Federated Networks Application Security Layer (ASL) Protocol Vulnerability Assessment

11/22/10

Introduction

BT performed a vulnerability assessment against Federated Network's Connect Secure Application Security Layer (ASL) Protocol. The overall purpose of this assessment was to identify application and protocol level security issues that could adversely affect or compromise network protocol communications.

BT has extensive experience helping clients secure their application and network infrastructures and evaluate the effectiveness of protections to the loss of intellectual property. Our Security Consultants have helped many of the world's largest institutions protect their Web-based service delivery systems and we have assisted clients that offer electronic commerce solutions. **BT's Global Ethical Hacking Center of Excellence** (EHCOE) is one of the largest security practices in the world, The team consists of a security community of 1800+ full time client facing consultants / architects / designers, including R&D/V. These industry leading resources that have produced over 20,000 engagements, 100 registered patents, 190 security papers, 108 registered patents. BT is recognized in the industry as "highest capability maturity" by the NSA and "Of the top Three" from Gartner. BT' engagements do not simply perform "scans" of a client's network. We perform highly detailed tests with our proven process and methodologies based from over 20,000 engagements. As not all vulnerabilities fall under the category of a specific published vulnerability, we also employ a proprietary library of manual tests and custom developed tools that are used to check for hard-to-find vulnerabilities, as well as many well-known commercial and public domain tools.

The assessment was conducted by consultants from the BT Ethical Hacking Center of Excellence (EHCOE), an industry leader in protecting business critical information assets.

Description of Testing

At the request of Federated Networks, BT has performed an application vulnerability assessment against the Federated Networks application identified in the Federated Networks FN ASL Protocol/ Network Vulnerability Final Report.pdf

The objective of the Federated Networks FN ASL Protocol/ Network Vulnerability Assessment was generally to determine the overall network/protocol security, including but not limited to an assessment of the FN ASL Protocol to thwart known limitations and vulnerabilities of SLL and/or its implementations, such as by way for example, Phishing, Pharming, DNS Poisoning attacks of any kind as well as sniffers and proxies, as outlined in greater detail in Appendix B.

BT has developed a customized process for conducting Ethical Hacking assessments of applications. This testing is designed to assess the security of the Federated Networks applications. BT performed a vulnerability testing against the applications to attempt to determine the extent to which an attacker can view, alter, or delete information without proper authorization.

This type of test includes many of the same testing methodologies that are used during a Web Application Testing Ethical Hacking assessment. However, this type of test focuses on the **software components in addition to the server systems.** The purpose is to attempt to collect as much information as possible about the application and server communication and to manipulate the client software without having inside knowledge of how the components operate.

BT took two approaches to examining the security controls being provided by the software. For the testing, BT's EHCOE posed as:

1. **Unauthorized users:** For example, an unauthenticated attacker that happens to target the application. BT will test the integrity of the application and strength of the authentication mechanism, as well as check for vulnerabilities associated with the application.

2. **Authorized users:** For example, a customer with access to the application that attempts to exceed the intended privileges and authority. As an authorized user, BT will test the security provided by the authentication mechanism and session management mechanism. Attempts will be made to bypass the normal, or given, authentication process. In addition, using Federated Networks provided test accounts, BT will attempt to bypass the session management capabilities and gain access to parts of the application normally not authorized for access. This is assessed by testing vertical and horizontal privilege escalation. For example, vertical privilege escalation is the ability of a regular user to access an administrator's role. Horizontal privilege is the ability of a regular user to access another role that is of the same type (or role). BT will also attempt to manipulate or enumerate the backend database of the application.

During this testing, BT utilized several test or "dummy" accounts created by Federated Networks for the testing. BT attempted to view and modify information between these test accounts without utilizing the passwords for the accounts. BT also attempted to circumvent assigned user access rights and gain access to functionality not otherwise authorized for access.

BT has created a documented, proprietary methodology for conducting these tests. Tests that BT may have performed as part of the Web Application Ethical Hacking assessment include, but are not limited to, the following:

1. **Strength of the session credentials used by type:** URL rewriting, cookies, hidden form elements and HTTP authentication (Basic, NTLM, Digest, etc.). BT will test for the predictability of session tokens, whether or not it is subject to manipulation, cloning, or hijacking and other common weaknesses in the mechanism employed to track user sessions.

2. **Strength and proper logic flow of server executables** (.CGI, .ASP, .ASPX, .PHP, Cold Fusion, PERL, etc.), and the lack of proper bounds checking, which can lead to buffer overflow attacks.

3. Strength of the login function against common attacks such as username enumeration/harvesting and password brute-forcing. Proper and complete use of the logout and timeout functions will also be tested.

4. Examination of ASL encryption used.

5. Analysis of all information passed across the communication channel between the client software and the server. BT will capture information, and attempt to manipulate and replay the information that has been captured. In addition, BT will attempt to modify the client-server network communication in real-time where possible.

6. Appropriate use of warnings and error messages and browser warnings such as unsigned code, AutoComplete, etc.

Additional testing that was performed is itemized in Appendix A, but generally focused on known weaknesses and limitations of the SSL protocol and/or current implementations. This information was provided directly from Federated Networks.

Various commercial, publicly available, and BT developed proprietary tools are used during testing. Publicly available tools used by BT have undergone a detailed review and evaluation. Review methods include—but are not limited to—validation of functionality, source code review, and sniffer log analysis. A detailed but obfuscated list of the tools and exploits utilized as part of this test are outline in Appendix B.

