Towards enabling Secure Web-Based Cloud Services using Client-Side Encryption

Martin Johns, Alexandra Dirksen

Institute for Application Security
Technische Universität Braunschweig

November 9, 2020

Encrypt all the things!...but web apps?

Encrypt all the things!...but web apps?

- End2End encryption gains popularity

Encrypt all the things!...but web apps?

- End2End encryption gains popularity
- Client-side apps uses native encryption

Encrypt all the things!...but web apps?

- End2End encryption gains popularity
- Client-side apps uses native encryption
- Web-apps can’t use encryption
  → **Active JavaScript attacker**

Encrypt all the things!...but web apps?

- End2End encryption gains popularity
- Client-side apps uses native encryption
- Web-apps can't use encryption
  → **Active JavaScript attacker**
- Encryption via 3rd-party extension not feasible

Web apps under fire!

Web apps under fire!

Cloud operator provides a web-based application for its cloud services

Web apps under fire!

Cloud operator provides a web-based application for its cloud services

Database operator stores the user’s data on behalf of the cloud operator

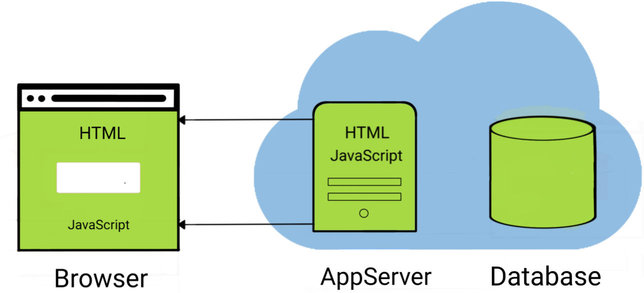
Web apps under fire!

Cloud operator provides a web-based application for its cloud services

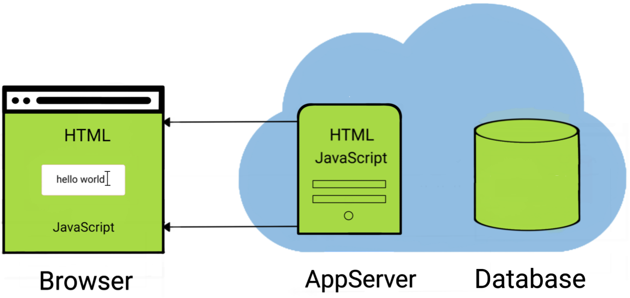
Database operator stores the user's data on behalf of the cloud operator

User utilized her web browser to access the application of the cloud operator

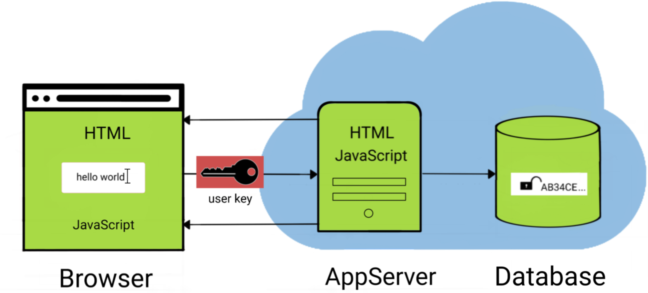
Web apps under fire!



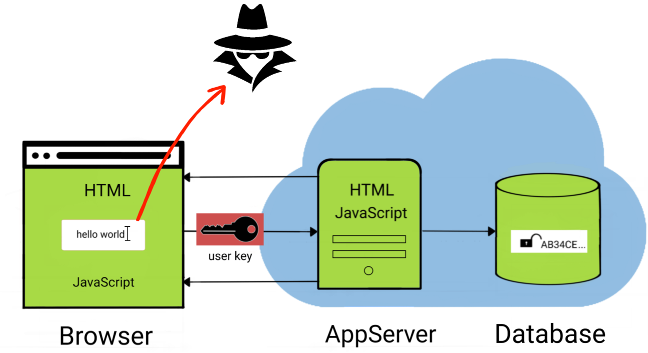
Web apps under fire!



Web apps under fire!



Web apps under fire!



Web apps under fire!

Security Objective

The user want to keep her personal data private while still using the cloud operators web-based application.

Encrypt ALL the things!

Encrypt ALL the things!

- Isolation against untrusted JS

Encrypt ALL the things!

- Isolation against untrusted JS
- Protection against malicious code injection

Encrypt ALL the things!

- Isolation against untrusted JS
- Protection against malicious code injection
- Protection against UI-redressing attacks

Encrypt ALL the things!

- Isolation against untrusted JS
- Protection against malicious code injection
- Protection against UI-redressing attacks
- Incremental deployment possible

Encrypt ALL the things!

