

Morellian Analysis for Browsers: Making Web Authentication Stronger With Canvas Fingerprinting







Pierre Laperdrix, Gildas Avoine, Benoit Baudry, Nick Nikiforakis




DIMVA 2019

- Attacks on the web happen more and more frequently and are getting bigger.

NEWS
'Collection #1' reveals 773 million email addresses, passwords in one of largest data breaches ever
You can check to see if your username and password have been leaked.

 By [Mark Hachman](#)
Senior Editor, [PCWorld](#) | JANUARY 17, 2019 01:25 PM PT

January 10, 2019

Credential stuffing attack prompts Reddit to force password reset

[Bradley Barth](#)

DailyMotion discloses credential stuffing attack

DailyMotion falls to credential stuffing attack two weeks after Reddit had the same fate.



By [Catalin Cimpanu](#) for [Zero Day](#) | January 27, 2019 -- 12:02 GMT (12:02 GMT) | Topic: [Security](#)

- Attacks on the web happen more and more frequently and are getting bigger.

NEWS
'Collection #1' reveals 773 million email addresses, passwords in one of largest data breaches ever
You can check to see if your username and password have been leaked.

By [Mark Hachman](#)
Senior Editor, PCWorld | JANUARY 17, 2019 01:25 PM PT

January 10, 2019

Credential stuffing attack prompts Reddit to force password reset

[Bradley Barth](#)

DailyMotion discloses credential stuffing attack

DailyMotion falls to credential stuffing attack two weeks after Reddit had the same fate.



By [Catalin Cimpanu](#) for [Zero Day](#) | January 27, 2019 -- 12:02 GMT (12:02 GMT) | Topic: [Security](#)



[Zeljka Zorz](#), Managing Editor
April 29, 2019

Share this article



Attackers breached Docker Hub, grabbed keys and tokens

- Attacks on the web happen more and more frequently and are getting bigger.

Protecting an account
with just a password is
not enough.

- Low adoption of multi-factor authentication
 - A 2017 survey from Duo Security indicated that more than half of Americans never heard of 2FA before.
 - A talk in January 2018 revealed that less than 10% of Gmail users have 2FA enabled.

- Low adoption of multi-factor authentication
 - A 2017 survey from Duo Security indicated that more than half of Americans never heard of 2FA before.
 - A talk in January 2018 revealed that less than 10% of Gmail users have 2FA enabled.
- Problems: education gap towards the benefits of 2FA/MFA, usability issues that come with having it activated.

- Low adoption of multi-factor authentication
 - A 2017 survey from Duo Security indicated that more than half of Americans never heard of 2FA before.
 - A talk in January 2018 revealed that less than 10% of Gmail users have 2FA enabled.
- Problems: education gap towards the benefits of 2FA/MFA, usability issues that come with having it activated.
- There is a need for a technical solution that bridges the gap between the insufficiency of passwords and the low onboarding of 2FA.

- Low adoption of multi-factor authentication
 - A 2017 survey from Duo Security indicated that more than half of Americans never heard of 2FA before.
 - A talk in January 2018 revealed that less than 10% of Gmail users have 2FA enabled.
- Problems: education gap towards the benefits of 2FA/MFA, usability issues that come with having it activated.
- There is a need for a technical solution that bridges the gap between the insufficiency of passwords and the low onboarding of 2FA.

Can browser fingerprinting be a viable alternative?



Introduction - Internet in 2019

4



4



Introduction - Internet in 2019

4





A bigger and richer web



- Audio
- Video
- 3D rendering
- Real-time communications
- Web payments
- Virtual reality
- ...

Introduction - Internet in 2019

4

Browser



1995	2019
Browser: Netscape Language: Fr	Browser: Chrome v74 OS: Linux Screen: 1920x1080 Language: Fr Timezone: GMT+1 Graphic card: GTX 1080Ti ...

A bigger and richer web



- Audio
- Video
- 3D rendering
- Real-time communications
- Web payments
- Virtual reality
- ...

Browser



1995	2019
Browser: Netscape Language: Fr	Browser: Chrome v74 OS: Linux Screen: 1920x1080 Language: Fr Timezone: GMT+1 Graphic card: GTX 1080Ti ...

A bigger and richer web



- Audio
- Video
- 3D rendering
- Real-time communications
- Web payments
- Virtual reality

...

What happens when we start collecting all the information available in a web browser?

Definitions

- A **browser fingerprint** is a set of information related to a user's device from the hardware to the operating system to the browser and its configuration.
- Browser **fingerprinting** refers to the process of collecting information through a web browser to build a fingerprint of a device.

Introduction - Example of a browser fingerprint

6

Attribute	Value
User agent	Mozilla/5.0 (X11; Fedora; Linux x86_64; rv:66.0) Gecko/20100101 Firefox/66.0
HTTP headers	text/html, application/xhtml+xml, application/xml;q=0.9,*/*;q=0.8 gzip, deflate, br en-US,en;q=0.5
Plugins	Plugin 0: QuickTime Plug-in 7.6.6; libtotem-narrow-space-plugin.so; Plugin 1: Shockwave Flash; Shockwave Flash 26.0 r0; libflashplayer.so.
Fonts	Century Schoolbook, Source Sans Pro Light, DejaVu Sans Mono, Bitstream Vera Serif, URW Palladio L, Bitstream Vera Sans Mono, Bitstream Vera Sans, ...
Platform	Linux x86_64
Screen resolution	1920x1080x24
Timezone	-480 (UTC+8)
OS	Linux 3.14.3-200.fc20.x86 32-bit
WebGL vendor	NVIDIA Corporation
WebGL renderer	GeForce GTX 650 Ti/PCIe/SSE2
Canvas	<div>Cwm fjordbank glyphs vext quiz, ☺</div> <div>Cwm fjordbank glyphs vext quiz, ☺</div>



Maverick
Ocean Front Villas
Mandarin tea
Regency
Sassafras & Ginger
Dollhouse
Athletics Dept.



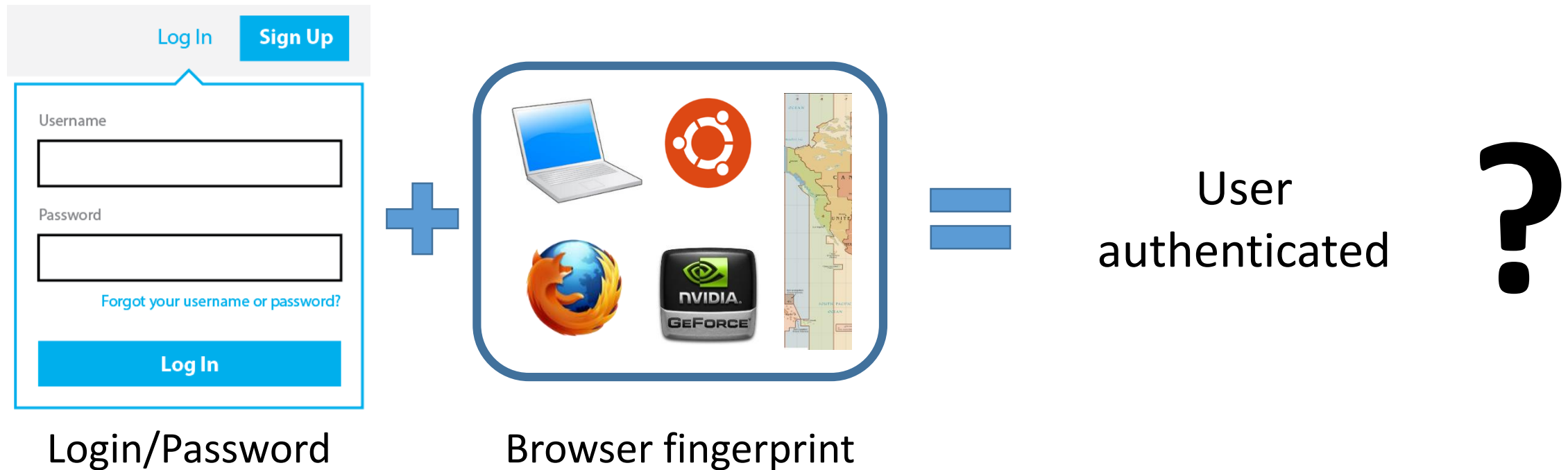
Using fingerprinting for authentication

7



Using fingerprinting for authentication

7



One major problem: what if the user's fingerprint is stolen (i.e. collected)?

- Fingerprints can be manipulated in JavaScript. An attacker can send any information to the authentication server.

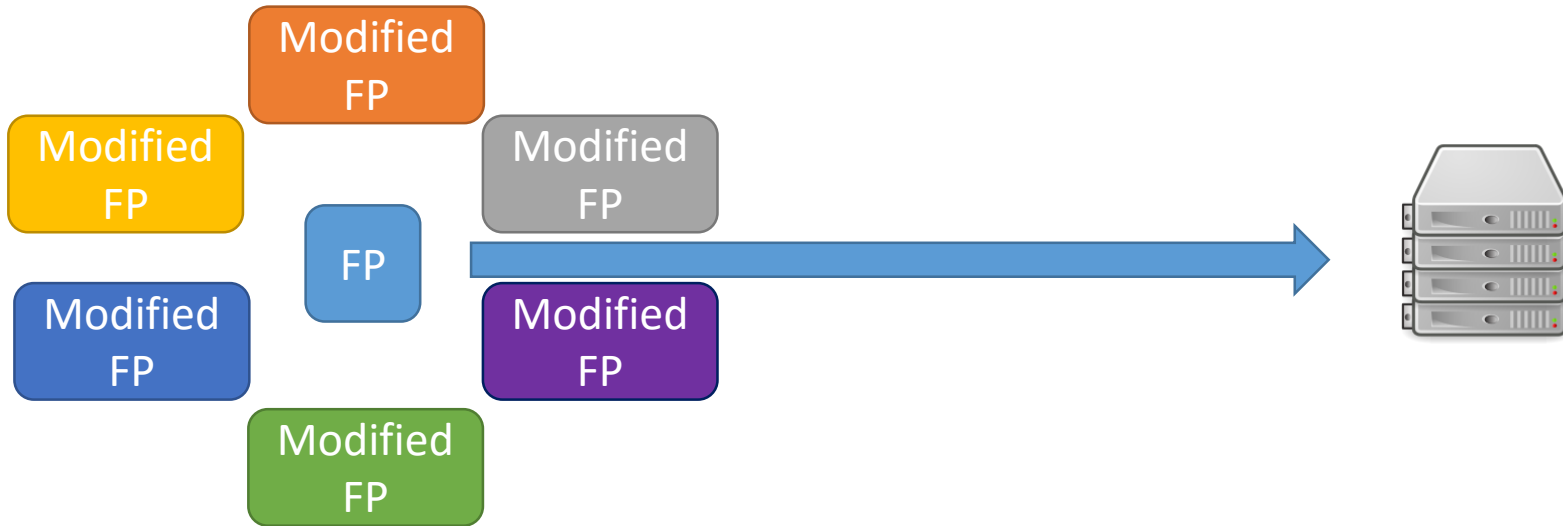
One major problem: what if the user's fingerprint is stolen (i.e. collected)?

- Fingerprints can be manipulated in JavaScript. An attacker can send any information to the authentication server.



