Notes browser because these products were not available.

1.5. Configuration Guideline Interpretation/Implementation of the Policy.

1.5.1 The first task determines if the configuration guideline reasonably interprets the policy for realistic implementation. It identifies gaps in the configuration guide that were found confusing, missing, or weak.

1.5.2 The second task verifies the configuration guideline procedures that implement the policy. It points to a gap that may need to be modified, improved, or created.

GAP Analysis

The GAP Analysis focuses on volume 1, Configuration Guidance for Client Workstations, and Applications. It determines if the configuration guidelines reasonably interpret the policy, and it verifies if the configuration guideline procedures properly implement the policy.

To achieve this effort, two questions were asked:

- Does the configuration guideline reasonably interpret the policy? This means does the configuration guide reasonably translate and explain what it is the policy wants to achieve, i.e, reduce the mobile code threat on DoD systems, and what is it the policy wants us to do (requirements), i.e., disable unsigned ActiveX.
- Does the configuration guideline procedure implement the policy. This means are the procedures in the configuration guide written in such a fashion that when followed, execute that which is required in the policy. Both questions accompany each section.

There are four possible answers to each question, “Yes”, “Yes**”, “No”, and “NA”.

- Yes means the configuration guideline reasonable interprets the policy, and that the procedure implements the policy correctly.

- Yes** means the configuration guideline reasonably interprets the policy, and that the procedure implements the policy, but points to a gap in the configuration guide that was found confusing, missing, or weak.
- No means that the configuration guideline does not interpret the policy accurately, nor do the procedures properly implement the policy correctly.
- NA means the question(s) do not relate to the topic being reviewed.

For simplicity, answers are provided after each question, and the response, or gap the answer points to follow each topic in the order that they appear in the configuration guide table of contents.

Section 1

Introduction

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? NA

1.1 Purpose

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? NA

Response: Missing - Suggest adding “enclave boundary” to the second paragraph to bind the meaning of enclave (end-to-end), and where the firewall, proxies, and gateways are located. Recommend the second paragraph to read, “Volume 2 provides configuration guidance for selected firewall and third-party gateway products residing at the enclave boundary”.

1.2 Background

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? NA

Response: Confusing: The meaning of "authority" is not clear. The definition of enclave in the configuration guide is "an information system environment that is end-to-end under the control of a single authority and has a uniform security policy, including personnel and physical security." The words "single authority" should be replaced with "Designated Approving Authority". The policy states "This policy is focused on the receipt of executable information from sources outside the Designated Approving Authority's area of responsibility". Missing is the Designated Approving Authority (DAA) definition on page 1-2.

1.3. Scope

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? NA

1.4 Naming Conventions

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? NA

1.5. Document Structure

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? NA

Response: a. The follow definitions are missing from the configuration guide, and should be added for clarification.

1. INFOCON. Recommend adding to terms. It's assumed the reader knows what INFOCON is.

2. ActiveX. Recommend adding to terms. For example - ActiveX is a Microsoft technology that allows a web browser to download and execute ActiveX Controls to extend the users interactive experience.

3. ActiveX control. Recommend adding to terms. For example - ActiveX controls are small programs that can extend the capability of the browser by invoking the functions contained in other programs.

4. Netscape Plugin. Recommend adding to terms. For example, it's a method of extending the capabilities of Netscape that allows third party applications to run inside the browser.

Response: b. Weak - Although not directly related to the procedures, or interpretation, it is related to the ease of implementation. The document structure is fine, however, to provide it to the IT department for implementation in such a format is not recommended. Volume 1 focuses on configuring specific browsers by mobile code categories. This means when configuring one browser you have to jump from one mobile code category to another to complete the security settings, and often the procedures are the same in each category. Organizations will configure according to the browsers installed on the workstation, not by mobile code category. Therefore, recommend creating a separate

configuration guide for each browser with procedures to configure all mobile code security settings.

