Security and ArcIMS

An ESRI White Paper • January 2001

ESRI 380 New York St., Redlands, CA 92373-8100, USA • TEL 909-793-2853 • FAX 909-793-5953 • E-MAIL info@esri.com • WEB www.esri.com

Copyright © 2001 Environmental Systems Research Institute, Inc.
All rights reserved.
Printed in the United States of America.

The information contained in this document is the exclusive property of Environmental Systems Research Institute, Inc. This work is protected under United States copyright law and other international copyright treaties and conventions. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, except as expressly permitted in writing by Environmental Systems Research Institute, Inc. All requests should be sent to Attention: Contracts Manager, Environmental Systems Research Institute, Inc., 380 New York Street, Redlands, CA 92373-8100, USA.

The information contained in this document is subject to change without notice.

U.S. GOVERNMENT RESTRICTED/LIMITED RIGHTS

Any software, documentation, and/or data delivered hereunder is subject to the terms of the License Agreement. In no event shall the U.S. Government acquire greater than RESTRICTED/LIMITED RIGHTS. At a minimum, use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR §52.227-14 Alternates I, II, and III (JUN 1987); FAR §52.227-19 (JUN 1987) and/or FAR §12.211/12.212 (Commercial Technical Data/Computer Software); and DFARS §252.227-7015 (NOV 1995) (Technical Data) and/or DFARS §227.7202 (Computer Software), as applicable. Contractor/Manufacturer is Environmental Systems Research Institute, Inc., 380 New York Street, Redlands, CA 92373-8100, USA.

ESRI, ARC/INFO, ArcCAD, ArcView, *Business*MAP, MapObjects, PC ARC/INFO, SDE, and the ESRI globe logo are trademarks of Environmental Systems Research Institute, Inc., registered in the United States and certain other countries; registration is pending in the European Community. 3D Analyst, ADF, ARC COGO, the ARC COGO logo, ARC GRID, the ARC GRID logo, the ARC/INFO logo, AML, ARC NETWORK, the ARC NETWORK logo, *ArcNews*, ARC TIN, the ARC TIN logo, ArcInfo, the ArcInfo logo, ArcInfo LIBRARIAN, ArcInfo—Professional GIS, ArcInfo—The World's GIS, ArcAtlas, the ArcAtlas logo, the ArcCAD logo, the ArcCAD WorkBench logo, ArcCatalog, the ArcData logo, the ArcData Online logo, ArcDoc, ARCEDIT, the ARCEDIT logo, ArcEurope, the ArcEurope logo, ArcEditor, ArcExplorer, the ArcExplorer logo, ArcExpress, the ArcExpress logo, ArcFM, the ArcFM logo, the ArcFM Viewer logo, ArcGIS, ArcIMS, the ArcIMS logo, ArcLogistics, the ArcLogistics Route logo, ArcMap, ArcObjects, ArcPad, the ArcPad logo, ARCPLOT, the ARCPLOT logo, ArcPress, the ArcPress logo, the ArcPress for ArcView logo, ArcScan, the ArcScan logo, ArcScene, the ArcScene logo, ArcSchool, ArcSDE, the ArcSDE logo, the ArcSDE CAD Client logo, ArcSdl, ArcStorm, the ArcStorm logo, ArcSurvey, ArcToolbox, ArcTools, the ArcTools logo, ArcUSA, the ArcUSA logo, *ArcUser*, the ArcView GIS logo, the ArcView 3D Analyst logo, the ArcView Business Analyst logo, the ArcView Data Publisher logo, the ArcView Image Analysis logo, the ArcView Internet Map Server logo, the ArcView Network Analyst logo, the ArcView Spatial Analyst logo, the ArcView StreetMap logo, the ArcView StreetMap 2000 logo, the ArcView Tracking Analyst logo, ArcVoyager, ArcWorld, the ArcWorld logo, Atlas GIS, the Atlas GIS logo, AtlasWare, Avenue, the Avenue logo, the *Business*MAP logo, DAK, the DAK logo, DATABASE INTEGRATOR, DBI Kit, the Digital Chart of the World logo, the ESRI Data logo, the ESRI Press logo, ESRI—Team GIS, ESRI—The GIS People, FormEdit, Geographic Design System, Geography Matters, GIS by ESRI, GIS Day, the GIS Day logo, GIS for Everyone, GISData Server, *Insite*MAP, MapBeans, MapCafé, the MapCafé logo, the MapObjects logo, the MapObjects Internet Map Server logo, ModelBuilder, MOLE, the MOLE logo, NetEngine, the NetEngine logo, the PC ARC/INFO logo, PC ARCEDIT, PC ARCPLOT, PC ARCSHELL, PC DATA CONVERSION, PC NETWORK, PC OVERLAY, PC STARTER KIT, PC TABLES, the Production Line Tool Set logo, *Route*MAP, the *Route*MAP logo, the *Route*MAP IMS logo, Spatial Database Engine, the SDE logo, SML, StreetEditor, StreetMap, TABLES, The World's Leading Desktop GIS, *Water Writes*, and Your Personal Geographic Information System are trademarks; and ArcData, ArcOpen, ArcQuest, *ArcWatch*, ArcWeb, Rent-a-Tech, Geography Network, the Geography Network logo, www.geographynetwork.com, @esri.com, and www.esri.com are service marks of Environmental Systems Research Institute, Inc.