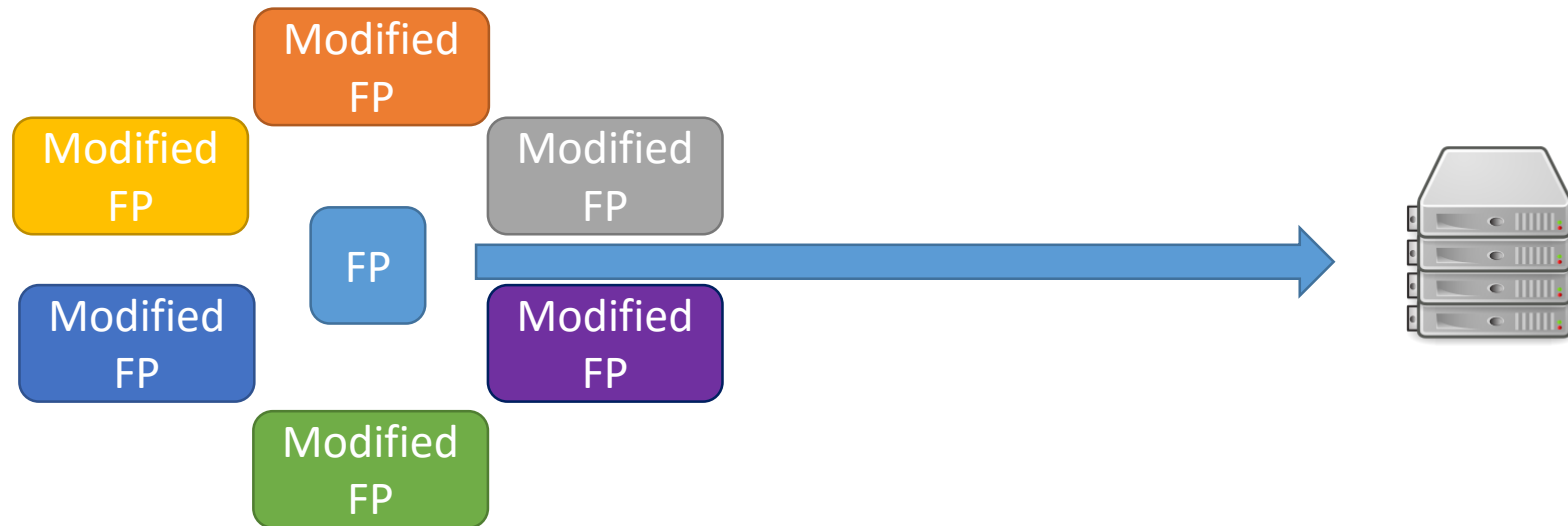
One major problem: what if the user's fingerprint is stolen (i.e. collected)?

- Fingerprints can be manipulated in JavaScript. An attacker can send any information to the authentication server.



One major problem: what if the user's fingerprint is stolen (i.e. collected)?

- Fingerprints can be manipulated in JavaScript. An attacker can send any information to the authentication server.



- An attacker can also try to reconstruct the environment of his victim to bypass verification.

One major problem: what if the user's fingerprint is stolen (i.e. collected)?

➤ Traditional fingerprinting scripts always collect the same attributes.

What is the
user agent?

What is the
language?

What is the
browser?

What is the list
of plugins?

What is the list
of fonts?

What is the
screen
resolution?

What is the
timezone?

What is
platform?

Are cookies
enabled?

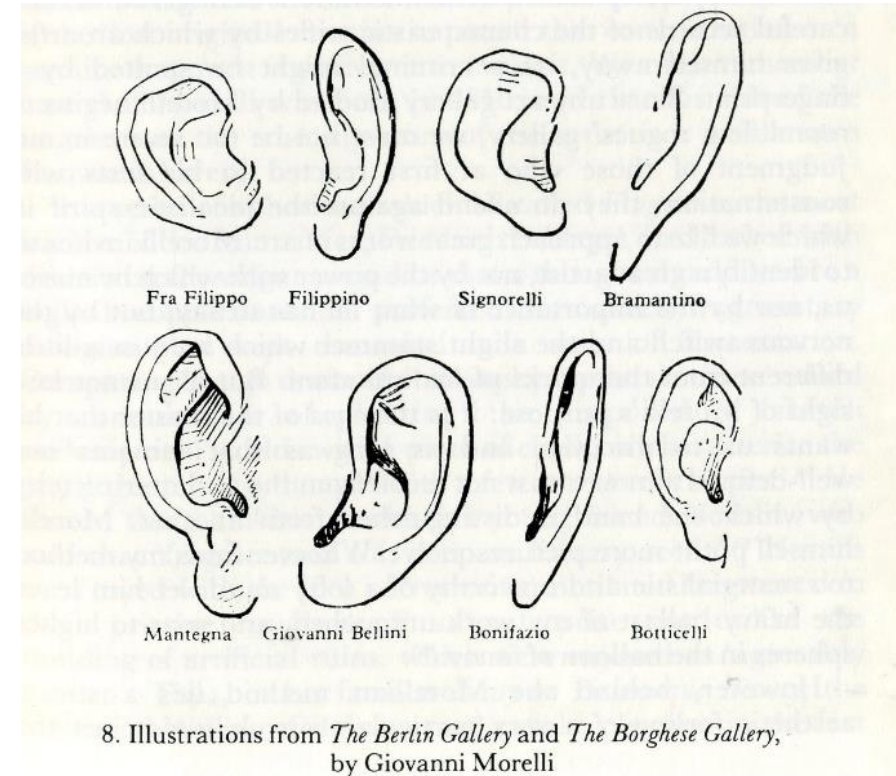
...

≈20 questions



Giovanni Morelli (1816-1891)

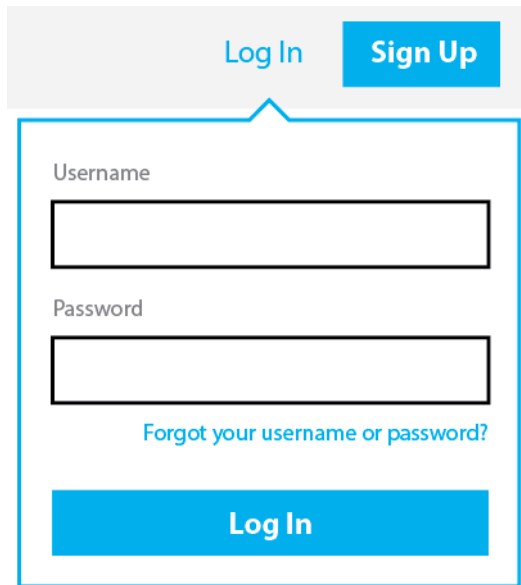
- Studied medicine and taught anatomy
- Identified the characteristic "hands" of painters through scrutiny of minor details in paintings



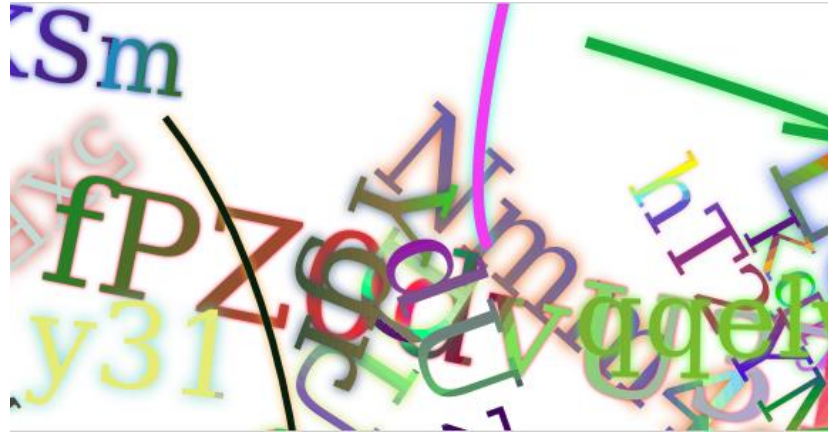
8. Illustrations from *The Berlin Gallery* and *The Borghese Gallery*, by Giovanni Morelli

Using canvas fingerprinting for authentication

11

A login form with a light gray header containing 'Log In' and 'Sign Up' buttons. The main form area has a blue border and contains 'Username' and 'Password' labels, each followed by a text input field. Below the password field is a link 'Forgot your username or password?'. At the bottom is a large blue 'Log In' button.

Login/Password



Canvas fingerprint



User
authenticated

Example from the AmlUnique.org website

```
canvas = document.createElement("canvas");
canvas.height = 60;
canvas.width = 400;
canvasContext = canvas.getContext("2d");
canvas.style.display = "inline";
canvasContext.textBaseline = "alphabetic";
canvasContext.fillStyle = "#f60";
canvasContext.fillRect(125, 1, 62, 20);
canvasContext.fillStyle = "#069";
canvasContext.font = "11pt no-real-font-123";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 2, 15);
canvasContext.fillStyle = "rgba(102, 204, 0, 0.7)";
canvasContext.font = "18pt Arial";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 4, 45);
canvasData = canvas.toDataURL();
```

Example from the AmlUnique.org website



1

```
canvas = document.createElement("canvas");
canvas.height = 60;
canvas.width = 400;
canvasContext = canvas.getContext("2d");
canvas.style.display = "inline";
canvasContext.textBaseline = "alphabetic";
canvasContext.fillStyle = "#f60";
canvasContext.fillRect(125, 1, 62, 20);
canvasContext.fillStyle = "#069";
canvasContext.font = "11pt no-real-font-123";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 2, 15);
canvasContext.fillStyle = "rgba(102, 204, 0, 0.7)";
canvasContext.font = "18pt Arial";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 4, 45);
canvasData = canvas.toDataURL();
```

Example from the AmlUnique.org website

```
canvas = document.createElement("canvas");
canvas.height = 60;
canvas.width = 400;
canvasContext = canvas.getContext("2d");
canvas.style.display = "inline";
canvasContext.textBaseline = "alphabetic";
```

1

```
canvasContext.fillStyle = "#f60";
canvasContext.fillRect(125, 1, 62, 20);
```

2

```
canvasContext.fillStyle = "#069";
canvasContext.font = "11pt no-real-font-123";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 2, 15);
canvasContext.fillStyle = "rgba(102, 204, 0, 0.7)";
canvasContext.font = "18pt Arial";
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 4, 45);
canvasData = canvas.toDataURL();
```



Cwm fjordbank glyphs vext quiz, 😄

Example from the AmlUnique.org website

```
canvas = document.createElement("canvas");  
canvas.height = 60;  
canvas.width = 400;  
canvasContext = canvas.getContext("2d");  
canvas.style.display = "inline";  
canvasContext.textBaseline = "alphabetic";
```

1

```
canvasContext.fillStyle = "#f60";  
canvasContext.fillRect(125, 1, 62, 20);
```

2

```
canvasContext.fillStyle = "#069";  
canvasContext.font = "11pt no-real-font-123";  
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 2, 15);
```

3

```
canvasContext.fillStyle = "rgba(102, 204, 0, 0.7)";  
canvasContext.font = "18pt Arial";  
canvasContext.fillText("Cwm fjordbank glyphs vext quiz, \ud83d\ude03", 4, 45);  
canvasData = canvas.toDataURL();
```



Cwm fjordbank glyphs vext quiz, 😄

Cwm fjordbank glyphs vext quiz, 😄

Example from the AmlUnique.org website

Cwm fjordbank glyphs vext quiz, ☺

Cwm fjordbank glyphs vext quiz, ☺

Using canvas fingerprinting for authentication

13

Use the Canvas API as a drawing board for a morellian analysis.

Use the Canvas API as a drawing board for a morellian analysis.

- Dynamic

Cwm fjordbank glyphs vext quiz, ☺

Cwm fjordbank glyphs vext quiz, ☺

Draw an
orange
rectangle of
size 63x45 at
position (7,89)

Render the string
“stnalpehtretlaw”
with a size 30pt at
position (1337,42)
with the font Arial
in purple

Draw a green
circle with a
circumference
of 24 pixels at
position (4,8)

Using canvas fingerprinting for authentication

13

Use the Canvas API as a drawing board for a morellian analysis.

- Dynamic

Draw a purple circle with a circumference of 122 pixels at position (44,86)
Draw an orange rectangle of size 63x45 at position (7,89)
Render the string "dumbledore" with a size 30pt at position (1337,40) with the font Comic sans MS in white
Render the string "fingerpring" with a size 26pt at position (45,54) with the font Georgia in red
Draw a yellow rectangle of size 33x44 at position (55,66)
Render the string "stnalpehtretlaw" with a size 30pt at position (1337,42) with the font Arial
Draw a red rectangle of size 36x54 at position (8,88)
Draw a blue circle with a circumference of 22 pixels at position (42,8)
Draw a blue rectangle of size 2x2 at position (2,2)
Draw a green circle with a circumference of 24 pixels at position (4,8)
Render the string "noG04,8" with a size 48pt at position (57,69) with the font Helvetica in grey

Use the Canvas API as a drawing board for a morellian analysis.