- Isolation against untrusted JS
- Protection against malicious code injection
- Protection against UI-redressing attacks
- Incremental deployment possible

Solution

Native encryption tools for web devs via new standarized DOM elements

CryptoMembranes (CM)

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML
2. Each DOM element → CM element
   (e.g. DIV → CryptoDIV)

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML
2. Each DOM element → CM element
   (e.g. DIV → CryptoDIV)
3. Same interface as corresponding DOM element

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML
2. Each DOM element → CM element
   (e.g. DIV → CryptoDIV)
3. Same interface as corresponding DOM element
4. CM maintains cipher and plain value

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML

2. Each DOM element → CM element
   (e.g. DIV → CryptoDIV)

3. Same interface as corresponding DOM element

4. CM maintains cipher and plain value

5. Plain value displayed to browser UI

CryptoMembranes (CM)

1. Usage of CM DOM elements directly in HTML

2. Each DOM element → CM element
   (e.g. DIV → CryptoDIV)

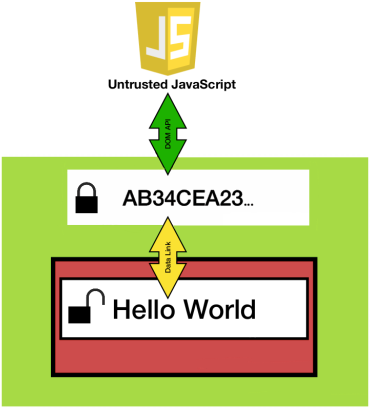
3. Same interface as corresponding DOM element

4. CM maintains cipher and plain value

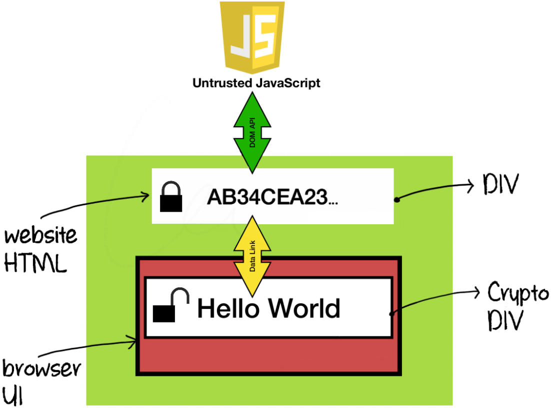
5. Plain value displayed to browser UI

6. Cipher displayed to website JS

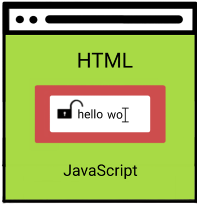
CM Details


Untrusted JavaScript
DOM API
AB34CEA23...
Data Link
Hello World

CM Details

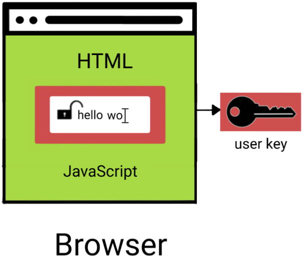

Untrusted JavaScript
DOM API
AB34CEA23...
DIV
website HTML
Data Link
Hello World
Crypto DIV
browser UI