The names of other companies and products herein are trademarks or registered trademarks of their respective trademark owners.

Security and ArcIMS

An ESRI White Paper

Contents **Page**

Security and ArcIMS

Introduction

Security is an important topic to consider when setting up Internet Web sites. Because of the inherent lack of security on the Internet, Web and system administrators must stay current with the latest security updates. Making a Web site 100 percent secure is a nearly impossible task, but taking some basic steps can eliminate most security holes. The purpose of this document is to identify and detail areas of security as they relate to ArcIMS™.

ArcIMS 3 provides a set of security features that allow you to build a secure Web site. ArcIMS can also be integrated with other popular authentication/security mechanisms.

This document covers the following topics about security and ArcIMS:

- Security concerns of a typical ArcIMS installation
- Security with the ActiveX and ColdFusion Connectors
- Leveraging Web server security
- Firewalls and ArcIMS

These topics will present the ArcIMS architecture as it relates to security and what levels of protection a Web site can provide.

Security Concerns of a Typical ArcIMS Installation

Review of MapServices and a Typical ArcIMS Installation

To understand the security concerns of ArcIMS, you should be familiar with the basics of publishing data in ArcIMS. To publish data through ArcIMS, you first author a Map configuration file (.axl). This file contains information about data sources and layer rendering. You then use the administration tools, either in ArcIMS Administrator or ArcIMS Manager, to publish the Map configuration file as a MapService. End users can view this MapService in a Web site you create in ArcIMS Designer or in ArcExplorer™ 3. If you want more information on this process, see *Using ArcIMS.*

In a typical ArcIMS installation, the ArcIMS Servlet Connector is installed. The purpose of the connector is to take requests coming into the Web server and pass them on to the Application Server. The Application Server then passes the request along to the ArcIMS Spatial Server. The ArcIMS Servlet Connector is a Java servlet.

Security Through ArcXML and Administrator Login

Through the ArcIMS Servlet Connector, you can send any valid ArcXML requests to the ArcIMS Spatial Server. The ArcIMS Servlet Connector does not check to see if the requests are unauthorized, but the requests can only use valid ArcXML functionality.

ArcXML functionality does not allow, for example, requests that might cause data corruption or illegal data access. This implementation provides security on the MapService in two ways: the users can only access data layers in the MapService, and they can only access the data layers through ArcXML.

ArcIMS provides user name and password protection for the administration tools. All administration requests come through the Servlet Connector and are encrypted between the ArcIMS Administrator and the Web server. Because the ArcIMS Servlet Connector resides on the Web server, you can administer your site from anywhere. This can be a disadvantage because anyone who knows the administrator login can administer your site. To avoid unauthorized use, change the default administrator login (user name: admin, password: admin). This is easily accomplished from the Tools menu. It is highly recommended that you change the default administrator login to control the security on your site.

Security Through Web Server Access and Custom Connectors

Another security measure is to move the ArcIMS Servlet Connector from an external Web server onto a Web server that has only internal access. In this configuration you install and administer the site on a secure internal Web server and have all requests for maps and other data come to ArcIMS as part of a request to an ActiveX or ColdFusion connector on the external server. More information on security with the ActiveX or ColdFusion connectors is discussed in the next section.

