

Clustering Functional Sections Using Finer Grained ACDC

A Case Study Document

By Pengxiang Zhu and Tianhang Liu

Team Member
Zhaoqi Zhu
Tianhang Liu
Pengxiang Zhu

Secure-related Architectural Decision Picked

The following document illustrates the process of recovering the security decision of introducing “CredentialHandler” for user credential management using the proposed method.

Background

Realm component in Tomcat “represent a “database” of usernames, passwords, and roles (similar to Unix Groups)”[1], and it provides functions for user authentication. For versions before 8.0, Realm component handles user authentication within itself, including credential comparison functions, and this decision has been related with several vulnerabilities ([CVE-2009-0580](#), [CVE-2011-1184](#), and [CVE-2016-0762](#)). After version 8, Tomcat abstracts the credential comparison functions into a separate CredentialHandler component, which makes the user authentication a multi-component process. The CredentialHandler component is critical for the user authentication functions provided by Realm component that “a **CredentialHandler** element MUST be nested inside a [Realm](#) component”[1]; however, results from ACDC did not help us to identify this design decision.

Results from original ACDC

Our teams find out following problems from ACDC results:

1. While CredentialHandler and RealmBase (an implementation of Realm) are closely related for user authentication, they are distributed into different clusters, which prohibits us from recovering this design decision.

CredentialHandler is clustered to “org.apache.catalina.storeconfig.ss”.

org.apache.catalina.storeconfig.ss	org.apache.catalina.realm.NestedCredentialHandler org.apache.catalina.storeconfig.CredentialHandlerSF org.apache.catalina.CredentialHandler org.apache.catalina.ha.session.JvmRouteBinderValve org.apache.catalina.ha.tcp.SimpleTcpCluster org.apache.catalina.storeconfig.CatalinaClusterSF org.apache.catalina.ha.tcp.SendMessageData org.apache.catalina.ha.session.ClusterSessionListener org.apache.catalina.Valve org.apache.catalina.ha.CatalinaCluster org.apache.catalina.ha.ClusterMessage org.apache.catalina.ha.ClusterListener org.apache.catalina.ha.ClusterDeployer org.apache.catalina.ha.ClusterManager org.apache.catalina.tribes.Channel org.apache.catalina.tribes.ChannelListener org.apache.catalina.ha.ClusterValve org.apache.catalina.ha.tcp.ReplicationValve org.apache.catalina.ha.session.SessionMessage org.apache.catalina.ha.session.SessionMessageImpl org.apache.catalina.ha.session.DeltaManager org.apache.catalina.session.PersistentManager org.apache.catalina.ha.tcp.Constants org.apache.catalina.ha.ClusterSession org.apache.catalina.storeconfig.StoreConfigLifecycleListener org.apache.catalina.storeconfig.IStoreConfig org.apache.catalina.storeconfig.StandardContextSF org.apache.catalina.Cluster org.apache.catalina.Manager org.apache.tomcat.util.descriptor.web.ApplicationParameter org.apache.catalina.storeconfig.StoreFactoryBase org.apache.catalina.storeconfig.StoreDescription
------------------------------------	---

RealmBase is clustered to “org.apache.catalina.realm.ss”