For example:

Mobile Code Workstation configuration guidance for Internet Explorer 5.5
Category 1
Category 2
Category 3
Email
Emerging Technology

Section 2

2. Workstation Configuration Guidance for Category 1 Mobile Code Technologies

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.1 Configuration Guidance for Using ActiveX Controls

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - The initial paragraph states "for those products that do not differentiate between signed and unsigned Active X controls or cannot be configured to disable unsigned Active X Controls e.g.. (Netscape Active X plugin, Lotus Notes Browser), guidance is given to disable all Active X Controls". Yet in paragraph 2.1.1, it states “Netscape Communicator (including Navigator and Messenger) does not support ActiveX Controls”. Then it says, “No configuration setting are required to disable Active X within Netscape”.

2.1.1 ActiveX Controls and Netscape Communicator

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: a. The following statements were confusing when reading the topic:

1 . In paragraph 2.1 it stated that the "guidance is given to disable all Active X Controls", which included Netscape, yet it paragraph 2.1.1, it says, "No configuration settings are required to disable ActiveX within Netscape".

2. Procedure for deleting Netscape ActiveX Plugins is confusing. In step 3, it states to "Scroll through the list of plugins looking for any ActiveX Plugins". Yet, how can you tell which DLL is an ActiveX Plugin? Or, are all DLL's in the "About Plugins ActiveX,

and must be deleted. In Step 5 it says "Go to the directory that contains the ActiveX Plugin and delete only those .dll files that pertain to the ActiveX Plugin(s)". Again, how can you tell which .dll is ActiveX? In step 6 it says "Search for other files related to the Active X Plugin. (For example: Click Start, click Find, Click Files or Folders,...) If you find them delete them." How can you tell what files are related to ActiveX? Are any of the .dll files being deleted shared with other applications?

Response: b. Requires additional study - Although not tied to mobile code, deleting all ActiveX plugins in Netscape greatly limits the functionality of Netscape, and the users interactive multimedia experience, especially given the number of government Netscape users, and where organizations may require the use of Netscape only. Also, it effectively eliminates the choice to use Netscape. The primary difference between ActiveX controls and Netscape plugins is the method of installation. ActiveX controls can be downloaded and executed automatically without user intervention, whereas a Netscape, in **most cases** have to find the plugin, manually download it, install it, and then restart Netscape before the plugin can be used.. More testing is needed in this area. The consequences of the deleting all ActiveX plugin are too stringent.

2.1.2 ActiveX Controls and Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - The sentence “Changing the settings in one product automatically changes them in the other products” is too vague. Recommend removing this sentence, or put it in the first paragraph and explain how IE is tied into the windows operating system to include its consequences relative to security vulnerabilities. For example, the integration of Internet Explore and the Windows operating System allow operations, which would otherwise be performed within Windows also run in Internet Explorer. Hence, changing settings in Internet Explorer automatically affects other products tied to the Windows operating system, such as, Microsoft office products, and other pre-installed components and applications. This is somewhat explained on pages 2-24, and 2-25 under ActiveX Controls and Microsoft Office Products and Configuration Guidance for Disabling Mobile Code in Windows Scripting Host. At least this will help those reading the configuration guide understand why would an action performed in Internet Explorer affect “executing local pre-installed ActiveX controls” and other like kind statements throughout the configuration guide.

Response: Move - Pages 2-13, 2-24, The configuration guide asks the user to jump to the mail sections 3.4, 3.5, or 3.6 to “disable the execution of all ActiveX controls in the Restricted Sites Zone”, then jump back in the guide to continue configuring Microsoft IE Version 5.0. The user has to configure email anyway. Suggest removing the statement “Next it is essential that the user follow the guidance in Sections 3.4, 3.5, or 3.6 to disable the execution of all Active X controls in the restricted Sites Zone”.

2.1.3 ActiveX Controls and Microsoft Outlook Express.

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - Other than a pointer, you're asking the user to jump to the email section to configure Outlook Express and jump back again to continue. Recommend removing.