Security with the ActiveX and ColdFusion Connectors

A more secure configuration than the ArcIMS Servlet Connector provides can be implemented with the ActiveX or ColdFusion connector (custom connectors). Unlike the ArcIMS Servlet Connector that does not filter the ArcXML requests, the custom connectors contain logic that can filter out unauthorized messages. By using these connectors you can disable the ability to send ArcXML to the Web site and, in doing so, create a more secure and controlled site.

Using the custom connectors, a developer can easily integrate ArcIMS with an external security authentication system to allow for different levels of security. This has the advantages of leveraging an existing authentication mechanism and also gives the developer much more flexibility. Using this type of security helps address the issue of unauthorized access to data layers. For example, a site may want to restrict users to only view the data but not to query the attributes, or they may want to control access to MapServices based on the user login. This is a particular concern for large Internet sites with commercial data.

How ArcXML Is Handled by the Custom Connectors

The ArcIMS Servlet Connector works as an ArcXML pass-through. The ArcIMS Servlet Connector does not generate ArcXML or do any integrity checks on ArcXML—it simply accepts a MapService Name and an ArcXML string and forwards it to the Application Server, which then forwards it to the Spatial Server.

The custom connectors, on the other hand, are ArcXML generators. They run inside the Web server, take a request via a URL, convert that into an ArcXML request, and then forward it to the Application Server. The ArcXML request is generated by either directly writing an ArcXML request in the script or by the connector application programming interface (API) writing the ArcXML request.

In between the parsing of the URL and the ArcXML generation, a developer can perform security checks using ColdFusion or Active Server Page (ASP) security methods. For example, your ColdFusion script or ASP could connect to a Lightweight Directory Access Protocol (LDAP) server or database and look up user access rights to a particular MapService or layer. It could then respond with a message or display only the layer the user is authorized to see. An outline of this process using a ColdFusion script is shown below. (Note: The following example does not use the ColdFusion connector.)

1. The client calls a ColdFusion script (drawMap.cfm) with x and y parameters for the map extent:

   http://host/drawMap.cfm?minx=-180.0&miny=-90.0&maxx=180.0&maxy=90.0

2. ColdFusion parses the parameters from the URL.

```
<CFIF #ParameterExists(URL.minx)#><CFSET cminx = “#URL.minx#”></CFIF>
<CFIF #ParameterExists(URL.minx)#><CFSET cminy = “#URL.miny#”></CFIF>
<CFIF #ParameterExists(URL.maxx)#><CFSET cmaxx = “#URL.maxx#”></CFIF>
<CFIF #ParameterExists(URL.maxy)#><CFSET cmaxy = “#URL.maxy#”></CFIF>
```

3. Here you can insert your security script to check access rights to MapServices or layers and respond appropriately.

4. If the access is valid, then the appropriate ArcXML request is generated.

```
<CFSET AXLInput =
        '<?xml version="1.0"?><ARCXML
version="1.0.1"><REQUEST><GET_IMAGE><PROPERTIES>' &
        '<ENVELOPE minx="' & #cminx# & '" miny="' & #cminy# & '" maxx="' &
#cmaxx# &
        '" maxy="' & #cmaxy# & '" />' &
'<IMAGESIZE height="400" width="500" />' &
'</PROPERTIES></GET_IMAGE></REQUEST></ARCXML>'>
```

5. Finally, the ArcXML request is sent to ArcIMS.

```
<CFX_ESRIMAP ACTION="REQUEST"
SERVICENAME=#mapServiceName#
SERVERNAME=#serverName#
SERVERPORT=#serverPort#
CUSTOMSERVICE=""
AXLTEXT="#AXLInput#"
GENERATEHTML="false"
```

Web Server/Connector Configuration

To implement security in this way, the ArcIMS Servlet Connector should be located on a Web server instance that does not have external access. For example, you could be running two Web server instances on the same machine—one containing the ColdFusion or ASP connector and security scripts with external access and one containing the

ArcIMS Servlet Connector with internal access only. If the ArcIMS Servlet Connector is not on an internal Web server, users can access all the MapServices, thus bypassing the security implemented by ColdFusion or ASP.

