Hadoop Security Design
Just Add Kerberos? Really?

Andrew Becherer (andrew@isecpartners.com)

The Apache Foundation's Hadoop Distributed File System (HDFS) and MapReduce engine comprise a distributed computing framework inspired by Google MapReduce and the Google File System (GFS). As originally implemented Hadoop security was completely ineffective. In late 2009 and early 2010 Apache Foundation and Yahoo! developers embarked on an effort to improve the state of Hadoop security. This paper documents and provides an analysis of those efforts.

The following section summarizes the outline of this Whitepaper:

This paper focuses on the design of new Hadoop security features available in Hadoop 0.20.S. The focus is to determine whether the new security mechanisms will scale to meet the requirement of large enterprise users.

What is Hadoop?

The Apache Foundation's Hadoop Distributed File System (HDFS) and MapReduce engine comprise a distributed computing infrastructure inspired by Google MapReduce and the Google File System (GFS). The Hadoop framework allows processing of massive data sets with distributed computing techniques by leveraging large numbers of physical hosts. Hadoop's use is spreading far beyond its open source search engine roots. The Hadoop framework is also being offered by "Platform as a Service" cloud computing providers.

In 2003 and 2004 Google employees released two papers describing a method for large scale distributed data intensive applications. Inspired by these papers Doug Cutting created a distributed computing framework, called Hadoop, to support the open source Nutch search engine. At this time secure deployment and use of Hadoop was not a concern. The data in Hadoop was not sensitive and access to the cluster could be sufficiently limited.

Hadoop is made up of two primary components. These components are the Hadoop Distributed File System (HDFS) and the MapReduce engine. HDFS is made up of geographically distributed Data Nodes. Access to these Data Nodes is coordinated by a service called the Name Node. Data Nodes communicate over the network in order to rebalance data and ensure data is replicated throughout the cluster. The MapReduce engine is made up of two main components. Users submit jobs to a Job Tracker which then distributes the task to Task Trackers as physically close to the required data as possible. While these are the primary components of a Hadoop cluster there are often other services running in a Hadoop cluster such as a workflow manager.

Hadoop is in use at many of the world's largest online media companies including Yahoo, Facebook, Fox Interactive Media, LinkedIn and Twitter. Hadoop is entering the enterprise as evidenced by Hadoop World 2009 presentations from Booz Allen Hamilton and JP Morgan Chase. Hadoop is making its way into the federal government as well. In 2009 the National Security Agency began testing a Hadoop based system for intelligence gathering to link disparate intelligence data sources.

The size of Hadoop deployments can grow quite large. According to media reports Yahoo currently maintains 38,000 machines distributed across 20 different clusters. Hadoop has even been elevated to the "cloud" and made available as a "Platform as a Service" offering by Amazon and Sun.

Hadoop Risks

When Hadoop development began in 2004 no effort was expended on creating a secure distributed computing environment. The Hadoop framework performed insufficient authentication and authorization of both users and services. The insufficient authentication and authorization of users allowed any user to impersonate any other user. The framework did not perform mutual authentication and this would allow a malicious network user to impersonate cluster services. The Hadoop File System's (HDFS) lax authorization allowed anyone to write data and any data to be read. Deploying a secure Hadoop cluster was essentially impossible.

As a result of the insufficient authentication and authorization performed by both HDFS and the MapReduce engine any user could impersonate any other user. Arbitrary java code could be submitted to Job Trackers to be executed as the Job Tracker user account. HDFS file permissions were easily circumvented. The framework did not perform mutual authentication and this allowed malicious network users to impersonate cluster services. If a malicious user could discover a data block's ID the data could be read. Write access was essentially not limited.

The only way to securely deploy Hadoop was to enforce strict network segregation. In this scenario any user given access to the cluster was trusted absolutely.

A New Approach to Security

In 2009 discussion about Hadoop security reached a boiling point. Security was made a high priority. The Hadoop developers' 2010 goals included strong mutual authentication of users and services that would be transparent to end users. In addition to the changes of Hadoop core a new workflow manager, Oozie, was introduced.

The developers chose to use the Simple Authentication and Security Layer (SASL) with Kerberos, via GSSAPI, to authenticate users to the edge services. When a user connects to a Job Tracker that connection is mutually authenticated using Kerberos. Operating system principles are matched to a set of user and group access control lists maintained in flat configuration files.