CM Architecture: Encryption

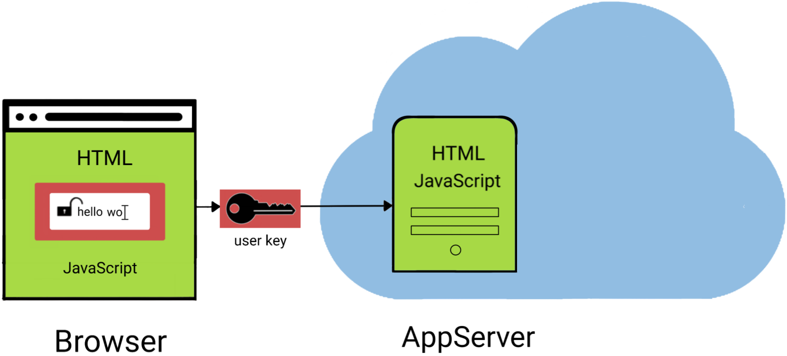


Browser

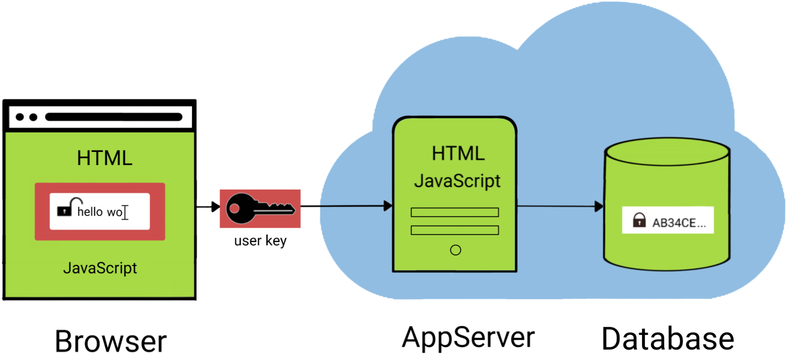
CM Architecture: Encryption



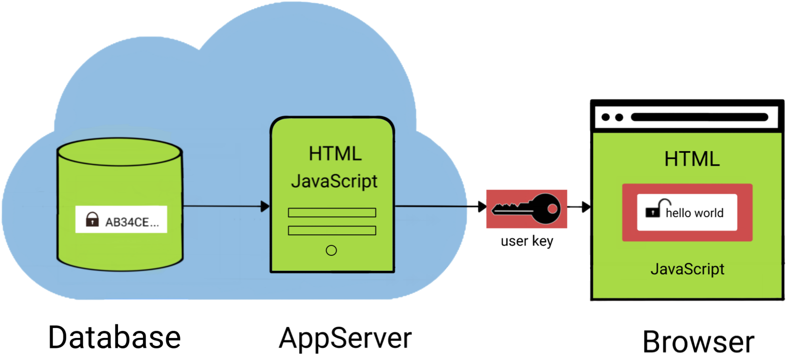
CM Architecture: Encryption



CM Architecture: Encryption



CM Architecture: Decryption



CM Details: Display

HTML Elements for data output:

```
<DIV> AB34CEA23...</DIV>
```

CM Details: Display

HTML Elements for data output:

```
<DIV> AB34CEA23...</DIV>
```

Corresponding CM element:

```
<CryptoDIV CMKeyID="123" CMAlgID="OrderPreserving">
AB34CEA23...
</CryptoDIV>
```

CM Details: Input

HTML Element for data entry:

```
<INPUT Type="text" Name="confinput">
```

CM Details: Input

HTML Element for data entry:

```
<INPUT Type="text" Name="confinput">
```

Corresponding CM element:

```
<CryptoINPUT Type="text" Name="confinput" CMKeyID="345"
↪ CMAlgID="Deterministic">
```

Client-Side Programming

```
<CryptoDIV ID="CM1" CMKeyID="911" CMAlgID "Deterministic">
</CryptoDIV>

<CryptoINPUT ID="CM2" Type="text" name="conf" CMKeyID="911"
↪  CMAlgID="Deterministic" onchange="moveData()">

<script>
function moveData(){
    var cm1 = document.getElementById("CM1");
    var cm2 = document.getElementById("CM2");
    var cValue = cm2.value   // cValue is encrypted
    cm1.innerText = cValue;
}
</script>
```

Legacy Browser Support

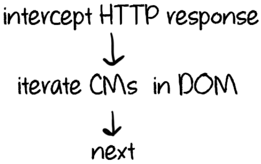
Extension-based support of CryptoMembranes

