

## **Ingrian Networks**

### Product Penetration Test of the i140 Secure Networking Platform

Final Report

April 3, 2002

#### **mission**

@stake offers comprehensive digital security consulting services for Global 2000 businesses whose success depends upon developing secure electronic relationships with customers, suppliers, partners and employees. With practice areas serving financial services, communications service providers and e-markets, @stake applies industry expertise and pioneering research to design and build strategic security solutions that enable long-term e-business objectives.



Where Security & Business Intersect<sup>SM</sup>

[www.atstake.com](http://www.atstake.com)

565 COMMERCIAL STREET

SAN FRANCISCO, CA 94111

MAIN: 415.392.6900

FAX: 415.392.8100



Copyright ©2002 by @stake, Inc.  
All Rights Reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the written permission of @stake, Inc.

While every precaution has been taken in the preparation of this document, @stake, Inc. assumes no responsibility for errors, omissions, or for damages resulting from the use of the information herein.

Products or corporate names may be trademarks or registered trademarks of other companies and are used only for the explanation and to the owner's benefit, without intent to infringe.

# Contents

- Executive Summary ..... 1**
- Introduction..... 1
- Analysis Methodology and Tools..... 1
- Conclusion..... 1
  
- Business Context ..... 2**
- Business Objectives ..... 2
- Critical Success Factors ..... 2
  
- Objectives and Process ..... 3**
- Goals and Objectives ..... 3
- Analytical Process ..... 3
  
- Analysis Findings..... 4**
- Network Security ..... 4
- Network Security ..... 4
- User Account Security..... 5
- Certificate Security ..... 5
- Conclusion..... 5
  
- Appendix A: Analytical Tools Used..... 6**

## Executive Summary

### Introduction

@stake worked with Ingrian Networks (Ingrian) to perform a Blind Product Penetration Test of the i140 Secure Networking Platform and its related infrastructure. Blind Product Penetration Tests provide insight into methods of attack against a product in a specific environment, and present a reasonable example of what an attacker might accomplish. @stake's goals were to model specific threat scenarios, locate vulnerabilities, and validate specific exploitation possibilities.

The engagement had the following key objectives:

- Identify key areas of vulnerability, including but not limited to, authentication and access control mechanisms, input validation, privilege escalation, and integrity of private keys
- Attempt to exploit potential vulnerabilities, and determine the extent of unauthorized access obtained via those vulnerabilities
- Check third-party products supporting the application for the existence of any known vulnerabilities that could lead to a compromise
- Perform risk assessment to identify critical areas of exposure and difficulty of exploit

During this blind penetration assessment, no prior intelligence regarding the product implementation was provided to the @stake testing team. The mechanisms and protocols encountered were reverse-engineered and analyzed in an attempt to identify any exploitable weaknesses that would compromise the specific business objectives of the product.

The engagement began on December 18, 2001 and ended on January 25, 2002. All testing was performed from the @stake labs.

### Analysis Methodology and Tools

@stake conducted its analysis of Ingrian's i140 Secure Networking Platform through on-site interviews, desk research, and consultation with the @stake internal knowledge base. The penetration testing was performed from an external perspective, where the i140 was implemented outside a firewall and access was attempted from the Internet. Additionally, tests were performed simulating an attacker who has physical access to the device.

### Conclusion

@stake team was unable to expose any vulnerabilities during this engagement. In general, the i140 Secure Networking Platform incorporates sound security design principles including strong key management and operating system integrity. Additionally, operating in its primary task as a secure reverse proxy server, the device did not appear to introduce additional security risk to a network environment. As a core security design principle, the default installation contains no open ports and no default administration account/password. The device also provides strong protection of the private keys. @stake recommends that the secure design principles practiced by Ingrian continue through the lifetime of the product.

