Handling Sensitive Data in Logs, Memory, and Exceptions

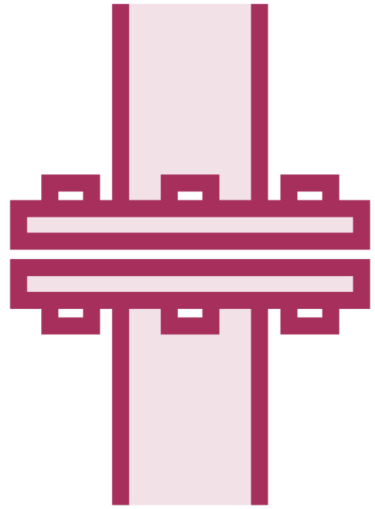
Josh Cummings
PRINCIPAL SOFTWARE ENGINEER

@jzheaux blog.jzheaux.io

Logging Levels

Application Logging

Code has enough context to determine data sensitivity



Infrastructural Logging

Code lacks context to determine data sensitivity

What's Okay to Log?

Don't log it

Don't log sensitive information

Don't log sensitive information in plaintext

Log Correlation

```
021-02-12 12:34:19 INFO   - Registration Passed
021-02-12 12:34:23 INFO   - Registration Passed
021-02-12 12:36:08 ERROR  - Registration Failed
021-02-12 12:36:19 INFO   - Registration Passed
021-02-12 12:39:47 ERROR  - Registration Failed
```

```
2021-02-12 12:59:19 INFO   - Activation Passed
2021-02-12 13:01:43 ERROR  - Activation Failed
2021-02-12 13:13:51 INFO   - Activation Passed
2021-02-12 13:14:19 INFO   - Activation Passed
2021-02-12 13:14:47 ERROR  - Activation Failed
```

Log Correlation

```
021-02-12 12:34:19 INFO   - Registration Passed (bob@jzheaux.io)
021-02-12 12:34:23 INFO   - Registration Passed (mary@jzheaux.io)
021-02-12 12:36:08 ERROR  - Registration Failed (josh@jzheaux.io)
021-02-12 12:36:19 INFO   - Registration Passed (josh@jzheaux.io)
021-02-12 12:39:47 ERROR  - Registration Failed (cal@jzheaux.io)
```

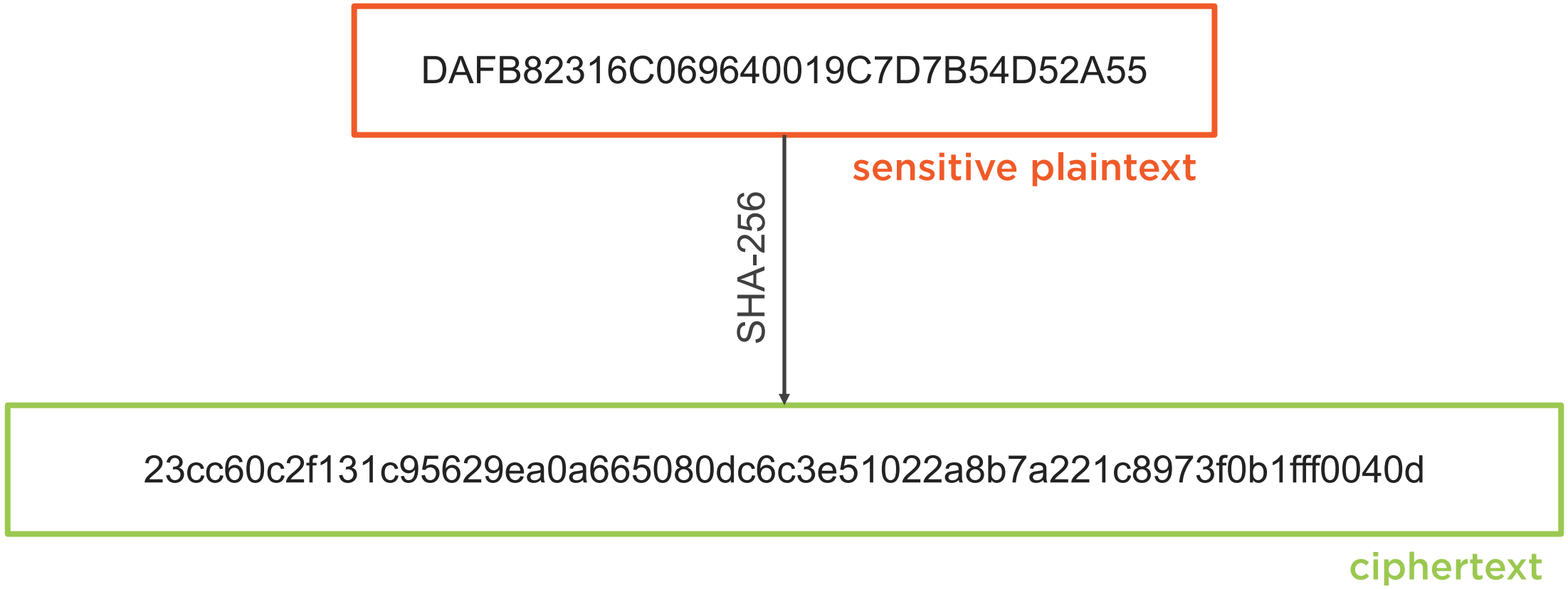
```
2021-02-12 12:59:19 INFO   - Activation Passed (mary@jzheaux.io)
2021-02-12 13:01:43 ERROR  - Activation Failed (josh@jzheaux.io)
2021-02-12 13:13:51 INFO   - Activation Passed (bob@jzheaux.io)
2021-02-12 13:14:19 INFO   - Activation Passed (clint@jzheaux.io)
2021-02-12 13:14:47 ERROR  - Activation Failed (sarah@jzheaux.io)
```