- Dynamic

Draw a purple circle with a circumference of 122 pixels at position (4,86)
Draw an orange rectangle of size 63x45 at position (7,89)
Render the string "dumbledore" with a size 30pt at position (1337,40) with the font Comic sans MS in white
Render the string "fingerpring" with a size 26pt at position (45,54) with the font Georgia in red
Draw a yellow rectangle of size 33x44 at position (55,66)
Render the string "stnalpehtretlaw" with a size 30pt at position (1337,42) with the font Arial
Draw a red rectangle of size 36x54 at position (8,88)
Draw a blue circle with a circumference of 22 pixels at position (42,8)
Draw a blue rectangle of size 2x2 at position (2,2)
Draw a green circle with a circumference of 24 pixels at position (4,8)
Render the string "noG04,8" with a size 48pt at position (57,69) with the font Helvetica in grey

Incredibly high number of questions



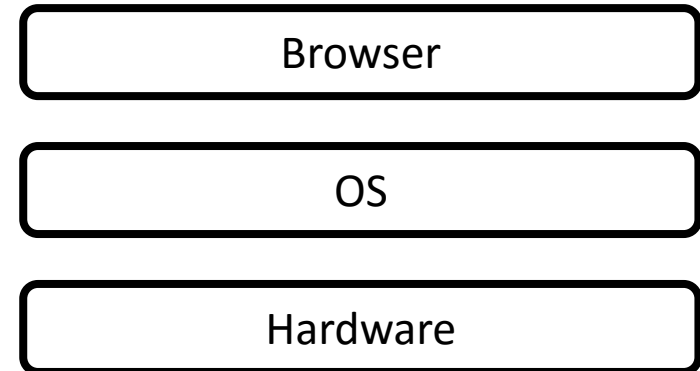
Generation of a new test at each connection

Using canvas fingerprinting for authentication

13

Use the Canvas API as a drawing board for a morellian analysis.

- Dynamic
- Hard to spoof



Incredibly high number
of questions



Generation of a new
test at each connection

Our challenge-response system

14

Bootstrapping phase

Server



Client



Our challenge-response system

14

Bootstrapping phase

Server

Client

1

Generating a
new canvas
challenge c1

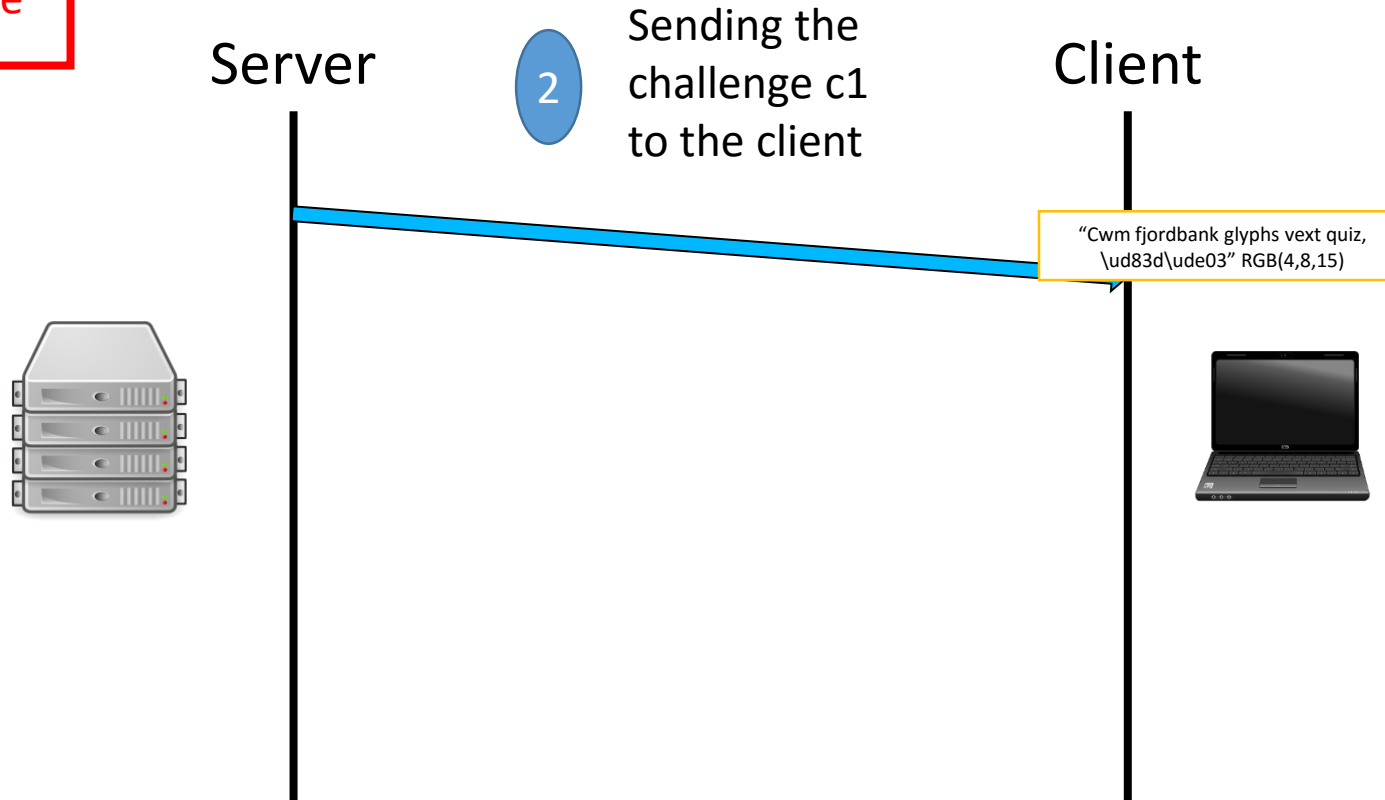
"Cwm fjordbank glyphs vext quiz,
\ud83d\ude03" RGB(4,8,15)



