Introduction

Rumors of my death have been greatly exaggerated.
—Mark Twain

Tell a new university graduate that you work on mainframe security, and chances are he or she will look at you incredulously and say, "Do they *still* have mainframes?"

As in the famous quote from Mark Twain, rumors of the death of mainframes have been greatly exaggerated. Mainframes are not only alive and well; they are, in fact, the backbone of almost all IT installations in large corporations, and in many medium-sized companies, too.

About Mainframe Security

One of the strengths of the mainframe is its security. Compared to other computing platforms, mainframe security is versatile and robust. There are good reasons for this.

Mainframes have always been designed with multiple users in mind. Basic security considerations were laid out in the very foundation of the operating system, right from the start, to protect information, data, program code, and whatever else might be shared. Contrast this with the history of personal computers. Even the name "personal computer" implies that it would not be shared! These small machines were initially meant for single users only;

therefore, no thought was given to security. And so it is that in the world of personal computers, security evolved after the fact. It was added later in their evolutionary process, and only as the need arose.

There's another reason why mainframe security is miles ahead of rival platforms: personal computers were initially targeted for non-business applications, such as gaming and word processing. Mainframes, on the other hand, were built to provide financial benefits to large organizations such as financial institutions, where it would be unthinkable not to consider security from the very beginning.

Due to the superior design, performance, and stability of the mainframe system, there has been very little need to constantly update the tools and menus that accompany it. TSO, ISPF, JCL, RACF®, and other mainframe products look and feel very much the same today as they did 30 years ago. Personal computers, on the other hand, are constantly evolving, so time must be dedicated to learning their constantly changing tools and interfaces.

Lastly, the very fact that mainframes are housed behind locked doors and at nondescript locations provides a large measure of physical security. Access to them is via terminals or personal computers using secure connections such as Virtual Private Network, or VPN. Quite often, a person working on a corporation's mainframe does not even know where the physical machine is located—and does not care. This is in sharp contrast to personal computers sitting in front of you, with their ubiquitous "Ctrl-Alt-Del" shutdown provision at your fingertips. Also, most PCs come equipped with a CD or DVD drive that can potentially be used to siphon away corporate data.

This is not to say that mainframe security was always as secure as we know it today. Over time, the technology evolved, and with it, security was strengthened. The inherent benefits of mainframe security, however, are not to be taken for granted. It is left up to the installation to customize and implement many of the optional, installation-specific security features.

The proper implementation of mainframe security cannot be over-emphasized. It is vital to secure corporate assets. Auditors, both internal and external, are always on the lookout for security breaches, especially after incidents such as the Enron debacle. There are also compliance requirements, such as the

Sarbanes-Oxley Act in the United States, which mandate that adequate security and safeguards be in place to protect shareholder interests. In fact, there are even legal obligations on corporations to guard their information assets.

Mainframe security is as much about guarding business data as protecting the operating system features prone to misuse and abuse. Therefore, security practitioners must involve both application developers and system programmers to implement security. As you shall see in this book, the operating system (IBM® z/OS® or one of its predecessors, IBM OS/390® or IBM MVS™) has a number of security-related concerns that must be addressed to achieve an overall security comfort level.

About This Book

This book describes practical, real-life security issues and their solutions, gleaned from over 30 years of mainframe security experience. Wherever appropriate, quizzes are provided so you can test your knowledge with their questions and learn from their answers.

RACF, the IBM security software, is used throughout this book. Mainframe professionals who use other security software (such as ACF2 or Top Secret from CA Technologies) can also benefit from some parts of this book, as the concepts and ideas explained here apply to mainframe security in general, without regard to any particular security software.

To impart knowledge in the best way possible, the book is broken up into three major areas.

The first part focuses on how to deploy RACF properly to protect your company's business assets. RACF is, after all, just a tool to do this, and like all products that do many things, it is a complicated piece of software. Beginners to mainframe security might not appreciate all the subtle aspects of RACF. There are many levers and controls at their disposal, and using them improperly can lead not only to the inadequate protection of corporate data but even to open security "back doors" that could go unnoticed for a long time.

If RACF is complex, the z/OS operating system is even more so. It, itself, needs to be secured, and this is something many security professionals ignore.

There are two main reasons for this oversight: first, most security professionals are too busy doing daily security administration work, and second, even if they had the time, most of them do not understand the complexities of the z/OS operating system. The second part of this book, therefore, identifies the main areas of security weaknesses within the z/OS operating system and offers solutions in each case to mitigate, or close the security "gaps," as an auditor might say.

The third part of this book deals with many issues related to laying a strong security infrastructure, one that would be conducive to planting a solid security environment. Without this foundation, you cannot reap the benefits described in the other two parts of the book. The areas mentioned here must be nurtured in order to have a healthy security moat around the corporation's data.

Throughout the book, there are special sections titled, "How Secure Is *Your* Installation?" These sections will help you gauge the state of security at your installation, and strengthen it where necessary.

Who Should Read This Book

This book was written with the mainframe security practitioner in mind. However, its contents will also be useful to any IT professional who works on the mainframe platform and needs to understand its security. IT auditors will benefit by better understanding potential security weaknesses and their remedies.

The book takes the beginner beyond the basic mainframe security and RACF knowledge. For this reason, no attempt is made to explain basic RACF commands and their syntax—this information is readily available in IBM manuals. Also, basic knowledge about the mainframe, such as TSO and JCL, is assumed.