Validating URL Parameters

When a user is in a browser, he or she can type any parameters into a URL and send off the request, potentially creating a breach in security. You as the Web developer can play an important role in securing your site by paying close attention to the URL.

By checking the validity of the parameters passed into the URL, you can avoid security problems before they happen. For example, check to make sure numbers are numeric values and parameters are in a certain range of values. If your URL passes parameters directly to a command line executable, check to ensure that it does not contain any malicious statements. A user could append extra commands to this type of parameter and execute something on your server without your knowledge or permission.

Leveraging Web Server Security

Most major Web servers on the market today implement some form of authentication. Some can integrate with sophisticated security servers. There are methods to integrate ArcIMS with such authentication mechanisms.

Authentication Mechanisms

When you enter a user name and password for a Web site, there are a few different types of authentication mechanisms that may be implemented to verify the login. Most Web servers support Basic and Digest Authentication; most browsers only support Basic authentication. If the Web server and Web browser allow, use Digest Authentication. Basic Authentication encodes your user name and password using a technique that makes it unreadable, but it is trivial to decode. Digest Authentication encodes your user name and password using a technique that makes it virtually impossible to decode.

URL Restrictions

An Internet protocol address restriction can be applied to a URL. This restricts access to a URL based on the user's IP address. For this type of restriction, no user name or password is required—instead, the request from the client application is checked showing that it is from a valid machine or set of machines. This allows you to restrict access to the ArcIMS Servlet Connector while allowing access to the MapServices from the Java applets and applications.

An additional level of security can be implemented on the Web server by restricting access to http://host/servlet/com.esri.esrimap.Esrimap. The Java viewer and HTML viewer handle this restriction differently. The HTML viewer continues to work with the restricted access because the browser automatically prompts for a user name and password. On the other hand, access is disabled through any Java applet or application that cannot handle authentication. This includes the ArcIMS Manager, ArcIMS Administrator, ArcIMS Designer, and ArcExplorer 3. This issue can be solved by having an unrestricted ArcIMS Servlet Connector to work with these applications. This configuration is discussed under "Web Server/Connector Configuration" on the previous page.

If ColdFusion or ASP is being used, you have the option to restrict access to the scripts or directories where the scripts run. For instance, in the example on the previous page, http://host/drawMap.cfm can be restricted to a chosen set of users.

J-8593

Firewalls and ArcIMS

When security is discussed, a main topic of concern is firewalls. With ArcIMS, the topic is focused on where to place the firewall in the ArcIMS architecture. This section provides a discussion of what to keep in mind when placing firewalls and what the advantages and disadvantages are.

Introduction to Firewalls

When you connect a machine such as a Web server directly to your Internet connection, the machine is wide open. This means that anyone could, for example, mount disks if they are shared or log on to the machine with malicious intent. Setting some strict security policies can prevent most of these security concerns. However, in some cases machines need to be accessible from the internal network, and the operating system is not flexible enough to implement this properly. This is where firewalls play their greatest role.

Firewalls are software or hardware that allows the administrator to monitor and block communication between different networks. This is especially needed when one of these networks is the Internet. A firewall usually works based on a set of rules set up by the administrator of the firewall. The rules define which types of communication the firewall allows and which are forbidden. A firewall also monitors all the connections to ensure they are not malicious; for example, the client can send a fake IP address to conceal the origin of the connection.

Whether you are implementing your firewall with hardware—for example, through a router—or software, the placement of the firewall is important in determining the kind of protection it provides to your Web site and internal network.

Placement of the Firewall and ArcIMS

When you are setting up an ArcIMS site, the placement of the firewall has a significant impact on the security that can be provided. In general, the more components outside the firewall, the less secure your site is. Three basic configurations are described below.

1. The firewall between the Internet and your Web server

   The recommended technique for configuring your firewall with ArcIMS is to put the firewall between your Internet connection and your Web server. In this configuration you need to expose the Web server port (usually port 80) so that it can be accessed from outside the firewall. All other access, for example, ftp and telnet, can be restricted.

   The advantages of this configuration are that it can be set up easily by a person with cursory knowledge of ArcIMS administration, and only the Web server is exposed. This is recommended over the following approach because all the Web server and ArcIMS components are behind the firewall.