Our challenge-response system

14

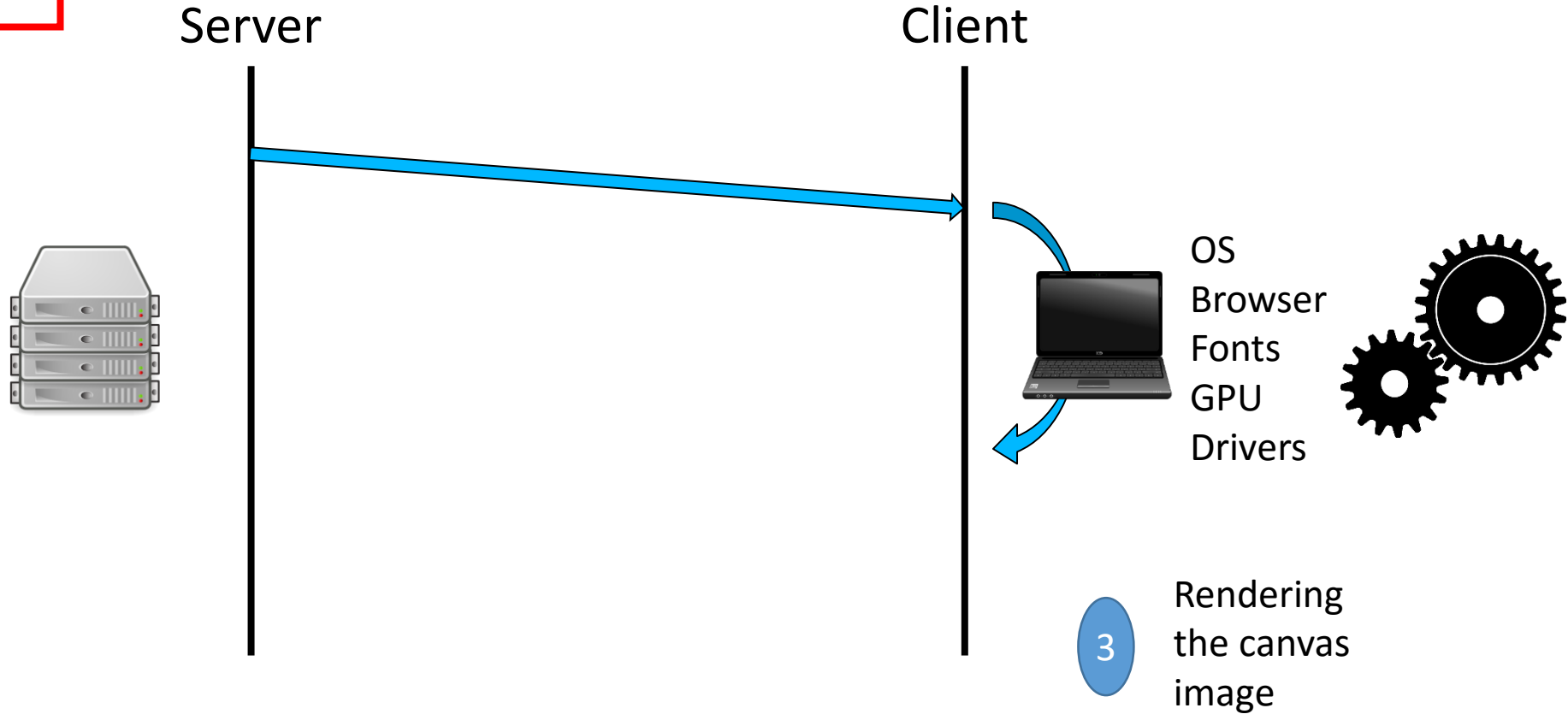
Bootstrapping phase



Our challenge-response system

14

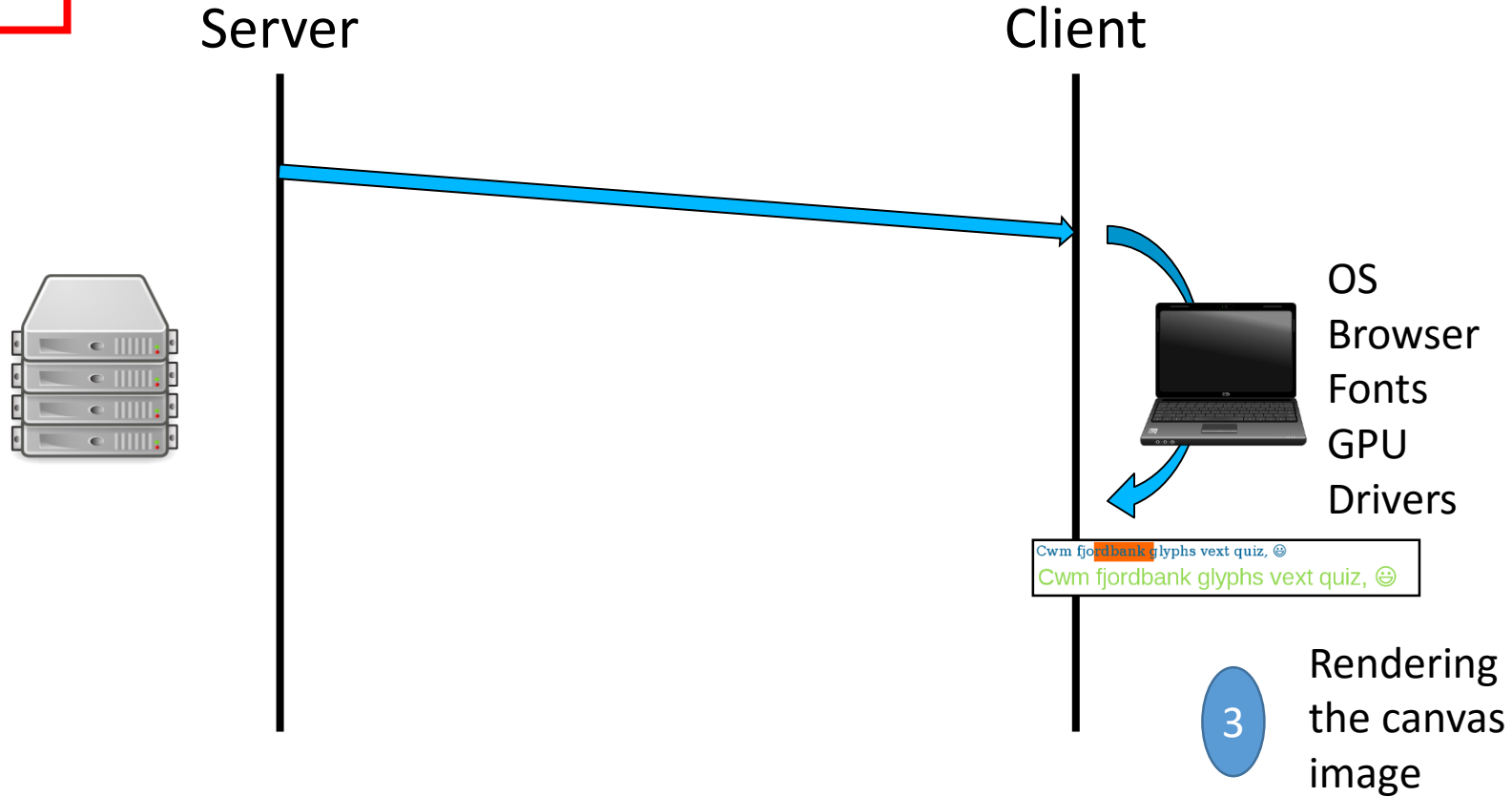
Bootstrapping phase



Our challenge-response system

14

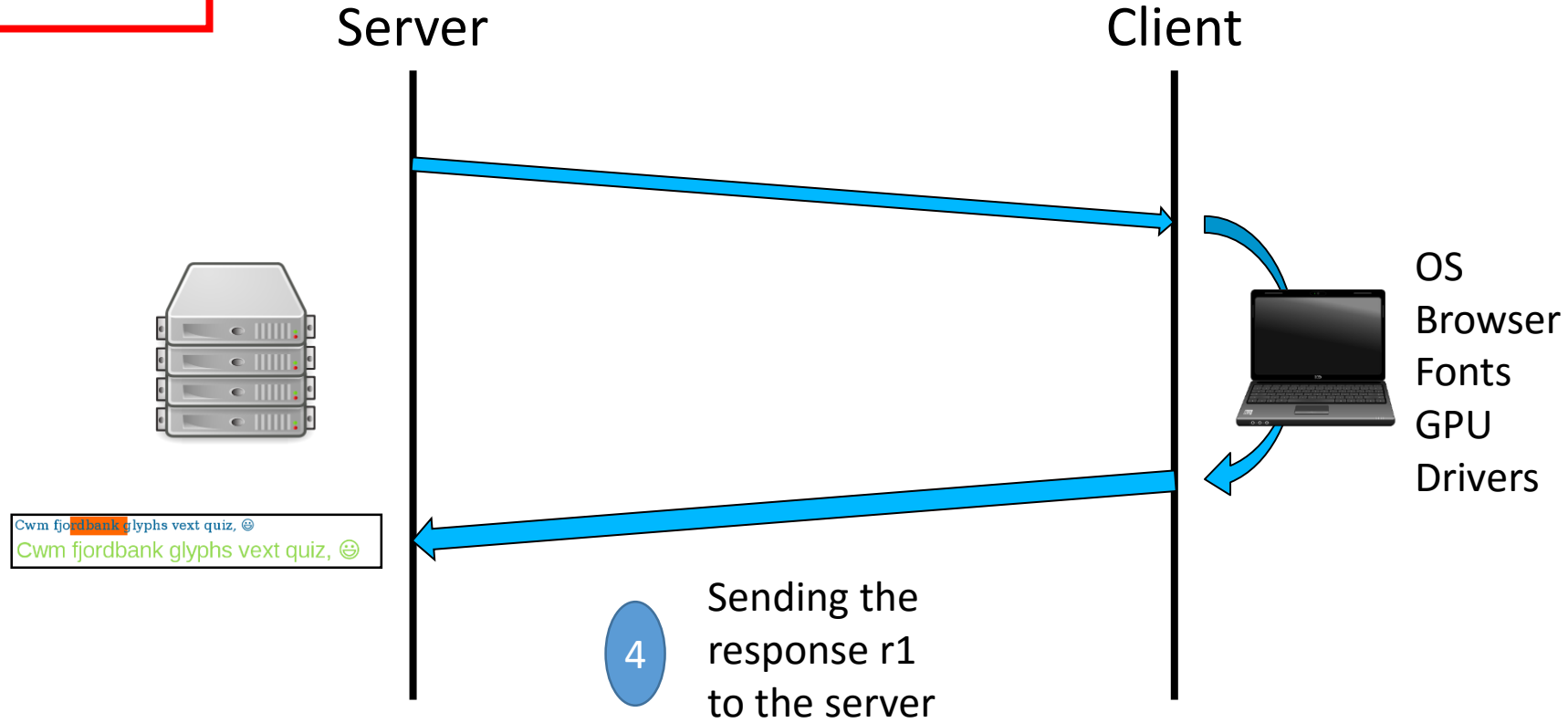
Bootstrapping phase



Our challenge-response system

14

Bootstrapping phase



Our challenge-response system

14

Bootstrapping phase

5

Storing both
the challenge
c1 and the
response r1



"Cwm fjordbank glyphs vext quiz,
\ud83d\ude03" RGB(4,8,15)

Cwm fjordbank glyphs vext quiz, ☹
Cwm fjordbank glyphs vext quiz, 😊

Server

Client

OS
Browser
Fonts
GPU
Drivers



Our challenge-response system

15

Connection phase

Server



Client



Our challenge-response system

15

Connection phase

Server

Client

1

Retrieving
c1 and r1
from the
previous
connection

"Cwm fjordbank glyphs vext quiz,
\ud83d\ude03" RGB(4,8,15)



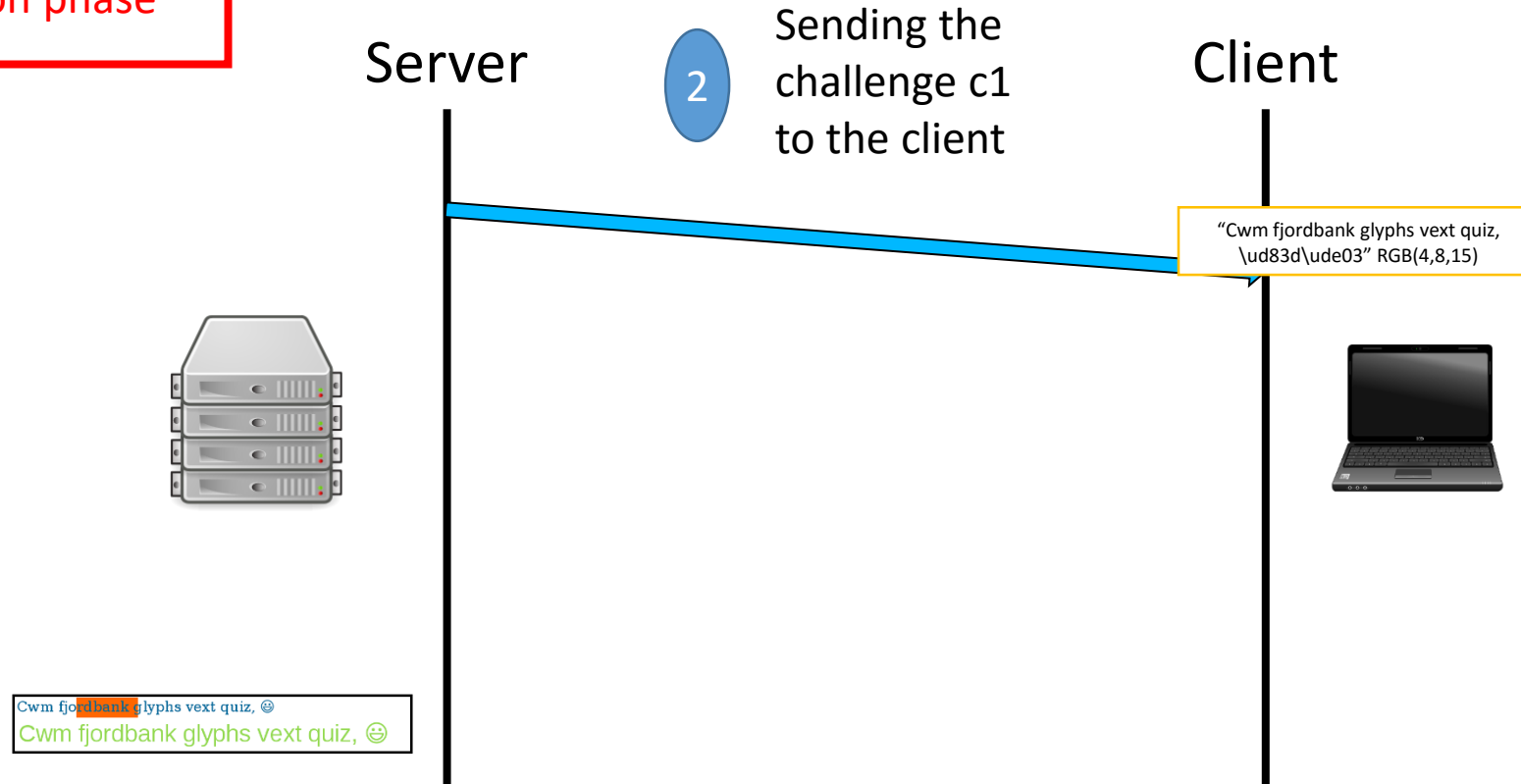
Cwm fjordbank glyphs vext quiz, ☹️
Cwm fjordbank glyphs vext quiz, 😊