1. Identifying all CM elements in HTML
2. Insertion of CMs secure compartments

ExtensionMembranes: Workflow

intercept HTTP response

ExtensionMembranes: Workflow



intercept HTTP response

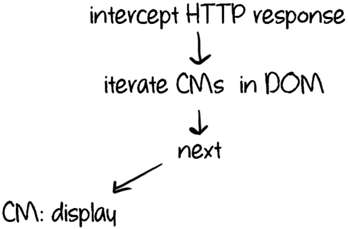
↓

iterate CMs in DOM

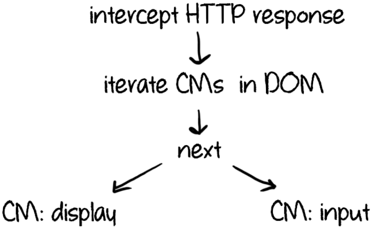
↓

next

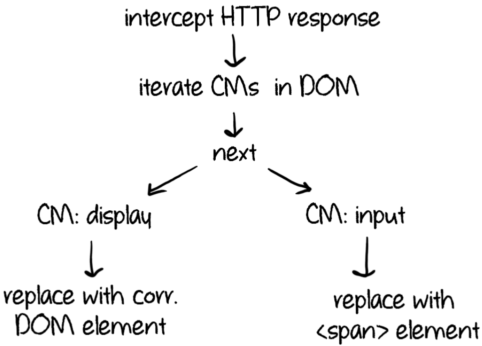
ExtensionMembranes: Workflow



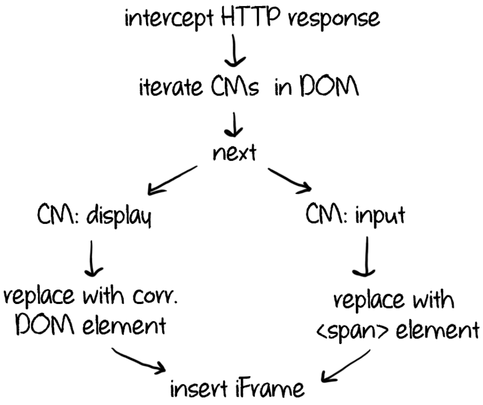
ExtensionMembranes: Workflow



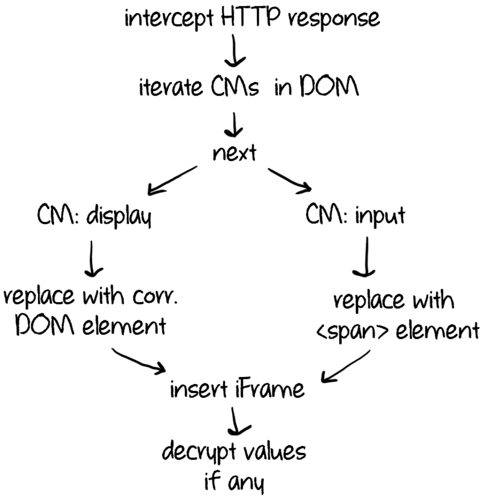
ExtensionMembranes: Workflow



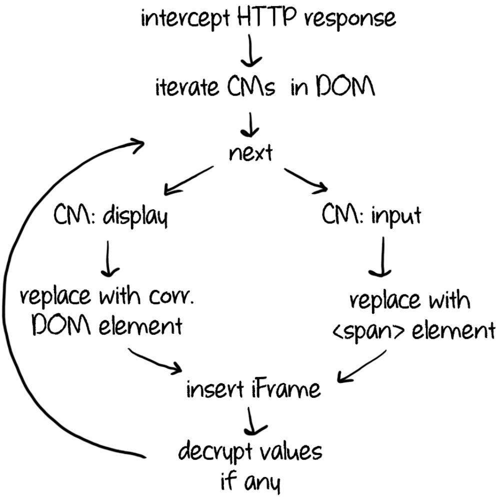
ExtensionMembranes: Workflow



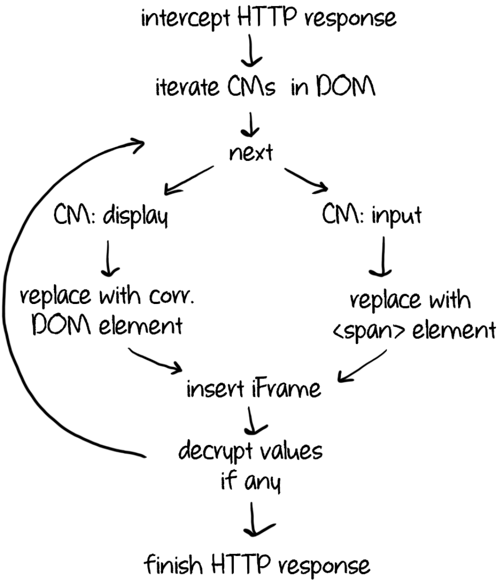
ExtensionMembranes: Workflow



ExtensionMembranes: Workflow



ExtensionMembranes: Workflow



Security Assessment

- □ Isolation properties
- □ Protection against code injection
- □ Protection against UI-redressing attacks
- □ Incremental Deployability

Security Assessment

☑ Isolation properties

☐ Protection against code injection

☐ Protection against UI-redressing attacks

☐ Incremental Deployability

Security Assessment

☑ Isolation properties

☑ Protection against code injection

□ Protection against UI-redressing attacks

□ Incremental Deployability

Security Assessment

- ☑ Isolation properties
- ☑ Protection against code injection
- ☑ Protection against UI-redressing attacks
- □ Incremental Deployability

Security Assessment & Conclusion

☑ Isolation properties

☑ Protection against code injection

☑ Protection against UI-redressing attacks

☑ Incremental deployability

Future Work

Future Work

□ Native browser implementation

Future Work

□ Native browser implementation

□ User study on secure input / visual indicator

Future Work

- □ Native browser implementation
- □ User study on secure input/visual indicator
- □ Identifying crypto needs
  (Order preserving? Searchable? Aggregated?)

🐦 @z4lem

✉ a.dirksen@tu-bs.de

🌐 www.tu-bs.de/ias