2. The firewall between the Web server and the ArcIMS Application Server

   When your corporate information technology (IT) infrastructure requires you to place the Web server outside the firewall, you can still place ArcIMS behind the firewall, but it is a slightly more complex configuration. In this case, you place the firewall between the Web server and the ArcIMS Application Server. You open the

Application Server's communication port (usually port 5300) through the firewall so your Web server can communicate with ArcIMS. This allows access to the ArcIMS Application Server directly from the Internet and is a potential security risk. However, you can use the firewall to ensure that all access to the ArcIMS Application Server comes from the Web server.

When you publish Image MapServices, another level of complexity is added to the configuration. The ImageServer places images into a directory that the Web server can access to transfer them to the client. This is typically the /output directory and contains the GIF, JPG, or PNG files requested by Image MapServices.

For this configuration, the firewall needs to allow mapped drives, and the /output directory must be shared by both the Web server and ArcIMS (all machines running ArcIMS Spatial Server). There are two ways to set up the shared drive: (1) you could mount a drive on the Web server from a shared drive on the ArcIMS machine, or (2) you could mount a drive on the ArcIMS machine from the shared drive on the Web server. The first is usually a security concern since you are exposing an internal machine (the ArcIMS machine) outside the firewall. This allows, for example, external users to access files from an internal machine. The second configuration is recommended since your Web server machine is already exposed outside the firewall and having the shared drive does not create any additional security risks.

3. The "Demilitarized Zone"

   In most cases, the firewall is there to protect your company's internal network from unauthorized access from the Internet. Allowing any sort of access from the Internet weakens the firewall and could allow outside entities to break into your network. In order to prevent this, many companies set up a Demilitarized Zone (DMZ).

   The DMZ is a network entirely separate from the main internal network. The machines in the DMZ can be accessed from the outside but do not have any access to the machines on the internal network. If someone breaks into one of these machines, they can only get to other machines on the DMZ, not to the main internal network.

   In an ideal world, the DMZ would have no physical connection to the internal network, and the administrators and developers would work on a dedicated machine in the DMZ to perform data and file management tasks. A more typical configuration is to place a second firewall between the DMZ and the internal network. No access from the DMZ to the internal network is allowed, but access from the internal network to the DMZ is allowed. In this way people can administer the DMZ from the internal network. The firewall that protects the DMZ from the Internet can be the same one that protects the internal network from the DMZ—it is just a matter of setting up enough network cards and rules for the firewall.

   The advantage of this configuration is that it provides a buffer between external and internal systems, thus providing more security.

Protecting the Data

When an ArcIMS system is set up, typically the most precious part of the system is the spatial and attribute data being served to the Web. By using any of the above configurations, one layer of protection is being put in front of the data to block people from getting it.

If a database server is being used, such as ArcSDE™, a second layer of protection can be added. In the DMZ configuration, the ArcSDE server can be put behind another firewall. In this case the firewall has to allow access from the DMZ to the correct instance of ArcSDE that needs to be used (port 5151, by default). Also, any file with a user name and password in the DMZ should be removed or protected. This makes accessing the ArcSDE server much more difficult, but if someone breaks into the DMZ they will not be able to get to the ArcSDE machine directly.

Other Configurations

Many additional configurations are possible with ArcIMS. The examples described above are the most popular and least costly. Several layers of firewalls can be added for security, and several layers of network can also be added. In all cases it is a trade-off between security and complexity—as the network, and management of it, becomes more complex, your system becomes more secure.

Redundancy and Performance

When considering the implications of configuring ArcIMS with firewalls, redundancy and performance are two topics of interest.

ArcIMS was designed and built to be fault-tolerant and redundant so that if part of the system goes down, the rest of the system can still function. However, using a firewall as the gateway to your system introduces a single point of failure. Firewalls are generally reliable but, if for any reason the firewall goes down, your entire site can potentially be down for an extended period of time. This is a concern if high availability of your site is required. Most firewalls come with a fail-over mechanism that takes over if the main firewall fails.

Every layer of firewall that is added to the system has a negative impact on the performance of the system. For a simple firewall that does not enforce many rules, the bandwidth can go as high as 80 megabits per second (Mbps). When you implement more rules on the firewall, the speed of the connection decreases. In order to avoid having your firewall create a performance bottleneck, the main thing to consider is the bandwidth of the connections coming into and going out of the firewall. For example, if you have a 100 Mbps connection into and out of the firewall, you want to make sure the firewall maintains a bandwidth that is close to that. If your connection into the firewall is 100 Mbps and the connection out of the firewall is only a T1 line (1.5 Mbps), then the firewall will not be an issue because it can maintain the outgoing bandwidth while enforcing many rules.