Our challenge-response system

15

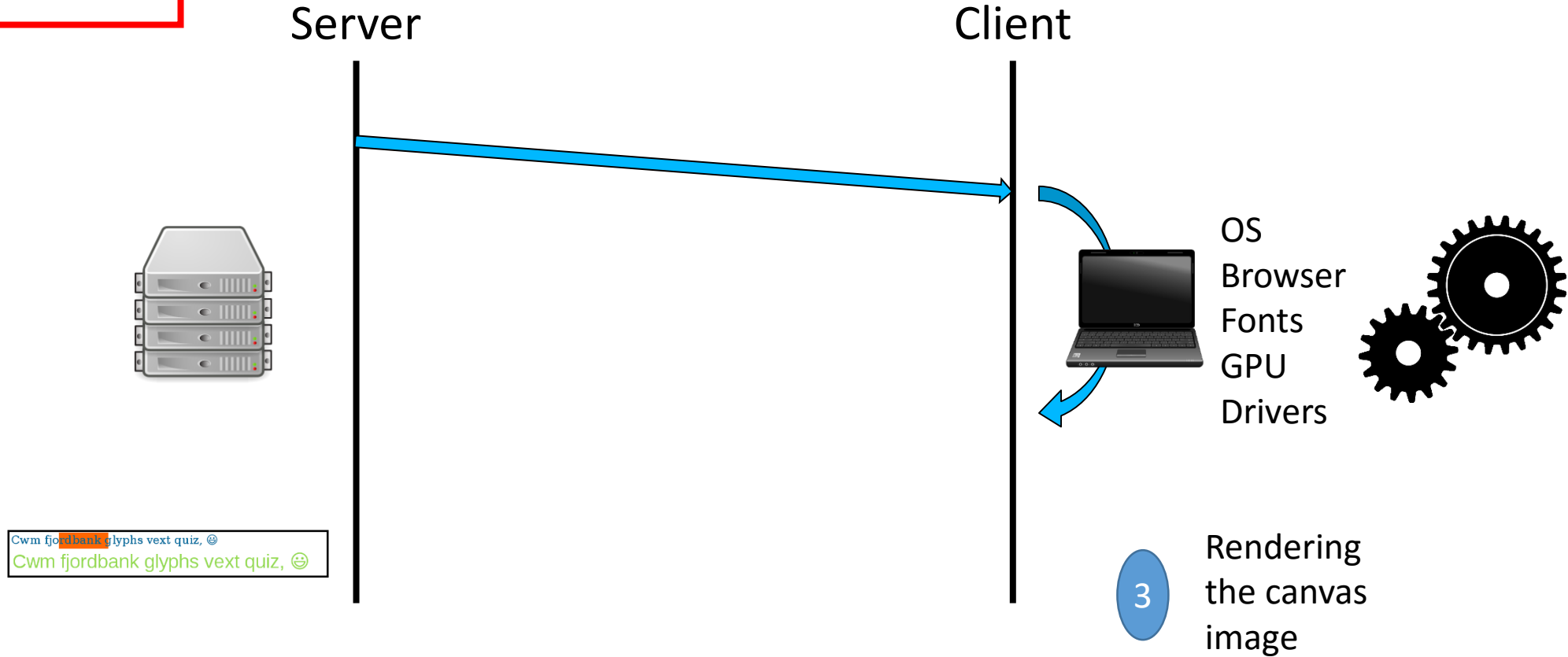
Connection phase



Our challenge-response system

15

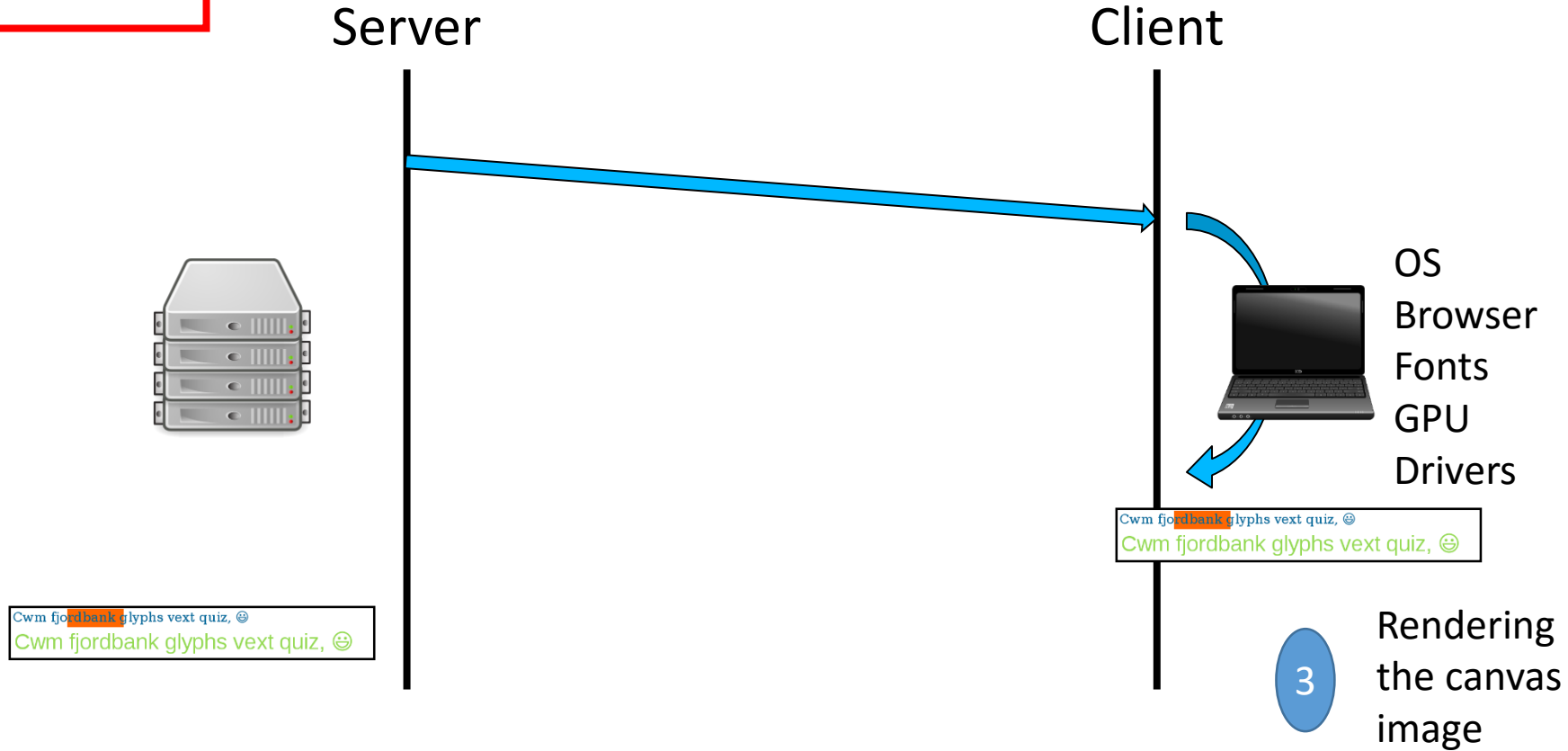
Connection phase



Our challenge-response system

15

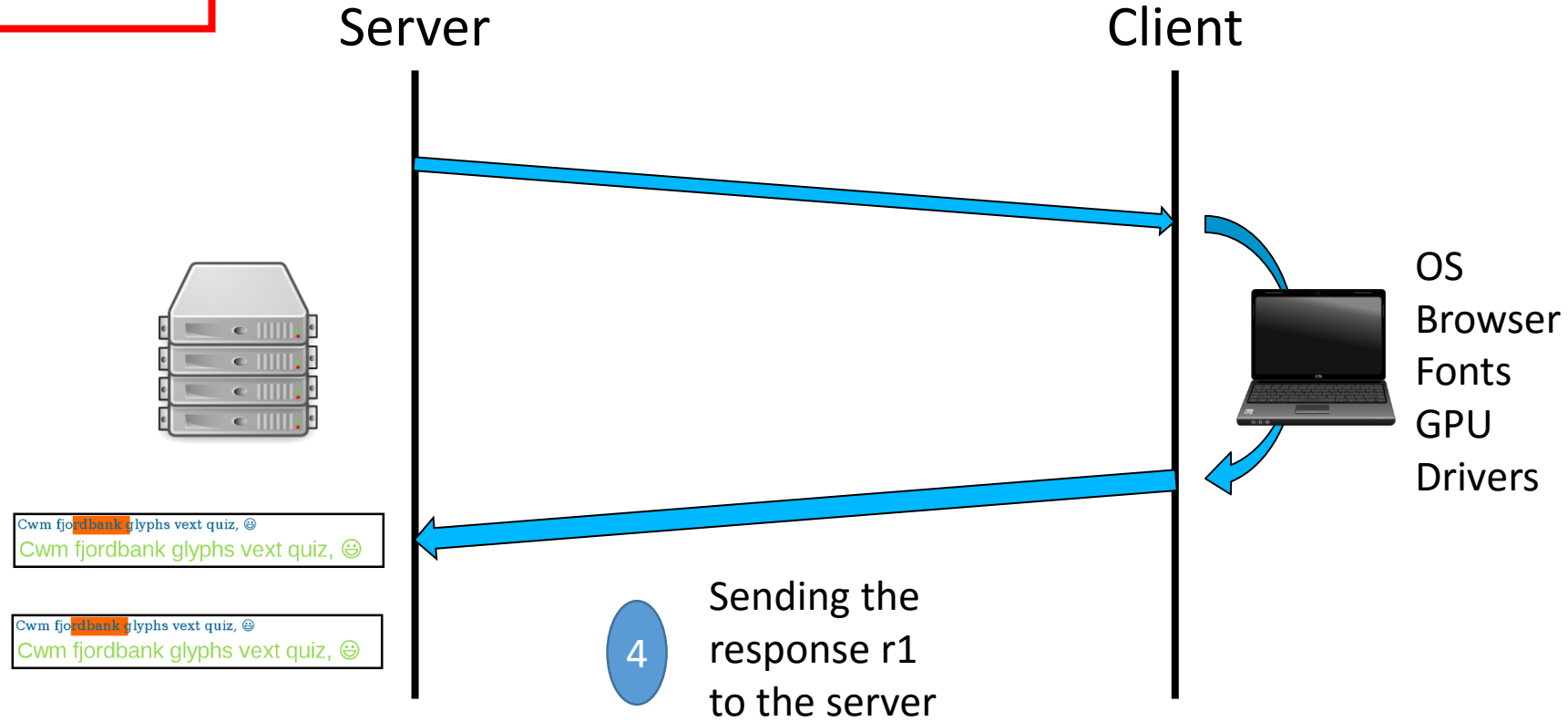
Connection phase