2.1.4 ActiveX Controls and Microsoft Outlook 98

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - Other than a pointer, you're asking the user to jump to the email section to configure Outlook Express and jump back again to continue. Recommend removing.

2.1.5 ActiveX Controls and QUALCOMM Eudora Pro Email 4.2.

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - Other than a pointer, you're asking the user to jump to the email section to configure Outlook Express and jump back again to continue. Recommend removing.

2.1.6 ActiveX Controls and Lotus Notes 5.0 Browser (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.1.7 ActiveX Controls and Microsoft Office Products

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2 Configuration Guidance for Disabling Mobile Code in Windows Scripting Host

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.1 WSH and Windows

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.2 WSH and Netscape Communicator

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.3 WSH and Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.4 WSH and Microsoft Outlook and Outlook Express

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.5 WSH and QUALCOMM Eudora Pro Email 4.2 (Not Tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.2.6 WSH and Lotus Notes (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3 Configuration Guidance for Disabling MS-DOS Batch Script Mobile Code

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.1 MS-DOS Batch Script Files and Windows

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.2 MS-DOS Batch Script Files and Netscape

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.3 MS-DOS Batch Scripts and Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.4 MS-DOS Batch Scripts and Microsoft Outlook 98 and Outlook Express
Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.5 MS-DOS Batch Scripts and QUALCOMM Eudora Pro Email 4.2 (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

2.3.6 MS-DOS Batch Scripts and Lotus Notes (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3. Workstation Configuration Guidance for Countermeasures for Mobile Code in Email Messages and Attachments

Does the configuration guideline reasonably interpret the policy? Yes**
Does the configuration guideline procedure implement the policy? Yes

3.1 Risks of Mobile Code in Email

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.2 Countermeasures for Mobile Code in Email

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.3 Email and Netscape Communicator 4.0

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes**

Response: Inconvenience - Page 3-5, has you jump to three different sections to configure Netscape (sections 2.2.2, 4.1.1, and 5.1.1), then back to page 3-5 to continue.

3.4 Email and Microsoft Outlook Express (Outlook Express 5.0 not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes

Question 2. Does the configuration guideline procedure implement the policy? Yes

3.5 Email and Microsoft Outlook 98

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - Page 3-14, the figure 3-15 "Outlook 98 Warning for Attachments {Outlook2000}" has Outlook 2000, is this saying that the configuration settings are the same for both products? I didn't have Outlook 2000, so I couldn't verify Outlook 2000.

Response: Modify - Page 3-15, Statement "The user should consult their Component CIO for advice" should read, "User should, consult their IT helpdesk, or Information Assurance Officer".

(Remove) Page 3-16, recommend not to include Microsoft or vendor specific URL for security updates, such as "Known issues with Outlook e-Mail Security Update". URL's are easily outdated, removed, redirected, and can lead to broken links.

3.6 Email and Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.6.1 Disable Mobile Code in IE 4.x

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.6.2 Disable Mobile Code in IE 5.x

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.7 Email and QUALCOMM Eudora Pro Email 4.2 (Not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.7.1 Disable Mobile Code (Executables in HTML Content) in Eudora (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.7.2 Enable Warnings Prior to Executing Mobile Code (Launching Programs) (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.8 Lotus Notes 5.0 (Not tested))

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.9 Enable User Prompts Prior To Opening Email Attachments

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.9.1 Enabling Prompts Via Windows File Types

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

3.9.2 Enabling Prompts Via Netscape Communicator 4.0 File Types

Question 1. Does the configuration guideline reasonably interpret the policy? Yes**
Question 2. Does the configuration guideline procedure implement the policy? Yes

Response: Confusing - In the title it references Netscape 4.0, yet in the body at the start of the procedure it states, "While running Netscape Communicator (version 4.6 and later)". Recommend removing the "4.0" in the title.