For more than 30 years ESRI has been helping people manage and analyze geographic information. ESRI offers a framework for implementing GIS in any organization with a seamless link from personal GIS on the desktop to enterprisewide GIS client/server and data management systems. ESRI® GIS solutions are flexible and can be customized to meet the needs of our users. ESRI is a full-service GIS company, ready to help you begin, grow, and build success with GIS.

Corporate

ESRI
380 New York Street
Redlands, California
92373-8100, USA
Telephone: 909-793-2853
Fax: 909-793-5953

For more information
on ESRI call

1-800-447-9778

(1-800-GIS-XPRT)

Send e-mail inquiries to

info@esri.com

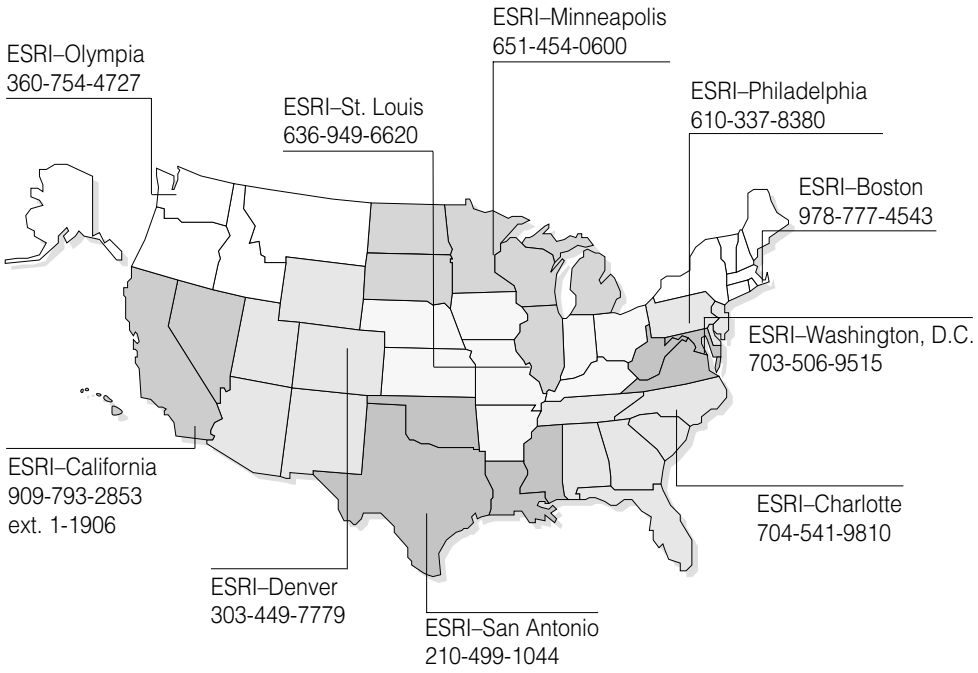
Visit ESRI's Web site at

www.esri.com

Outside the United States,
contact your local ESRI distributor.
For the number of your distributor,
call ESRI at 909-793-2853,
ext. 1-1235,
or visit our Web site at
www.esri.com/international

GSA Federal Supply Schedule
No. GS-35F-5086H

Regional Offices



International Offices

Australia
61-89-242-1005

Belgium/Luxembourg
32-2-460-7480

Canada
416-441-6035

France
33-1-46-23-6060

Germany and Switzerland
49-8166-677-0
41-1-360-2460

Hong Kong
852-2730-6883

Hungary
361-428-8040

India
91-11-620-3802

Indonesia and Malaysia
62-21-570-7685
603-7874-9930

Italy
39-06-406-96-1

Korea
82-2-571-3161

Netherlands
31-10-217-0700

Poland
48-22-825-9836

Romania
40-1-231-13-81

Singapore
65-742-8622

Spain
34-91-559-4375

Sweden
46-23-755-400

Thailand
66-2-678-0707

United Kingdom
44-1296-745-500

Venezuela
58-2-285-1134

Printed in USA