Our challenge-response system

15

Connection phase



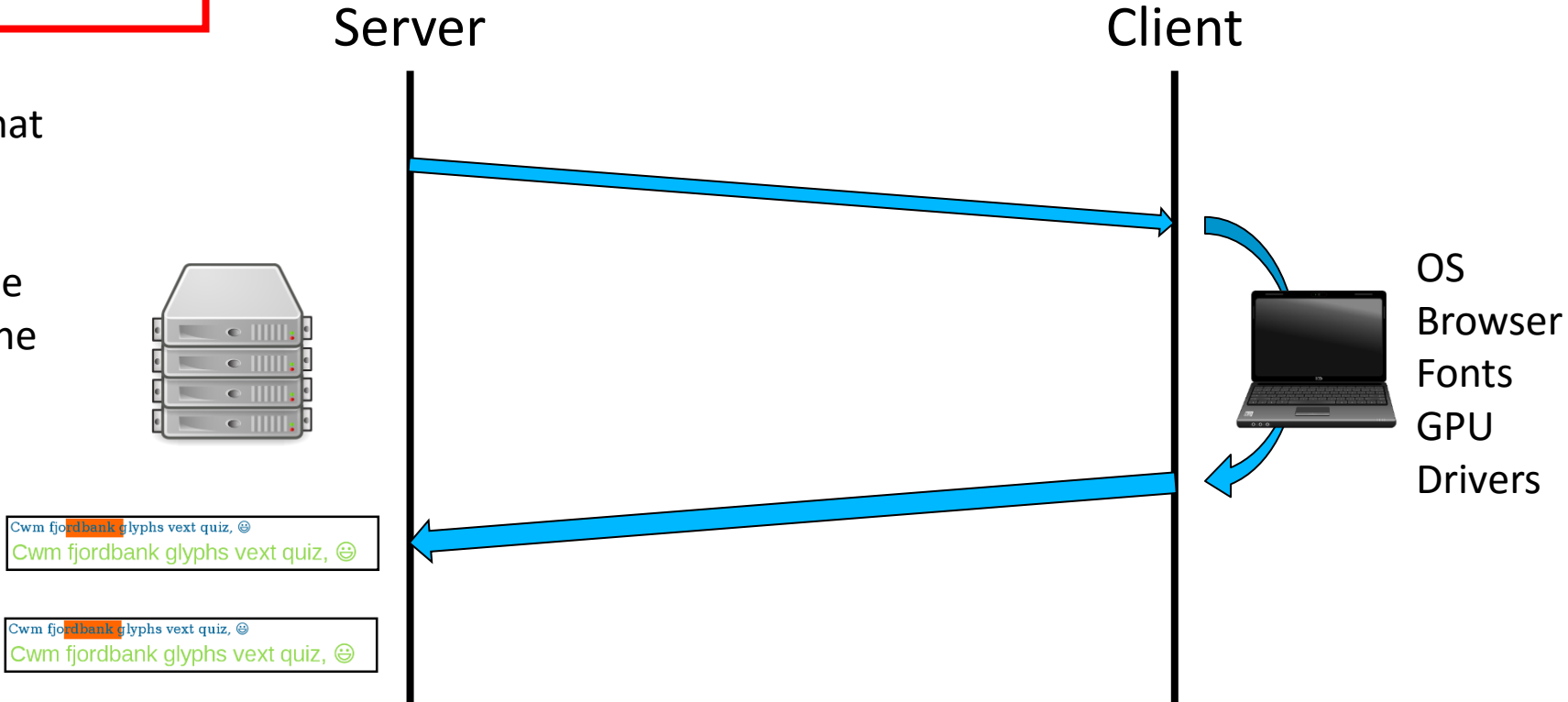
Our challenge-response system

15

Connection phase

5

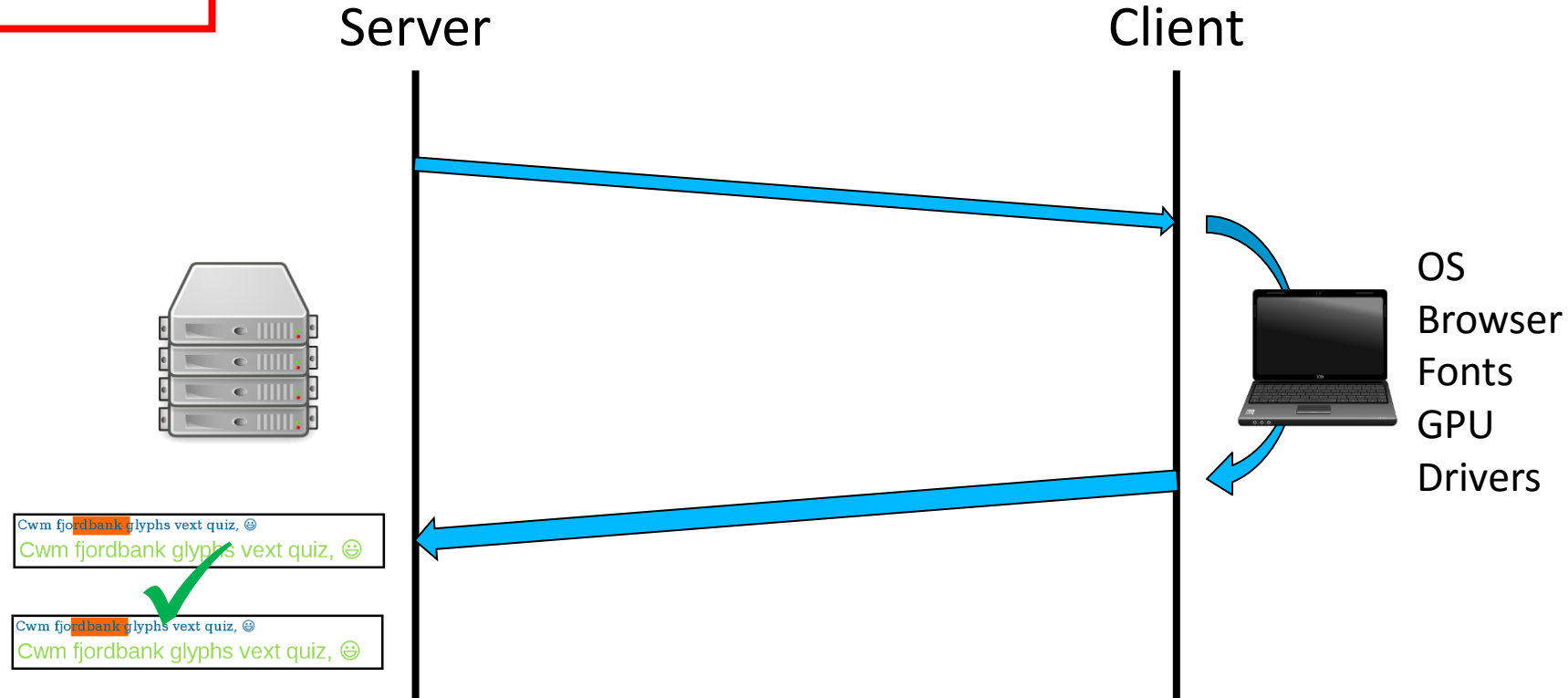
Verifying that the client's answer r_1 matches the one from the previous connection