## Business Context

### Business Objectives

Ingrian's mission is to provide secure, performance-oriented, end-to-end content delivery mechanisms for high-volume Internet networks worldwide. Ingrian products are designed to mitigate performance degradation associated with processing encrypted content through traditional load balancers and web servers. Software and hardware solutions developed by Ingrian focus on integrating performance, load balancing capabilities and secure transmission features within an affordable, extendable platform. As a result, Ingrian's customers can improve network performance, while preserving the security of front-end management and encrypted backend storage.

Business objectives must include the ability to:

- **Enable** businesses to maximize end-to-end network performance
- **Perform** all system management and content delivery in a secure manner that exceeds industry practices
- **Provide** a scalable and affordable solution that can be easily integrated into customer environments

### Critical Success Factors

In order for Ingrian to maintain and extend its leadership status in the secure content delivery market, the i140 Network Appliance needs to provide:

- **Secure content delivery.** Ensure reliable and secure delivery of critical data through tested security features including secure caching, access management and a FIPS 140 compliant key management system
- **System performance.** Continually improve system performance through SSL acceleration to minimize the performance impacts of encrypting content transmissions and maximize customers' business throughput
- **Ease of deployment.** Minimize capital expenditure and facilitate deployment and configuration of the appliance within customers' environment
- **Deny intruders platforms for attack.** Multi-party integration over the Internet exposes all involved to risk. The total security of a system is only as strong as its weakest link.

## Objectives and Process

### Goals and Objectives

@stake worked with Ingrian to perform a Blind Product Penetration Test of the of the i140 Network Appliance and its related infrastructure. As part of the engagement, @stake performed a “black box,” or uninformed penetration test of the i140 Network Appliance. Key engagement objectives entailed helping Ingrian detect and resolve security issues. The following factors were considered within the scope of this engagement:

- **Investigate** the i140 Network Appliance for vulnerabilities
- **Assess** the level of security needed for the i140 Network Appliance to interact securely with remote users
- **Recommend** best practice solutions for the design or configuration of i140 Network Appliance components including issues in need of immediate resolution and areas of potential weakness

The application assessment consisted of desk research, penetration testing, and a technical analysis of the i140 Network Appliance. Focus areas included:

- Vulnerabilities inherent in the i140 Network Appliance
- Opportunity and expertise required of an attacker to exploit various technical weak points in the i140 Network Appliance
- Relevance of local exploits in relation to remote access exploits

### Analytical Process

@stake employed several analytical methods to find security weaknesses in the i140 Network Appliance, including the ones listed below:

- Reviewed the i140 Network Appliance technical documentation
- Conducted Internet research for background material regarding various crypto accelerator cards
- Consultation with @stake Research and Development and internal knowledge sharing
- Analyzed remotely accessible endpoints, including open ports, communication protocols, and other services offered
- Analyzed the underlying architecture of the i140 Network Appliance as it applies to the external interfaces

## Analysis Findings

@stake organized analysis findings into the following sections:

- Operating System Security
- Network Security
- User Account Security
- Certificate Security

Each section addresses key focus areas that arose from the analysis findings.

### Operating System Security

Overall, the underlying operating system of the Ingrian Networks i140 Secure Networking platform is very secure. It appears that security has long been a consideration during the development of the product. Some of the precautions on the platform include encrypted configuration files, read-only file systems, “chrooted” processes, the removal of unnecessary system utilities, and file permissions designed to limit access to sensitive files. These are all best-in-class security practices.

Additionally, the platform utilizes a read-only root filesystem. This practice is highly recommended as it prohibits an attacker from adding or replacing binaries on the system. Further, it ensures that system configuration files do not change accidentally. Again, this is a best-in-class security practice.

### Network Security

Network security is of primary importance to potential clients of the Ingrian Networks platform, as they may not want to add additional components to a secure network configuration unless they can be assured that the additional components will not increase their risk. @stake found that overall, the Ingrian Networks platform provides strong network security:

- No known remote vulnerabilities that would result in a compromise within the i140 implementation were discovered during this investigation;
- The platform has a minimum number of services enabled and where possible, secure forms of communication are used (e.g. ssh instead of telnet);
- The secure reverse proxy service on the i140 device was found to be stable and did not appear to expose any vulnerabilities.