4. Workstation Configuration Guidance for Using Category 2 Mobile Code Technologies

Does the configuration guideline reasonably interpret the policy? Yes
Does the configuration guideline procedure implement the policy? Yes

4.1 Configuration Guidance for Using Java Applets in Browsers

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.1.1 Java Applets and Netscape Communicator 4.0

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes**

Response: Confusing – page 4-6, paragraph (d), it states "the applet cannot be trusted and should not be granted privileges. Click Deny." It then says "It is likely that the applet will not execute." In what cases will the applet execute even though I click to deny it's privileges?

4.1.2 Java Applets and Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.1.3 Java Applets and Lotus Notes 5.0 (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.2 Configuration Guidance for Using Visual Basic for Applications

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes**

Response: Change – first paragraph it says "See Section 4.2" it should read 5.2.

4.2.1 VBA and Microsoft Office 97

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.2.2 VBA and Microsoft Office 2000 (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.3 Configuration Guidance for Using PerfectScript (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.4 Configuration Guidance for Using LotusScript in Lotus Notes (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.5 Configuration Guidance for Using PostScript

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.5.1 Enable Warnings before Opening PostScript Files in Windows

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.5.2 Remove PostScript File Type Recognition From Netscape Communicator

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

4.5.3 Enable the Safer Mode in Ghostscript and GSView (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5. Workstation Configuration Guidance to Disable Category 2 Mobile Code Technologies

Does the configuration guideline reasonably interpret the policy? Yes
Does the configuration guideline procedure implement the policy? Yes

5.1 Configuration Guidance to Disable Java Applets

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.1 Disable Java Applets in Netscape Communicator 4.0

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.2 Disable Java Applets in Microsoft Internet Explorer

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.3 Disable Java Applets in QUALCOMM Eudora Pro Email 4.2 (procedure not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.4 Disable Java Applets in Microsoft Outlook Express

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.5 Disable Java Applets in Microsoft Outlook 98

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.1.6 Disable Java Applets in Lotus Notes 5.0 (procedure not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.2 Configuration Guidance for Visual Basic for Applications (VBA)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.2.1 Microsoft Office 97

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.2.2 Microsoft Office 2000 (Not tested)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.3 Configuration Guidance for PerfectScript in Corel Office (procedure not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.4 Configuration Guidance to Disable LotusScript in Lotus Notes (procedure not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.5 Configuration Guidance to Disable PostScript (procedures not verified)

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.5.1 Remove PostScript File Type Recognition From Browsers and Email Products

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.5.2 Remove PostScript File Type Recognition in Windows

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

5.5.3 Uninstall PostScript Application Software

Question 1. Does the configuration guideline reasonably interpret the policy? Yes
Question 2. Does the configuration guideline procedure implement the policy? Yes

6. Workstation Configuration Guidance for Using Category 3 Mobile Code Technologies

Does the configuration guideline reasonably interpret the policy? Yes
Does the configuration guideline procedure implement the policy? Yes

7. Miscellaneous Browser Settings

Does the configuration guideline reasonably interpret the policy? NA
Does the configuration guideline procedure implement the policy? NA

Appendix E: Sample output from web crawler

DYNAMIC PAGE -- UNCLASSIFIED

6 ActiveX Host Report

6.1.1 ActiveXHTMLModule Run Statistics:

Run Ending: Thu Jun 14 13:50:10 EDT 2001

Total Pages Scanned	4655
Total Hosts with ActiveX	6
Total Pages with ActiveX	16
Total ActiveX Control Instantiations Found	16
No. of ActiveX Control Instantiations with Codebase	16
Unique ActiveX ClassIDs Found	2

6.1.2 Bare Hosts Listing

Web site hosts where at least one page was found that included at least one <OBJECT> tag for an ActiveX control

1. iac.dtic.mil
2. www.dsp.dla.mil
3. www.itl.nist.gov
4. www.chemconnect.com
5. www.army.mil
6. www.cio.gov

6.1.3 Hosts and Pages Listing

Pages at the various hosts that contained at least one <OBJECT> tag for an ActiveX control.