Our challenge-response system

15

Connection phase



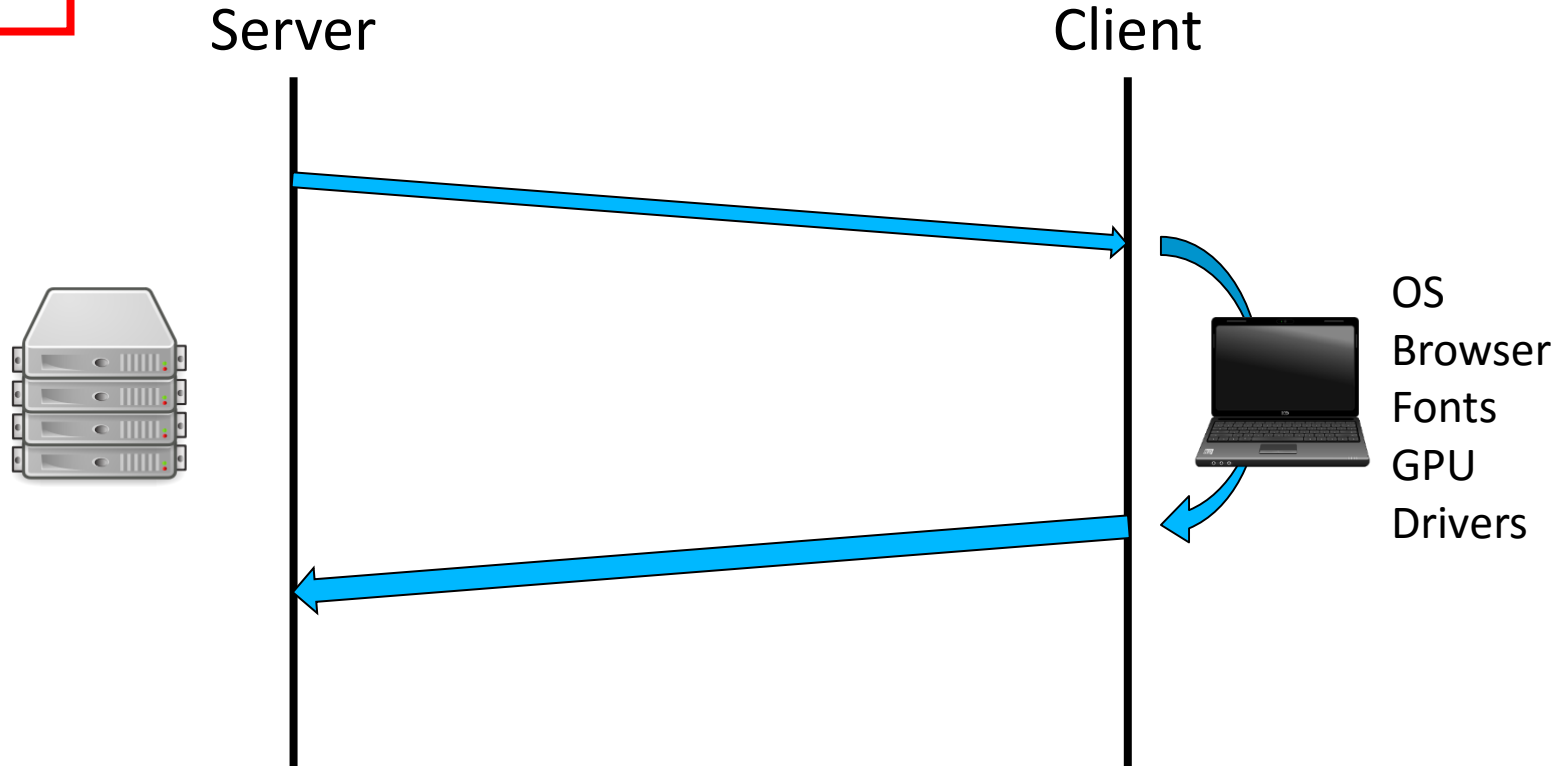
6

If the rendering is verified,
we generate and send a new
challenge c2

Our challenge-response system

15

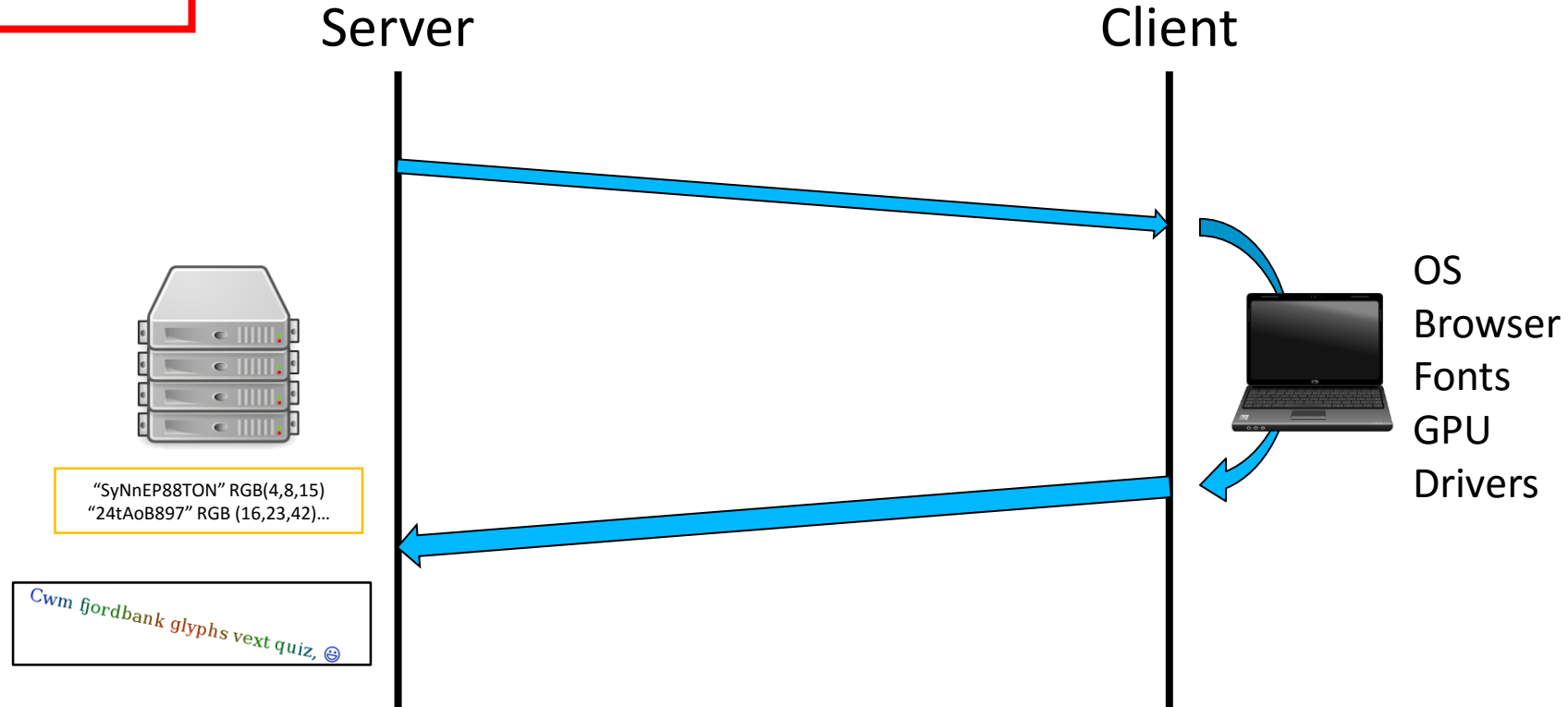
Connection phase



Our challenge-response system

15

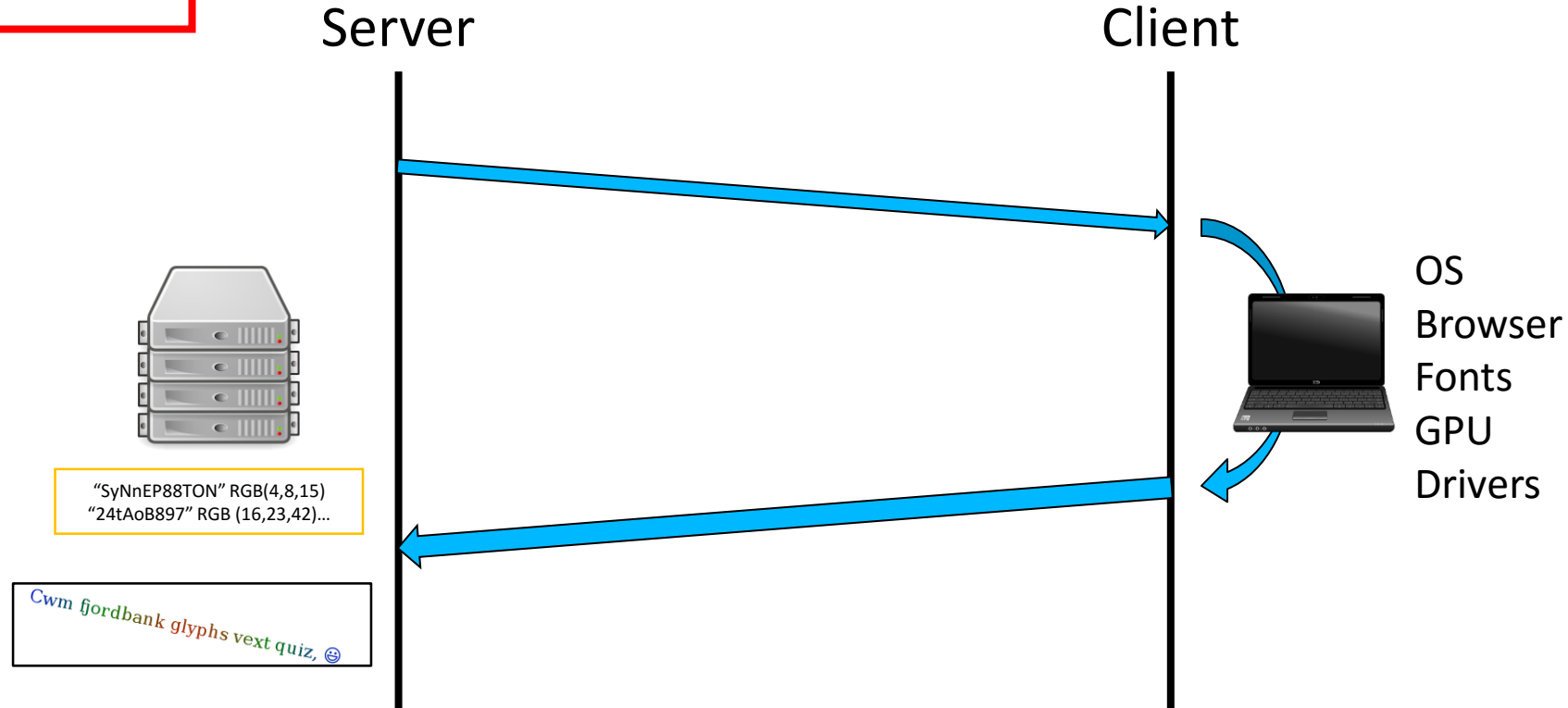
Connection phase



Our challenge-response system

15

Connection phase



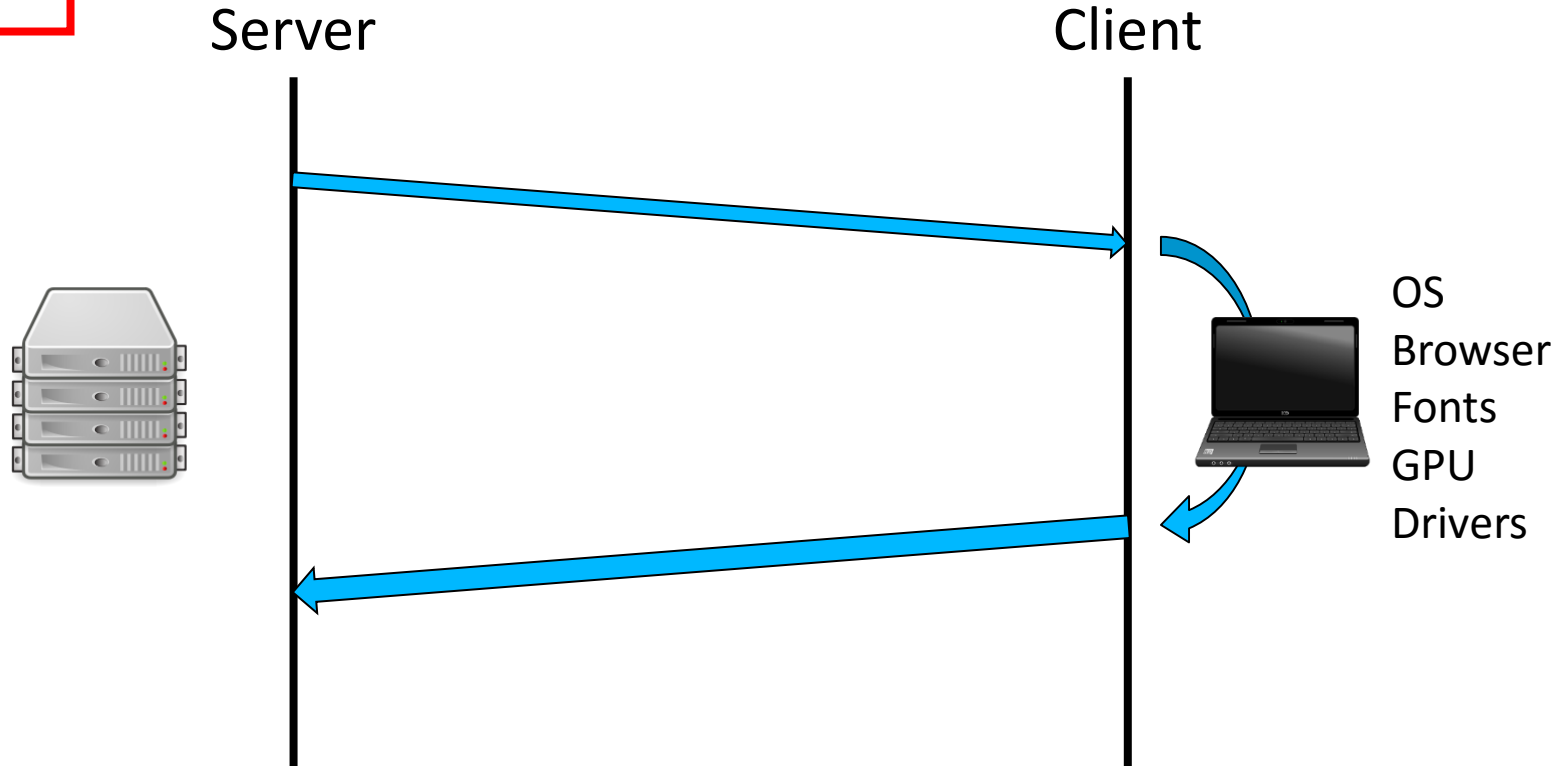
7

Storing both the challenge c2 and the response r2 for the next connection

Our challenge-response system

15

Connection phase



Loop n°1 with c_1, r_1 : verify the current connection

Loop n°2 with c_2, r_2 : verify the next connection

Cwm fjordbank glyphs vext quiz, 😊

~~Cwm fjordbank glyphs vext quiz, 😊~~

~~Cwm fjordbank glyphs vext quiz, 😊~~

~~Cwm fjordbank glyphs vext quiz, 😊~~

~~Cwm fjordbank glyphs vext quiz, 😊~~

Cwm fjordbank glyphs vext quiz, 😊


Cwm fjordbank glyphs vext quiz, 😊

Cwm fjordbank glyphs vext quiz, 😊


Cv

Phase 3

Incredible diversity of challenges

Parameter	Description	Number of combinations
String content	[A-Z] [a-z] [0-9]	62^{10}
Size	From size 30 to 78	49
Rotation	Precision up to the tenth digit	$360^{\circ} \times 10 = 3600$
Color with gradients 	RGB color model encoded on 8 bits	$((2^8)^3)^2 = 2^{48}$
Shadow color	RGB color model encoded on 8 bits	2^{24}
Shadow strength	From 0 to 50	51

Incredible diversity of challenges

Parameter	Description	Number of combinations
String content	[A-Z] [a-z] [0-9]	62^{10}
Size	From size 30 to 78	49
Rotation	Precision up to the tenth digit	$360^\circ \times 10 = 3600$
Color with gradients 	RGB color model encoded on 8 bits	$((2^8)^3)^2 = 2^{48}$
Shadow color	RGB color model encoded on 8 bits	2^{24}
Shadow strength	From 0 to 50	51

- $62^{10} \times 49 \times 3600 \times 2^{48} \times 2^{24} \times 51 \approx 2^{154}$ challenges
- 2.3×10^{50} bits of space with an average of 10kb per response