Other Federated Networks and third-party vendor systems, such as the underlying network infrastructure, were beyond the scope of this project. This testing also did not attempt any active network-based DoS attacks. Upon completion of the testing, BT presented all identified vulnerabilities/risks to Federated Networks in a detailed final report. Each vulnerability or risk identified was categorized as high, medium, or low, as follows:

High Risk: These findings identify conditions that could directly result in the compromise or unauthorized access of a network, system, application, or information.

Medium Risk: These findings identify conditions that do not immediately or directly result in the compromise or unauthorized access of a network, system, application, or information, but do provide a capability or information that could, in combination with other capabilities or information, result in the compromise or unauthorized access of a network, system, application, or information.

Low Risk: These findings identify conditions that do not immediately or directly result in the compromise of a network, system, application, or information, but do provide information that could be used in combination with other information to gain insight into how to compromise or gain unauthorized access to a network, system, application, or information. Low risk findings may also demonstrate an incomplete approach to or application of security measures within the environment.

Notes: In addition to Findings, our reports also may contain Notes. Notes can include testing notes, discussions of security best practices, and other supplemental information that may not necessarily be related to the security posture of the systems tested.

Testing Results – Summary Opinion

The vulnerability assessment and testing was performed as outlined above against Federated Network's Secure Connect Application Security Layer Protocol (ASL). As part of this assessment, BT presented all findings to Federated Networks. As a result of the testing and verification process completed on November 3, 2010, BT can confirm that there are **no open High-Risk, no open Medium-Risk, and no open Low-Risk** vulnerabilities identified at this time. Furthermore, the FN ASL Protocol completely mitigated those known limitations and vulnerabilities of SLL and/or its implementations, such as by way for example, Phishing, Pharming, DNS Poisoning attacks of any kind as well as sniffers and proxies, as outlined in greater detail in Appendix B.

Cautionary Note

The application assessments that BT performed was based on past experiences, currently available information, and known threats as of the date of testing. Given the constantly evolving nature of information security threats and vulnerabilities, there can be no assurance that any assessment will identify all possible vulnerabilities, or propose exhaustive and operationally viable recommendations to mitigate those exposures.

The statements relevant to the security of the Federated Networks applications in this letter reflect the conditions found at the completion of testing.

In accepting our report on the Federated Network's Connect Secure Application Client, FN Protected WebGoat Application, and Connect Secure Application Security Layer (ASL) Protocol, Federated Networks has acknowledged the validity of the above cautionary statement. BT also strongly recommends that any network, information system, or online application be subject to periodic reassessment and policy review, in addition to complementary training of the key support personnel on such policies and procedures for the above infrastructure in order to maintain a strong security profile in the face of potential threats.

Appendix A

The following information was provided to BT from Federated Networks. The following additional testing will be performed against the Connect Secure software solution:

1. **Hack/obtain the users password** to a website, either on first time input or subsequently, by any means by way of example, to potentially include but not be limited to:

   a. Phishing, Pharming, DNS or cookie poisoning

   b. Sniffing of any form

   c. Side channel attacks

   d. Man-in-browser or any form of man-in-middle

   e. Proxy

   As such BT performed the following actions to test the Connect Secure software solution:

   • BT attempted to attack a user that was protected with the ASL protocol to perform DNS cache poisoning, though the DNS cache poisoning attack succeeded, the encrypted information was considered useless and as such made all further attack scenarios useless.

   • BT attempted to conduct Arp cache poisoning in order to sniff the traffic that was being protected by the ASL protocol, when the traffic was obtained, the ASL encrypted information was totally useless and as such made all sniffing attempts useless.

   • BT employed advanced browser exploitation techniques to decrypt any ASL protected information, and attempted to strip off the encryption to subject all traffic to cleartext exploitation, the ASL protocol proved to more than adequately protect all information without any information compromised.

   • BT used advanced proxy techniques to intercept and attempt to decrypt and bruteforce information protected by the ASL protocol, none of the attempts were proven to be useful, and as such all proxy attempts failed.

2. **Assuming you were able** to obtain the full users login credential by some other means, such as the dreaded “sticky tab” attack attempt the following:

   a. Given you have the users login credentials to a website, login from a standard machine i.e. no FN Client software installed

   b. Given you have the users login credentials to a website (but not their fn client), attempt to login a different machine with different FN Client software

To satisfy the given test scenarios, BT attempted to compromise the FN protected user's account information by performing the following actions:

- BT attempted to connect to a ASL protected site and utilize the give Administrator credentials (i.e. root on *nix based systems) with no FN client, but because the service was Tcp-Wrapped and did not allow for raw HTTP connections, BT was in no way able to connect to the administrative console to utilize the given credentials.

- BT utilized a system with FN Client software installed, and used the supplied administrative credentials to attempt to log into the application; however the FN protected site properly stopped every attempt to gain unauthorized access to the application.

Appendix B

Tool Threat Category	Tool/Attack Reference Name	Threat/Attack Mitigated
Sniffer/Proxy	Tool #1	✓
	Tool #2	✓
	Tool #2.1	✓
Phishing	Tool #3	✓
Pharming	Tool #4	✓
etc.	Tool #5	✓