1. **iac.dtic.mil**
    1. http://iac.dtic.mil/
2. **www.dsp.dla.mil**
    1. http://www.dsp.dla.mil/main.htm
3. **www.itl.nist.gov**
    1. http://www.itl.nist.gov/iad/894.03/fing/fngcmpl.html
    2. http://www.itl.nist.gov/iad/894.03/fing/fngcmps.html
    3. http://www.itl.nist.gov/iad/894.03/fing/flash_tst.html

4. http://www.itl.nist.gov/iaui/vip/fing/fngcmpl.html
5. http://www.itl.nist.gov/iaui/vip/fing/fngcmps.html
6. http://www.itl.nist.gov/iaui/vip/fing/flash_tst.html
7. http://www.itl.nist.gov/iaui/894.03/fing/fngcmpl.html
8. http://www.itl.nist.gov/iaui/894.03/fing/fngcmps.html
9. http://www.itl.nist.gov/iaui/894.03/fing/flash_tst.html

4. **www.chemconnect.com**
    1. http://www.chemconnect.com/help/index.html
5. **www.army.mil**
    1. http://www.army.mil/coolstuff/default.htm
6. **www.cio.gov**
    1. http://www.cio.gov
    2. http://www.cio.gov/index.cfm?Fuseaction=Text&Section_1=&Section_2=&Function=
    3. http://www.cio.gov/index.cfm

Generated by the ActiveXHTMLModule, part of the ECCrawler.

Back to Previous Page

Module by Neal Ziring, ECCrawler by Scott Lake.

Appendix F – List of problems encountered accessing information during the mobile code tests.

Host	# URL's	Type	Browser
Mobile Code Policy Problems			
www.onr.navy.mil/sci_tech/engineering/ProgRev99/presentations/Clen	1	Active X	both
marines.nscs.com/feedback/reports/altis01.htm	16	Active X	both
Host			
**www.umr.edu/~telinfo/newsltr.html	1	Active X	both
www.xtremelearning.com/csvc/svm.asp	1	Active X	both
www.parallelgraphics.com	3	Active X	both
liftoff.msfc.nasa.gov/realtime/Jpass/20/Applet.asp	3	Active X	both
**this certificate was not approved by the CIO			
Browser Specific Problems			
www.tacom.army.mil/immc/Support/construction/cegroup.htm	1	Java	Net
www.keesler.af.mil/cc/CCbegin.htm	2	Java	IE
marines.nscs.com/caci/index.htm	1	Java	IE
www.lackland.af.mil/344trs/svscontactsnew.htm	32	Java	IE
www.altus.af.mil/pg54/ppg54.html	1	Java	IE
www.amsc.amedd.army.mil	1	Java	IE
www.umr.edu/~ima	1	Active X	IE
www.benning.army.mil/rtb/RANGER/rangerschool.htm	1	Java	IE
www.umr.edu/~aises	1	Java	IE
192.132.84.3/vr/OPQ.htm	1	Java	IE
www.armyrotc.com/basiccamp/index.html	1	Active X	Net
www.segs.fit.edu/Course_Schedule/body_course_schedule.html	1	Java	IE
www.hamptonroads.com/	5	Java	IE
www.senate.gov/~kennedy	1	Active X	IE
www.senate.gov/~lincoln/html/webform.html	1	Active X	IE
www.senate.gov/~lincoln/html/webform.html	1	Active X	Net
Guardnet Firewall			
162fw.ang.af.mil/UTA.htm	1	Active X	both
aec-www.apgea.army.mil/prod/aechome.htm	1	Active X	both
www.redstone.army.mil/ommcs	1	Active X	both
das.cs.amedd.army.mil/index3.htm	1	Active X	both
www-dcst.monroe.army.mil/sbt/	2	Java	both
chppm-www.apgea.army.mil	1	Java	both
www.misn.com/	2	Java	both
www.vt.edu/misc/publish/krtest.html	1	Java	both
lcweb2.;oc.gov/ammem/pihtml/pivid11.html	2	Active X	both