org.apache.catalina.realm.ss	org.apache.catalina.realm.MemoryRuleSet
	org.apache.catalina.realm.MemoryUserRule
	org.apache.catalina.realm.MemoryRealm
	org.apache.catalina.realm.GenericPrincipal\$SerializablePrincipal
	org.apache.catalina.realm.GenericPrincipal
	org.apache.catalina.realm.LockOutRealm\$1
	org.apache.catalina.realm.LockOutRealm\$LockRecord
	org.apache.catalina.realm.LockOutRealm
	org.apache.catalina.realm.CombinedRealm
	org.apache.catalina.realm.JAASRealm
	javax.security.auth.login.CredentialExpiredException
	javax.security.auth.login.AccountExpiredException
	org.apache.catalina.realm.JAASCallbackHandler
	javax.security.auth.login.Configuration
	javax.security.auth.login.LoginException
	javax.security.auth.login.FailedLoginException
	javax.security.auth.spi.LoginModule
	org.apache.catalina.realm.JAASMemoryLoginModule
	javax.security.auth.callback.UnsupportedCallbackException
	javax.security.auth.callback.NameCallback
	javax.security.auth.callback.PasswordCallback
	javax.security.auth.callback.TextInputCallback
	org.apache.catalina.realm.RealmBase
	org.apache.catalina.realm.SecretKeyCredentialHandler
	org.apache.catalina.realm.X509SubjectDnRetriever
	org.apache.catalina.realm.X509UsernameRetriever
	java.security.cert.X509Certificate
	org.ietf.jgss.GSSName
	org.apache.catalina.util.SessionConfig
	org.apache.catalina.realm.Constants
	org.apache.catalina.realm.RealmBase\$AllRolesMode
	org.apache.catalina.realm.DigestCredentialHandlerBase

2. ACDC is based on a structural approach and the basic units are files/classes[2], this makes it hard to understand the sub-class-level implementation of the system. For example, an ACDC component can have multiple concerns or “functional sections,” but ACDC does not identify or separate them in any ways. Different function an element provides may be buried by the general function of its cluster.

The highlighted elements form different functional sections.

org.apache.catalina.storeconfig.ss	org.apache.catalina.realm.NestedCredentialHandler
	org.apache.catalina.storeconfig.CredentialHandlerSF
	org.apache.catalina.CredentialHandler
	org.apache.catalina.ha.session.JvmRouteBinderValve
	org.apache.catalina.ha.tcp.SimpleTcpCluster
	org.apache.catalina.storeconfig.CatalinaClusterSF
	org.apache.catalina.ha.tcp.SendMessageData
	org.apache.catalina.ha.session.ClusterSessionListener
	org.apache.catalina.Valve
	org.apache.catalina.ha.CatalinaCluster
	org.apache.catalina.ha.ClusterMessage
	org.apache.catalina.ha.ClusterListener
	org.apache.catalina.ha.ClusterDeployer
	org.apache.catalina.ha.ClusterManager
	org.apache.catalina.tribes.Channel
	org.apache.catalina.tribes.ChannelListener
	org.apache.catalina.ha.ClusterValve
	org.apache.catalina.ha.tcp.ReplicationValve
	org.apache.catalina.ha.session.SessionMessage
	org.apache.catalina.ha.session.SessionMessageImpl
	org.apache.catalina.ha.session.DeltaManager
	org.apache.catalina.session.PersistentManager
	org.apache.catalina.ha.tcp.Constants
	org.apache.catalina.ha.ClusterSession
	org.apache.catalina.storeconfig.StoreConfigLifecycleListener
	org.apache.catalina.storeconfig.IStoreConfig
	org.apache.catalina.storeconfig.StandardContextSF
	org.apache.catalina.Cluster
	org.apache.catalina.Manager
	org.apache.tomcat.util.descriptor.web.ApplicationParameter
	org.apache.catalina.storeconfig.StoreFactoryBase
	org.apache.catalina.storeconfig.StoreDescription

From the information we gained from the analysis, we try to extend the ACDC recovery technique to recover design decisions that span multiple components, and please refer to rationale document for the full reasoning and description of the extension.

The process of discovering this design decision with our method

By analysing the existing implementation artifacts, we design 5 traits combined together to discover this specific security-related architectural decision - User Credential management.

- (1) Check if the function contains “authenticate”.
- (2) Check if the function contains “compare”, “match”.
- (3) Check if the function contains “password”, “credential”, “username”.
- (4) Check if the function contains “digest”, “md”.
- (5) Check if the function has return type of “java.security.principal”.

If a function matches a trait, that function will be added with 1 point and each function can obtain a maximum of 6 points in total.

The result of our method

After we go through the pipeline that is mentioned in the rational document, we acquire (1) a ranking of the original ACDC clusters and (2) a ranking of the functional sections with their corresponding original ACDC clusters. These two rankings will be shown below.