In order to improve performance and ensure the KDC is not a bottleneck the developers chose to use a number of tokens for communication secured with an RPC Digest scheme. The new Hadoop security design makes use of Delegation Tokens, Job Tokens and Block Access Tokens. Each of these tokens is similar in structure and based on HMAC-SHA1. Del-

egation Tokens are used for clients to communicate with the Name Node in order to gain access to HDFS data. Block Access Tokens are used to secure communication between the Name Node and Data Nodes and to enforce HDFS filesystem permissions. The Job Token is used to secure communication between the MapReduce engine Task Tracker and individual tasks. It is important to note that this scheme uses symmetric encryption and depending upon the token type the shared key may be distributed to hundreds or even thousands of hosts.

At the same time the new Kerberos and RPC Digest security mechanisms were unveiled the Hadoop developers at Yahoo open sourced a new workflow manager called Oozie. Oozie allows users to streamline the submission and management of MapReduce jobs. In order for Oozie to perform its function it has been designated a superuser and can perform actions on behalf of any Hadoop user. Authentication to Oozie has not been implemented. There is a pluggable authentication interface for Oozie but there are no public authentication mechanisms ready to plug in. Anyone planning to make use of Oozie will need to develop their own authentication mechanism. According to the Hadoop Security Design whitepaper, the Hadoop developers considered writing an authentication plugin based on SPNEGO, to support browser based Kerberos authentication, but the limitations of Jetty 6 and uneven browser support dissuaded them from this effort. In subsequent presentations by Hadoop developers the need for a default authentication plugin, with a preference for SPNEGO, has been discussed.

In order to meet their development schedule and maintain backwards compatibility with previous versions of Hadoop the developers made several compromises. The new design requires that end users cannot have administrative rights on any machines in the cluster. If end users had administrative access to cluster machines they could discover Delegation Tokens, Job Tokens, Block Access Tokens or symmetric encryption keys and subvert the security guarantees of the system. In developing the new security features it was decided that these features must not impact GridMix performance more than 3%. This decision guided the developers toward the use of symmetric encryption algorithms and did not encourage the use of secure network transports.

Concerns

The limitations of the threat model used in the development of the new security design produce a number of concerns. Chief among these concerns are the poor default SASL Quality of Protection (QoP), the wide distribution of symmetric cryptographic keys, incomplete pluggable web UI authentication and the use of IP Based Authentication.

Because of the emphasis on performance and the perception that encryption is expensive Hadoop uses a poor default SASL Quality of Protection (QoP). The SASL framework used to add Kerberos support to Hadoop RPC communication can do much better. Other options for QoP protect the integrity and privacy of network communication. The default QoP for Hadoop is authentication, which does not provide integrity or privacy of network communication. This leaves Hadoop RPC communication vulnerable to eavesdropping and modification.

The new Hadoop security design relies on the use of HMAC-SHA1, a symmetric key cryptographic algorithm. In the case of the Block Access Token the symmetric key used in the HMAC-SHA1 will need to be distributed to the Name Node and every Data Node in the cluster. This is potentially hundreds or thousands of geographically distributed machines. If the shared key is disclosed to an attacker the data on all Data Nodes is vulnerable. Given Data IDs the attacker could craft Block Access Tokens, reducing security of Hadoop to the previous level.

Many Hadoop services include HTTP interfaces. These services include the Job Tracker, Task Tracker, Name Node, Data Node and the new Oozie workflow manager. In order to provide authentication for these web interfaces the Hadoop developer have implemented pluggable web UI authentication. This requires the end user of Hadoop to provide a web UI authentication mechanism.

In some Hadoop deployments HDFS proxies are used for server to server bulk data transfer. The Hadoop platform uses the proxy IP addresses, and a database of roles, in order to perform authentication and authorization. IP addresses are not a strong method of authentication. This could lead to the bulk disclosure of all data the HDFS proxy is authorized to access.