## User Account Security

Overall, the user account security for the Ingrian Networks i140 platform is very strong. By design, the platform allows administrators to view all configuration items throughout the device, however the ability to change these configurations was disallowed. Ingrian Networks is currently addressing this point to provide its clients the flexibility to deploy the platform with more limited data viewability.

## Certificate Security

The primary defense of the cryptographic keys for Ingrian's SSL device is reliant on a hardware cryptographic module. This cryptographic module, and the way that Ingrian interfaces with it, is the focus for the following analysis segment.

Cryptographic modules, like the one used by Ingrian, are covered under the Federal Information Processing Standards (FIPS) 140-1 created by the NIST - National Institute of Standards and Technology (formerly the National Bureau of Standards). This standard specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information in computer and telecommunication systems (including voice systems) that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code.

The FIPS 140-1 standard was developed by a government and industry working group composed of both users and vendors. The working group identified four security level requirements for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data), and a diversity of application environments (e.g., a completely unprotected location, an office, and a guarded facility). Each security level offers an increase in security over the preceding level.

## Conclusion

Overall, the underlying operating system of the Ingrian Networks platform is very secure and it's clear that security has long been a consideration during the development of Ingrian Network's platforms. @stake's evaluation addressed a number of areas critical to networking security including network security, user account security and certificate security, and found that the Ingrian Networks platform consistently delivered outstanding results. In fact, @stake's penetration test of the Ingrian Networks platform identified no exploitable vulnerabilities, and confirmed that the platform incorporates industry-leading security design principles including strong key management and operating system integrity. @stake is confident that the addition of an Ingrian Networks Secure Networking platform to a network infrastructure could provide an additional level of security while introducing no additional security risks.

## Appendix A: Analytical Tools Used

The following analytical tools were used during this engagement:

**Nmap** – A free port scanner, used to evaluate if any ports were listening on the device.

**Nessus** – A free vulnerability scanner, used to verify @stake's observation that the device was not vulnerable to standard attacks.

**Custom @stake Nessus modules** – Over the years, @stake has incorporated additional checks into the Nessus scanner. These checks are for proprietary exploit and vulnerability conditions not covered in the standard release.

**SNMPWalk** – A UNIX utility used to access and browse the snmp MIBS of a system. This tool was used to evaluate the security of the SNMP daemon.

**Standard HTML Browser** – (e.g Netscape and Internet Explorer) Used to access the Administrative web application. Attacks were sent via standard HTML commands such as POST and GET.

**Large-closed-source-webserver-fuzzer** – The fuzzer is a proprietary @stake tool designed to automate certain classes of attacks against web servers. Specifically, the fuzzer will attempt to enumerate all valid extensions on a web server and then try to cause exceptions by sending various quantities and types of data. The results are then provided to the user for analysis.

**Netcat** – Often called the network Swiss-army knife, Netcat is a publicly available, multipurpose socket handler originally developed by one of @stake's R&D personnel. Netcat was used to test the device for sshd vulnerabilities as well as provide standard shell and file transfer functions.

**Ethereal** – Ethereal is a network sniffer with a robust, built-in, protocol analyzer. Ethereal was used in conjunction with most of the Network attacks and tools to monitor the packets as they entered and exited the device. Often, with proper analysis, weaknesses in native IP protocols can be discovered in this manner.

**Sping, et, al** – Sping and other programs like it are designed to facilitate in the creation of custom packets (ICMP packets in the case of Sping) The device can then be tested using custom packets to help magnify potential issues under investigation and to discover new attacks against the device.

**UNIX System Tools** – In addition, the following Unix system tools were used:

- find – used to locate files on a filesystem by name, permissions, and others
- grep – used to locate text within files or locate files with text
- ps – lists active processes running on a system
- perl – “The UNIX Swiss-army knife.” used for various utility scripts and analyses