(1) Ranking of the original ACDC clusters with their score

```
1  org.apache.catalina.realm.ss : 296.9212635023106
2  org.apache.catalina.startup.ss : 229.77021250503086
3  org.apache.catalina.connector.ss : 200.881324868993
4  org.apache.tomcat.util.descriptor.web.ss : 198.8759623959799
5  org.apache.catalina.core.ss : 198.71922910999567
6  org.apache.jasper.compiler.ss : 184.81350627815937
7  org.apache.tomcat.util.digester.ss : 118.3009091583364
8  org.apache.catalina.authenticator.ss : 112.0029681061306
9  org.apache.el.parser.ss : 93.12516324536922
10 org.apache.tomcat.util.net.openssl.ss : 72.02346301291091
11 org.apache.tomcat.util.net.ss : 60.109394821582846
12 org.apache.coyote.http11.ss : 59.54008467929673
13 org.apache.tomcat.dbcp.dbcp2.ss : 57.87039550263494
14 org.apache.tomcat.dbcp.dbcp2.datasources.ss : 52.52680322801048
15 org.apache.catalina.storeconfig.ss : 52.471632809279235
16 org.apache.catalina.ha.authenticator.ss : 50.093726655664966
17 org.apache.catalina.loader.ss : 41.828268821923345
18 org.apache.catalina.session.ss : 39.894866985770406
19 org.apache.catalina.webresources.ss : 39.007631564178006
20 org.apache.catalina.mbeans.ss : 38.979997727650556
21 org.apache.catalina.users.ss : 36.58467304313122
22 org.apache.catalina.ha.session.ss : 35.39419037547426
23 org.apache.catalina.ssi.ss : 28.526962512042896
24 org.apache.catalina.servlets.ss : 28.076997105852698
25 org.apache.tomcat.websocket.server.ss : 25.745813919385064
26 org.apache.catalina.manager.ss : 24.19412397784265
27 org.apache.catalina.valves.ss : 22.90190718349043
28 org.apache.catalina.ant.jmx.ss : 21.923794853032685
29 org.apache.catalina.mapper.ss : 19.406011840758244
```


The score of each cluster can be interpreted as the amount of code related to the user credential management. The increment rate of the score is linear, which means that if a cluster A's score is twice as cluster B's score, cluster A has twice as much user credential-related code as cluster B. In our result above, cluster "org.apache.catalina.realm.ss" has the highest score, which means that it is the most relevant cluster with respect to user credential management and contains the most amount of code implementation related to the security decision we picked.

(2) Ranking of the functional sections with their corresponding original ACDC clusters in Tomcat Version 8.5

```
org.apache.catalina.realm.LockOutRealm.ss3 : 5.728715546977509 : [org.apache.catalina.realm.ss, org.apache.catalina.authenticator.ss, org.apache.catalina.startup.ss]
org.apache.catalina.realm.JAASMemoryLoginModule.ss2 : 5.30722777603022 : [org.apache.catalina.realm.ss]
org.apache.catalina.authenticator.AuthenticatorBase.ss2 : 4.913538149119954 : [org.apache.catalina.realm.ss, org.apache.catalina.manager.ss, org.apache.catalina.authenticator.ss]
org.apache.catalina.authenticator.SingleSignOn.ss6 : 4.041451884327381 : [org.apache.catalina.realm.ss, org.apache.catalina.authenticator.ss]
org.apache.catalina.authenticator.AuthenticatorBase.ss4 : 4.0 : [org.apache.catalina.authenticator.ss]
org.apache.catalina.realm.RealmBase.ss14 : 3.5355339059327373 : [org.apache.catalina.realm.ss]
org.apache.catalina.realm.JNDIRealm.ss9 : 3.5355339059327373 : [org.apache.catalina.realm.ss]
org.apache.catalina.realm.RealmBase.ss11 : 3.3333333333333335 : [org.apache.catalina.realm.ss, org.apache.catalina.storeconfig.ss, org.apache.catalina.authenticator.ss]
org.apache.catalina.realm.MessageDigestCredentialHandler.ss1 : 3.0 : [org.apache.catalina.realm.ss, org.apache.tomcat.websocket.server.ss]
org.apache.catalina.realm.JNDIRealm.ss5 : 3.0 : [org.apache.catalina.realm.ss]
org.apache.catalina.authenticator.AuthenticatorBase.ss1 : 2.886751345948129 : [org.apache.catalina.authenticator.ss]
org.apache.catalina.authenticator.NonLoginAuthenticator.ss1 : 2.886751345948129 : [org.apache.catalina.manager.ss, org.apache.catalina.startup.ss]
org.apache.catalina.realm.JDBCRealm.ss3 : 2.82842712474619 : [org.apache.catalina.realm.ss]
org.apache.catalina.realm.DataSourceRealm.ss4 : 2.82842712474619 : [org.apache.catalina.realm.ss]
```