Log Correlation

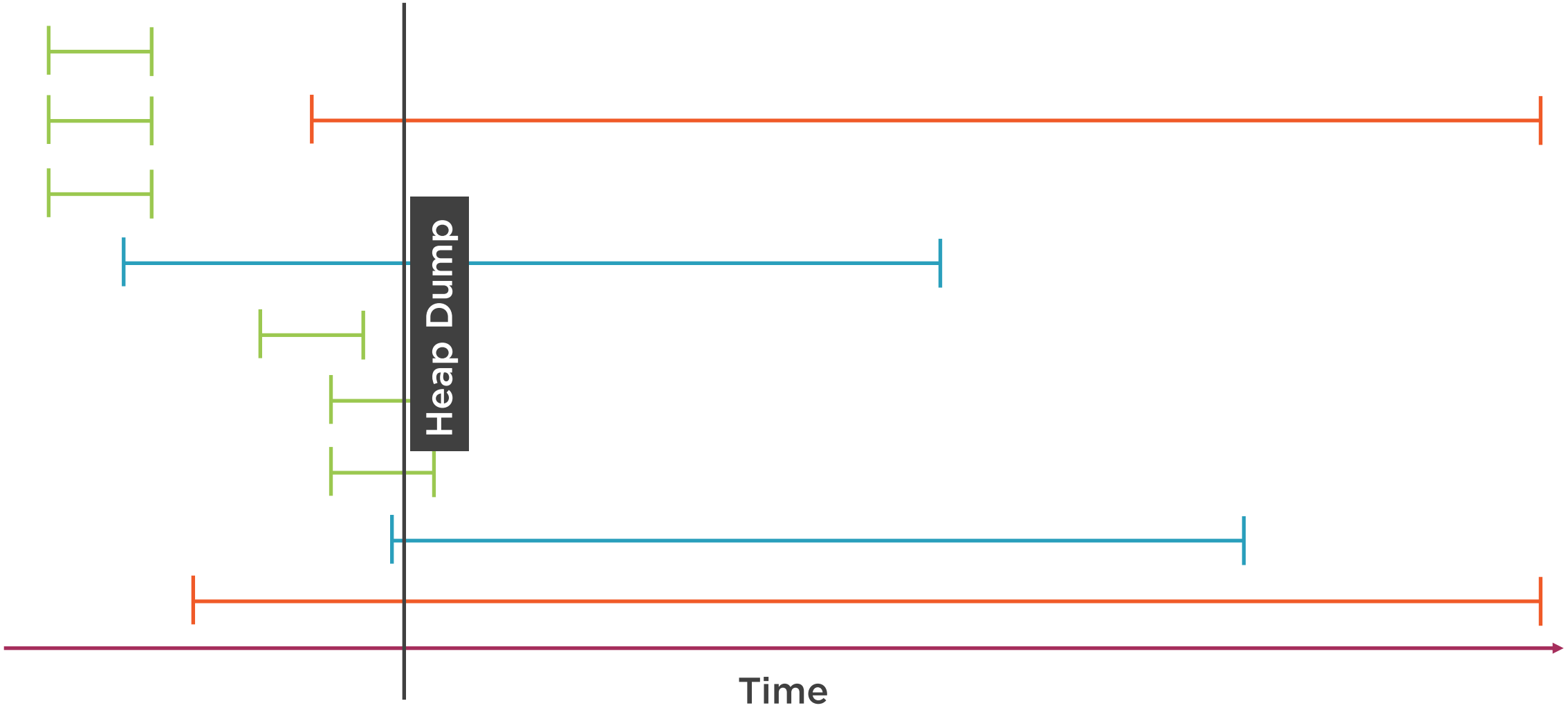
```
021-02-12 12:34:19 INFO   - Registration Passed (b83c-68b36a342cad)
021-02-12 12:34:23 INFO   - Registration Passed (a138-27783993e9fb)
021-02-12 12:36:08 ERROR  - Registration Failed (acdc-44141eca2ddb)
021-02-12 12:36:19 INFO   - Registration Passed (b814-75a1a9fca012)
021-02-12 12:39:47 ERROR  - Registration Failed (c937-70acb4ea2d47)
```

```
2021-02-12 12:59:19 INFO   - Activation Passed (a138-27783993e9fb)
2021-02-12 13:01:43 ERROR  - Activation Failed (b814-75a1a9fca012)
2021-02-12 13:13:51 INFO   - Activation Passed (b83c-68b36a342cad)
2021-02-12 13:14:19 INFO   - Activation Passed (14bc-4b234ebda320)
2021-02-12 13:14:47 ERROR  - Activation Failed (6c9a-1dc7923bac0f)
```

Log Correlation



Sensitive In-memory Data



What's Okay to Cache In-memory?

Don't cache it

Don't cache sensitive information

Don't cache sensitive information in plaintext

What Exceptions Can Be Shown?

Don’t show exceptions

Don’t show untrusted exception messages

```
public class User implements Serializable {

    private final String email;
    private final transient String password;

}
```

Using transient

Blocks a field from being serialized

```
public class User implements Serializable {

    private final String email;
    private final String password;

    private static final ObjectStreamField[]
        serialPersistentFields = {
            new ObjectStreamField("email", String.class)
        };
}
```

Using ObjectStreamField

Allows a field to be serialized

Not as readable as a keyword

Remove Sensitive Data

When logging:

- Don't log unnecessarily, avoid sensitive information
- Use log correlators or hashed info
- Avoid logging entire objects and printf

With memory:

- All data on the heap is visible
- Don't cache unnecessarily, avoid sensitive information

With exceptions:

- Don't show exceptions
- Replace untrusted exception messages

Use transient **or** ObjectStreamField