An Alternative Strategy

There are currently several proposals for the secure use of Hadoop. One such proposal is Hadoop over the Tahoe Least Access Filesystem (Tahoe-LAFS). The Tahoe-LAFS is an open source, decentralized data store that attempts to preserve your privacy and security even in the case where an individual server has been compromised. Aaron Cordova and colleagues developed this method of running Hadoop over Tahoe, a Least-Authority File System.

Hadoop over Tahoe-LAFS assumes the disk cannot be trusted, the network cannot be trusted but the memory on compute nodes can be trusted. As such individual nodes encrypt

files on disk and only communicate over a secure transport. Hadoop over Tahoe-LAFS has significant impact on GridMix performance. Write performance is especially impacted.

Conclusion

The new Hadoop security model requires additional time and effort before it will meet the requirements of many large enterprises. Changing the SASL Quality of Protection (QoP) should improve the security posture of the system but will have an unknown impact on performance. The wide distribution of symmetric cryptographic keys should be reviewed for alternative solutions. The incomplete pluggable web UI authentication and the use of IP Based Authentication are issues that must be resolved.

About the Author

Andrew Becherer is a Senior Security Consultant with iSEC Partners, a strategic digital security organization. His focus is web and mobile application security as well as emerging cloud computing models. Prior to joining iSEC Partners, he was a Senior Consultant with Booz Allen Hamilton. Mr. Becherer spent several years as a Risk and Credit Analyst in the financial services industry. His experience in the software security, consulting, financial, non-profit and defense sectors has provided him experience with a wide range of technologies.

Mr. Becherer has lectured on a number of topics including emerging cloud computing threat models, virtualization, network security tools and embedded Linux development. At the Black Hat Briefings USA 2009, Andrew, along with researchers Alex Stamos and Nathan Wilcox, presented on the topic "Cloud Computing Models and Vulnerabilities: Raining on the Trendy New Parade." Andrew's research on this topic focused on the effect of elasticity and virtualization on the Linux pseudorandom number generator (PRNG). At Black Hat USA 2008, he was a Microsoft Defend the Flag (DTF) instructor and, he is a recurring speaker at the Linuxfest Northwest conference. In addition to his educational outreach work with user groups, he is a member of several nationally recognized organizations. These organizations include the Association of Computing Machinery (ACM), FBI InfraGard and Open Web Application Security Project (OWASP).

References

- Hadoop Security Design
  by Owen O'Malley, Kan Zhang, Sanjay Radia, Ram Marti, and Christopher Harrell
  https://issues.apache.org/jira/secure/attachment/12428537/security-design.pdf

- MapReduce: Simplified Data Processing on Large Clusters
  by Jeffrey Dean and Sanjay Ghemawat
  http://labs.google.com/papers/mapreduce.html

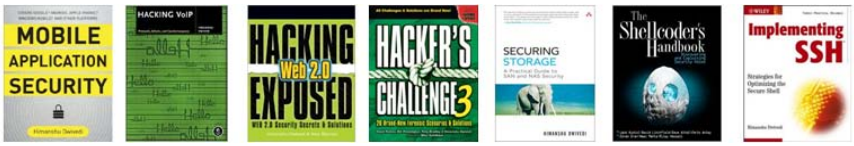
- MapReduce Over Tahoe
  by Aaron Cordova
  http://code.google.com/p/hadoop-lafs/wiki/HadoopTahoeSecureConfig

Appendix A: About iSEC Partners, Inc.

iSEC Partners is a proven full-service security firm, dedicated to making Software Secure. Our focus areas include:

- Mobile Application Security
- Web Application Security
- Client/Server Security
- OnDemand Web Application Scanning (Automated/Manual)

Published Books



Notable Presentations

RSA CONFERENCE
Black Hat
web 2.0 EXPO
InfoWorld
COMPUTERWORLD STORAGE NETWORKING WORLD
SNIA

Whitepaper, Tools, Advisories, & SDL Products

- 12 Published Whitepapers
  - Including the first whitepaper on CSRF
- 37 Free Security Tools
  - Application, Infrastructure, Mobile, VoIP, & Storage
- 9 Advisories
  - Including products from Google, Apple, and Adobe
- Free SDL Products
  - SecurityQA Toolbar (Automated Web Application Testing)
  - Code Coach (Secure Code Enforcement and Scanning)
  - Computer Based Training (Java & WebApp Security)