The result above shows functional sections that is closely associated with the user credential management, ranked by their scores. It also shows the original ACDC clusters that each function section is mapped back to. For example, "org.apache.catalina.realm.RealmBase.ss11" can be mapped back to original ACDC clusters "org.apache.catalina.realm.ss", "org.apache.catalina.storeconfig.ss", "org.apache.catalina.Authenticator.ss" because "org.apache.catalina.realm.RealmBase.ss11" contains functions that comes from these three clusters. In addition, by looking into "org.apache.catalina.realm.RealmBase.ss11", we can see the introduction of Credential Handler component in Tomcat Version 8.5, which does not exist in Tomcat Version 6.0. It will be discussed in detail in the following paragraph.

Function section of "org.apache.catalina.realm.RealmBase.ss11" in Tomcat Version 8.5

contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.RealmBase.getPassword()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.RealmBase.authenticate()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.RealmBase.getDigestCharset()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.RealmBase.getCredentialHandler()
contain	org.apache.catalina.realm.RealmBase.ss11	org.ietf.jgss.GSSContext.getCredDelegState()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.RealmBase.isStripRealmForGss()
contain	org.apache.catalina.realm.RealmBase.ss11	org.ietf.jgss.GSSContext.getDelegCred()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.CredentialHandler.matches()
contain	org.apache.catalina.realm.RealmBase.ss11	org.apache.catalina.realm.NestedCredentialHandler.matches()

Function section of "org.apache.catalina.realm.RealmBase.ss9" in Tomcat Version 6.0

contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.hasMessageDigest()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.digest()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.getDigestEncoding()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.authenticate()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.getPassword()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.getDigest()
contain	org.apache.catalina.realm.RealmBase.ss9	org.apache.catalina.realm.RealmBase.encode()

As you can see here, "org.apache.catalina.realm.RealmBase.ss11" in Tomcat Version 8.5 and "org.apache.catalina.realm.RealmBase.ss9" in Tomcat Version 6.0 are considered as the same

function section with respect to different versions because it is obvious to notice that two function sections contains many of the same functions like `authenticate()`, `getPassword()` and `getDigestCharset()`. However, in version 8.5, it reveals the introduction of `CredentialHandler` component by having functions like `CredentialHandler.matches()` and `NestedCredentialHandler.matches()`. Besides, in version 6.0, some digest-related functions are removed such as `digest()` and `MD5Encoder.encode()`. As we take a look into the actual code implementation, it turns out that in version 8.5, all these message digest functions are extracted into a new component - `Credential Handler`. In this case, by looking at the functional sections of “org.apache.catalina.realm.RealmBase.ss11” and “org.apache.catalina.realm.RealmBase.ss9”, we are able to successfully identify the security decision of introducing ‘`CredentialHandler`’ for user credential management.

Reference:

- [1] Y. Shapira, J. Arcand, and F. Hanik, “Apache Tomcat 8 Architecture,” Apache Tomcat, 7Oct-2019. [Online]
- [2] V. Tzerpos and R. Holt, “ACCD: an algorithm for comprehension-driven clustering,” *Proceedings Seventh Working Conference on Reverse Engineering*.