Licensed by the Texas Private Security Bureau

# Mainframe Penetration Testing

## What atsec offers

atsec has unparalleled expertise, skills and knowledge of mainframes. We are the company that has evaluated z/OS and other applications at the stringent EAL4 and EAL5 levels for the Common Criteria certification. These evaluations include thorough analysis of security functionality using design information from the architectural level to source code analysis. Included are independent tests (penetration tests) as well as assessment of developer testing and a thorough vulnerability analysis.

IBM z/OS

IBM z/VM

IBM DB2

IBM LPAR

IBM GS/Kit

IBM PR/SM

Vanguard Enforcer 7.1 EAL 3+

Oracle Database 10g

Check http://atsec.com/us/common-criteria-certificates.html for the full list.

Our principal consultants have many years of expertise including working with IBM in the design and development of security (RACF) software.

In order to offer the widest possible range of solutions, our consultants first define the attack profiles most appropriate for your organization. We provide methodology-level advice about planning and executing penetration tests in cases where very specific knowledge is required to analyze and present the results.

Our mainframe operating system penetration testing uses a four-step process to exploit your mainframe either via authorized access or by compromising access control mechanisms:

Organizational Review - to obtain an overview of the operational environment and security infrastructure, as well as establish project working protocols and goals.

System Audit - to further understand, in depth, the system configuration, enabling identification of potential vulnerabilities in the configuration. The audit identifies areas to potentially exploit for penetration.

Penetration Test - perform manual and automated penetration tests based on the acquired knowledge of the environment obtained in the previous steps and industry standard methods.

Security Impact and Recommendations - provide security impact statement and recommendations. These recommendations can be used as input to a risk treatment plan in order to implement recommended corrective actions.

### What exactly will happen during the penetration test phase?

atsec analyzes the common interfaces used to transition from user state to system state, looking for integrity exposures that would allow an unauthorized user to exploit the interface in a way to gain system level authorities. The goal is to produce PoC exploits for z/OS Supervisor Calls (SVC) interfaces and z/OS Program Call (PC) interfaces. The SVCs analyzed include user and vendor supplied SVCs, along with IBM supplied SVCs that have been either “front-ended” or “hooked”. Other IBM SVCs will typically not be analyzed due to having them already analyzed during the z/OS Common Criteria evaluations.

atsec uses automated tools to determine a definitive list of PC’s defined to the system. The list of PC’s is then trimmed to eliminate those PC’s which require the caller to be in supervisor state or with a Program Key Mask of 0-7, since these are already implicitly trusted. Priority is then given to analyzing PC’s that are available globally to all address spaces on the system.

atsec uses both manual and automated means to probe, test and analyze the user/vendor, “hooked” and “front-ended” SVC’s and the trimmed list of PC’s for insecure aspects. These insecure aspects might allow unauthorized access to information processed by the system, escalation of privileges, exploitation of vulnerabilities and circumvention of security functions. The analysis will concentrate on errors in parameter validation, parameter protection, “time of check” to “time of use” of parameters and storage into unverified locations.

Last, atsec develops methodologies for exploiting the potential vulnerabilities discovered. Code and/or procedural based exploits are developed to demonstrate the vulnerabilities found to facilitate interactions with the vendor responsible for the code containing the vulnerabilities. Code based exploits may utilize Assembler, REXX, CLIST and common utilities to demonstrate vulnerabilities. The development of exploits may be time consuming and is only performed by prior agreement.

## Why our services are important to you

The most prevalent attacker cited in most threat models is the insider. With mainframes threats involving insider attackers are a very serious issue. Mainframes are notoriously difficult to configure properly, and are very complex.

Many good companies, including financial institutions, insurance companies, and telecommunication companies realize the need to test the security posture of their mainframe systems and the applications that run on them. Whether this is necessary to meet regulatory requirements or is performed for “peace of mind” or for risk management purposes atsec have the expertise to perform a professional and thorough job.

z/OS penetration tests are deployed to assess the technical security of a single system, a large complex network, or a specific application from an attacker’s point of view. Even a well planned infrastructure design does not prevent the technical implementation from containing vulnerabilities. Those vulnerabilities can only be reliably detected by penetration testing, where extensive knowledge and experience are used to search for erroneous configurations and flaws in the programming.

Regular penetration tests are an appreciated measure to guarantee a current overview of your company's security. Deficiencies in organizational processes for intrusion detection and reaction can be identified. Penetration testing shows whether a company's security policy is a living document or just another piece of paperwork.

## For more information

Please contact us at info@atsec.com for more information.