Guardnet and Programming			
www.afrc.af.mil/9114aw	1	Java	both
www.af.mil/news/tv	3	Active X	both
www.af.aflinkplus	4	Active X	both
lcweb2.loc.gov/ammem/pihtml	9	Active X	both
www.hamptonroads.com/usswisconsin/wisconsin_video.html	2	Active X	both
www.onr.navy.mil	11	Active X	both
DoD Firewall			
www.umr.edu/~geo-geop	1	Java	both
rucker-dtac.army.mil/davis/airalst.html	12	Active X	both
http://www.afrc.af.mil/910aw	4	Java	both
www.boeing.com/commercial.bbj	2	Active X	both
Remote Server down			
www.same.org/forms/form.html?id=25	1	Java	both
www.asat.army.mil/support/441/release.htm	1	Active X	both
www.gordon.army.mil/garrcmd/default.htm	1	Java	both
www.senate.gov/chafee	1	Java	both
www.rollanet.org/~ktkwon	1	Active X	both
www.dmi.usma.edu/Branch/AD/Draft01/Draft01.html	2	Java	both
www.umr.edu/~amigos	1	Java	both
www.disa.mil/D2/dms/public/goodnews.html	1	Java	both
www.centcom.mil/foia	1	Java	both
www.keesler.af.mil/medctr/amds/PPIP/horseback_riding.htm	1	Java	both
www.bliss.army.mil/Other%20Sites%20at%20Ft%20Bliss/usacasbn/ca	1	Active X	both
www.onr.navy.mil/sci_tech/engineering/ProgReview99	34	Active X	both
topex-www.jpl.nasa.gov/education/orbit.html	1	Java	both
www.va.gov/	2	Java	both
www.usna.edu/ERC/MSCweb.htm	1	Active X	both
www.ngb.dtic.mil/hot_topics/environmental/ourprograms.htm	1	Java	both
www.lejeune.usmc.mil/mccsss/los	1	Java	both
Programming			
www-rotc.monroe.army.mil/Information/index2.html	1	Java	both
www.hq.navy.mil/cno/n09b/n09be/contents.htm	1	Java	both
www.hq.navy.mil/natops/..\default.htm	1	Active X	both
132.46.116.3/sptg/dpc/owcp/ca-11.htm	2	Java	both
www.smartforce.com	1		both
www.mism.cmu.edu	1	Active X	both
www.transchool.eustis.army.mil/	1	Active X	both
hiwaay.net/~crispen/vrmlworks/JavaTest/	6	both	both
www.acq.osd.mil/ar/arms/eterp1a.htm	1	Active X	both

Network and/or Programming			
www.army.mil/careers.htm	1	Active X	both
www.rollanet.org/~rcarmack	1	Java	both
www.blaxxun.com	27	Active X	both
www.navy.mil/homepages/hs142	1	Java	both
www.mathsci.usna.edu/~needham/courses/	3	Java	both
www.afji.com	1	Active X	both
www.rollanet.org/~demoman	1	Java	both
ir.chem.cmu.edu/irproject/	8	Java	both
www.forscom.army.mil/reeng/1-ssd/default.htm	1	Java	both
www.umr.edu/~w0eee	1	Java	both
http://nasm.edu/nasm/garber	2	Java	both
http://weather.noaa.gov/radar/mosaic.loop	183	Java	both
www.usna.edu/ERC/MSCweb.htm	1	Active X	both
salemmissouri.com/Salem_area_businesses/area_businesses/compu	1	Java	both
www.faa.gov/nfdcata100/130/130obta.html	1	Active X	both
www.parallelgraphics.com	1	Active X	both
www.afrc.af.mil/926FW/DPF/	10	Java	both
www.afji.com	1	Active X	both