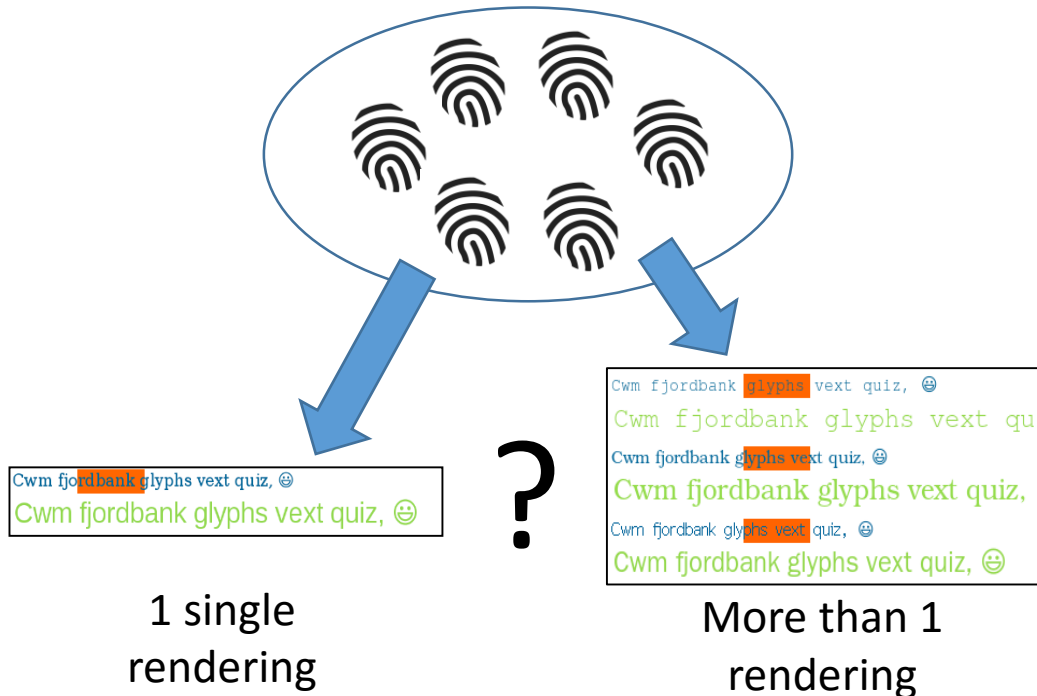
Great diversity of results

- Many different responses for the exact same set of instructions



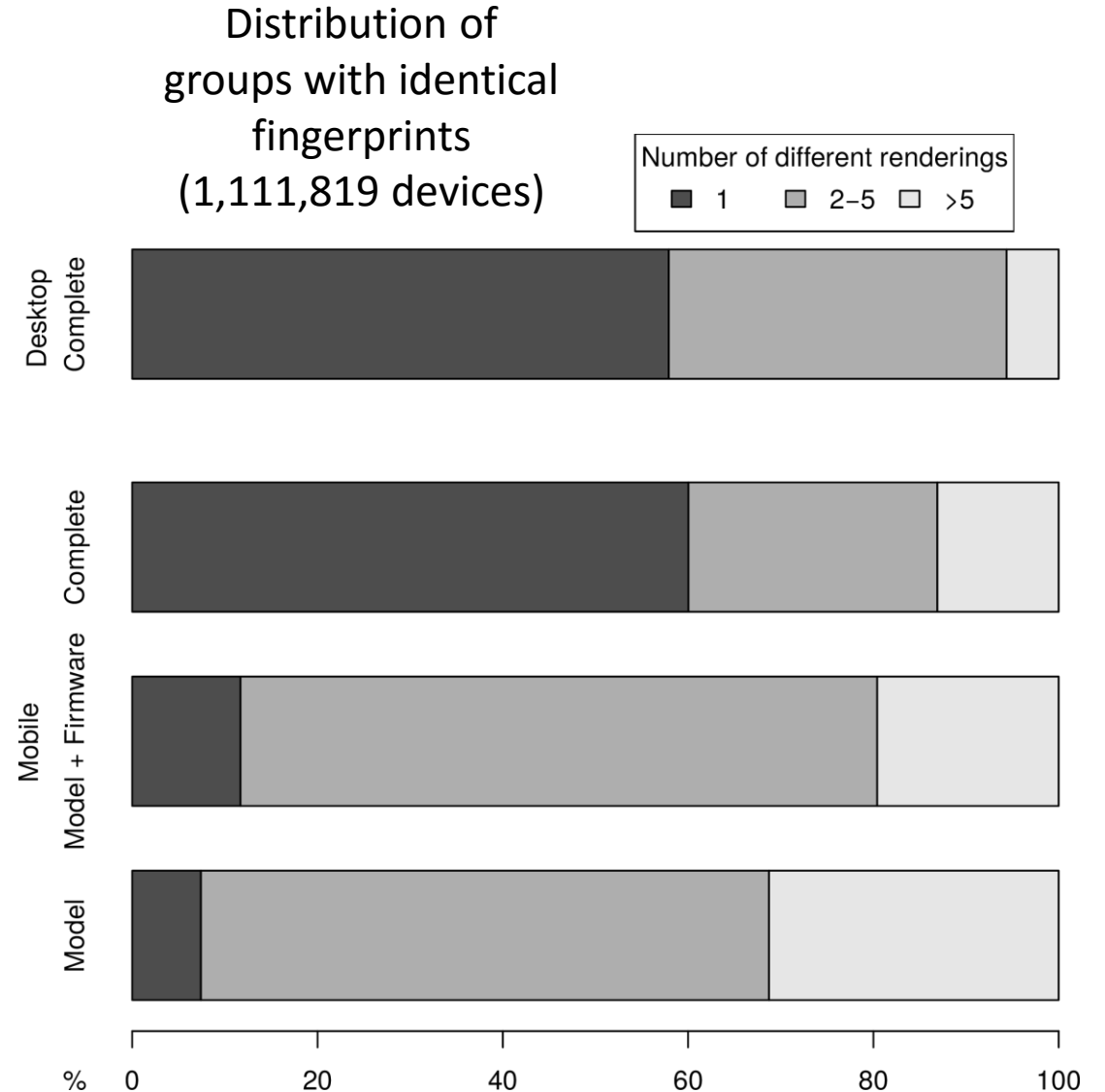
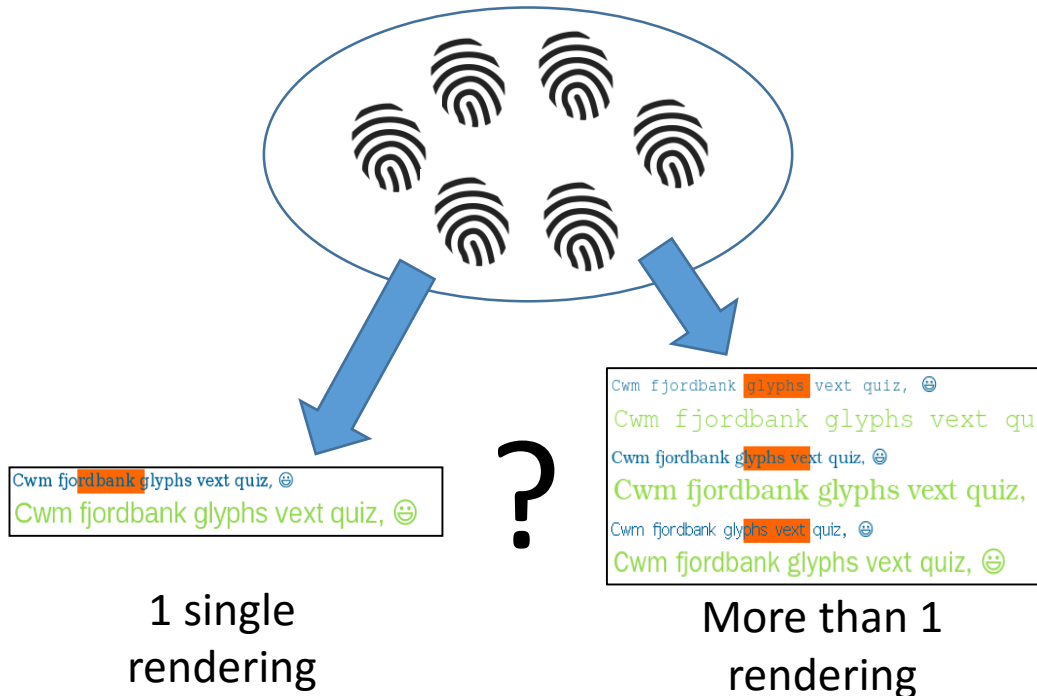
Great diversity of results

- Many different responses for the exact same set of instructions
- Protection against configuration recovery



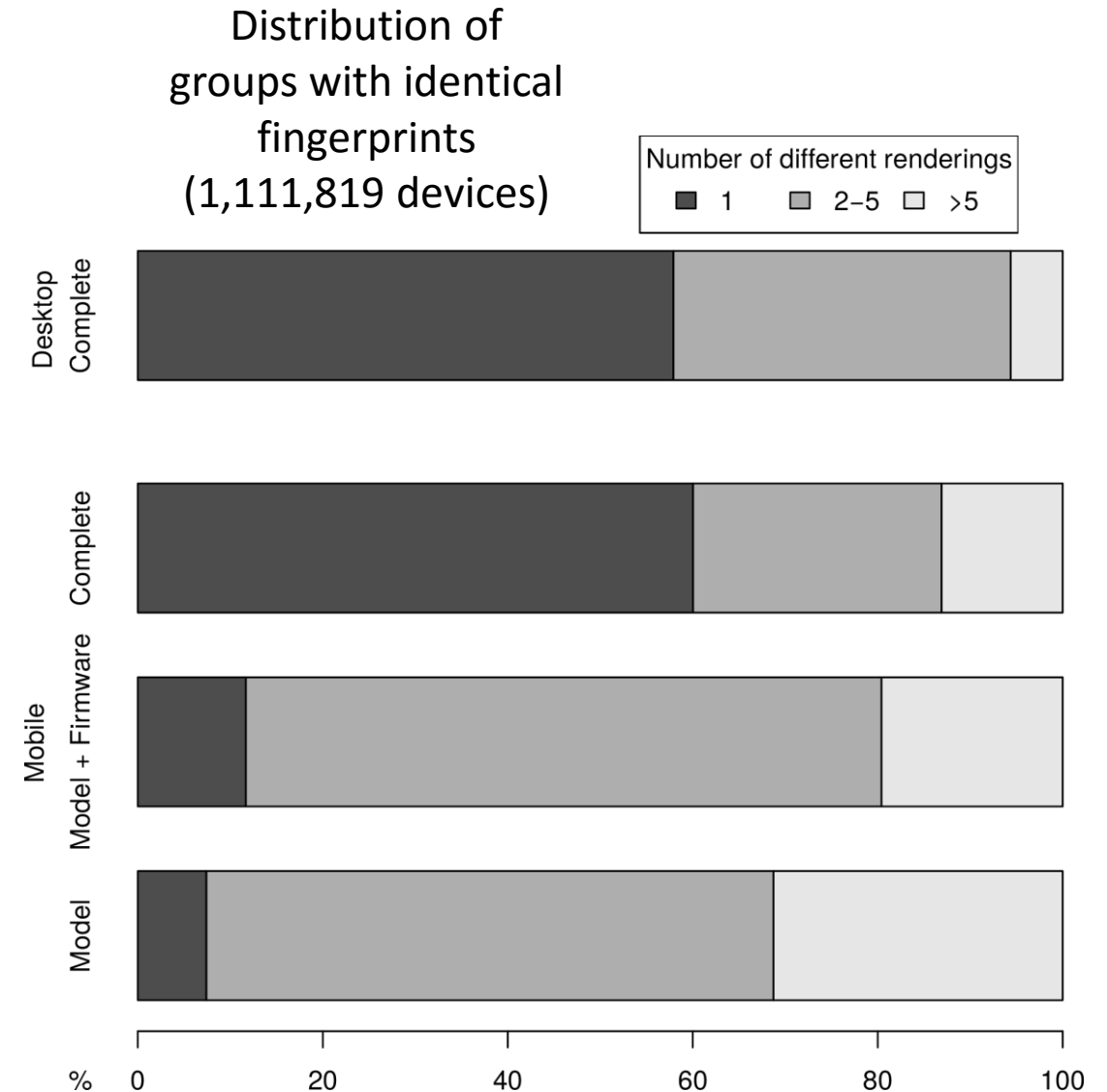
Great diversity of results

- Many different responses for the exact same set of instructions
- Protection against configuration recovery



Great diversity of results

- Many different responses for the exact same set of instructions
- Protection against configuration recovery
- Having the same device as your victim does not guarantee that it can reproduce the expected rendering with stolen credentials.



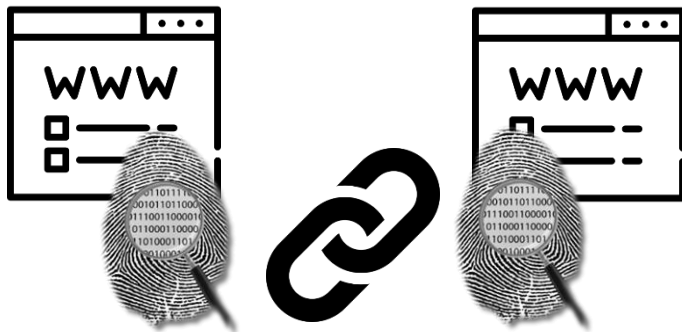
Attacks blocked or mitigated by our scheme

- Replay attack
- MITM or relay attacks
- Preplay attack (collecting all possible values beforehand)
- Guessing or building the right response
- Configuration recovery

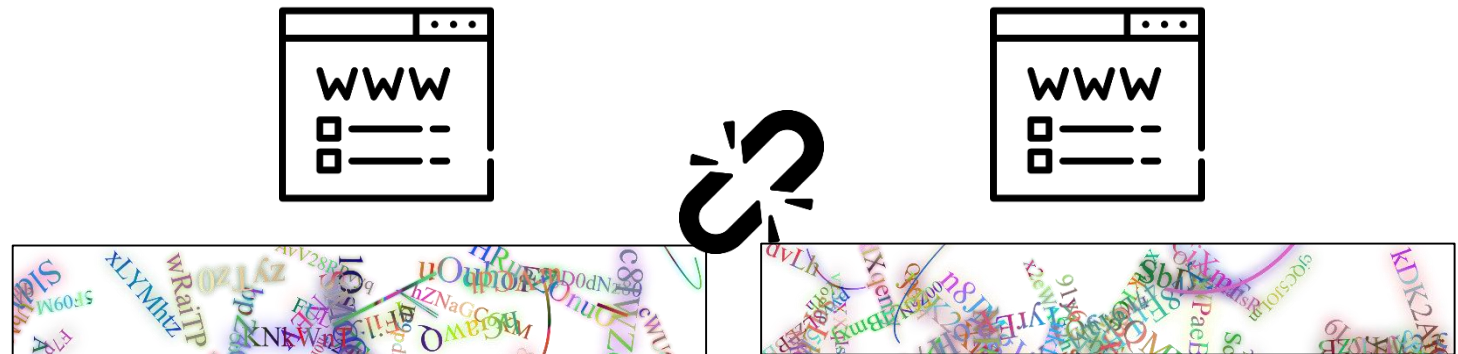


- In this work, canvas fingerprinting is used in a first-party context to augment authentication.
- It complements the use of traditional cookies as an extra layer of protection but it does not provide websites with any additional linking power (we collect only randomly generated canvas fingerprints).

Traditional fingerprinting



Our scheme with canvas fingerprinting



- Using canvas fingerprinting to augment authentication
- Fast, transparent and frictionless for the user
- Resiliency to a lot of different attacks because of the high diversity of challenges and results
- Code and demo: <https://plaperdr.github.io/morellian-canvas/>



Thank you!

Any questions?

Contact

 pierre.laperdrix@cispa.saarland

 @RockPartridge

Websites

<https://amiunique.org>

<https://plaperdr.github.io/morellian-canvas/>