Arcade

URL Elicitation deep dive

Third-party OAuth solved (and more!)

Nate Barbettini Founding Engineer, Arcade.dev
email nate@arcade.dev
X @nbarbettini

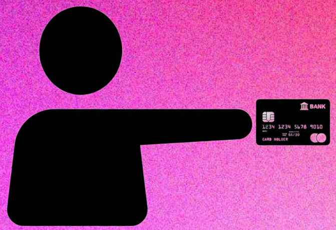
Arcade

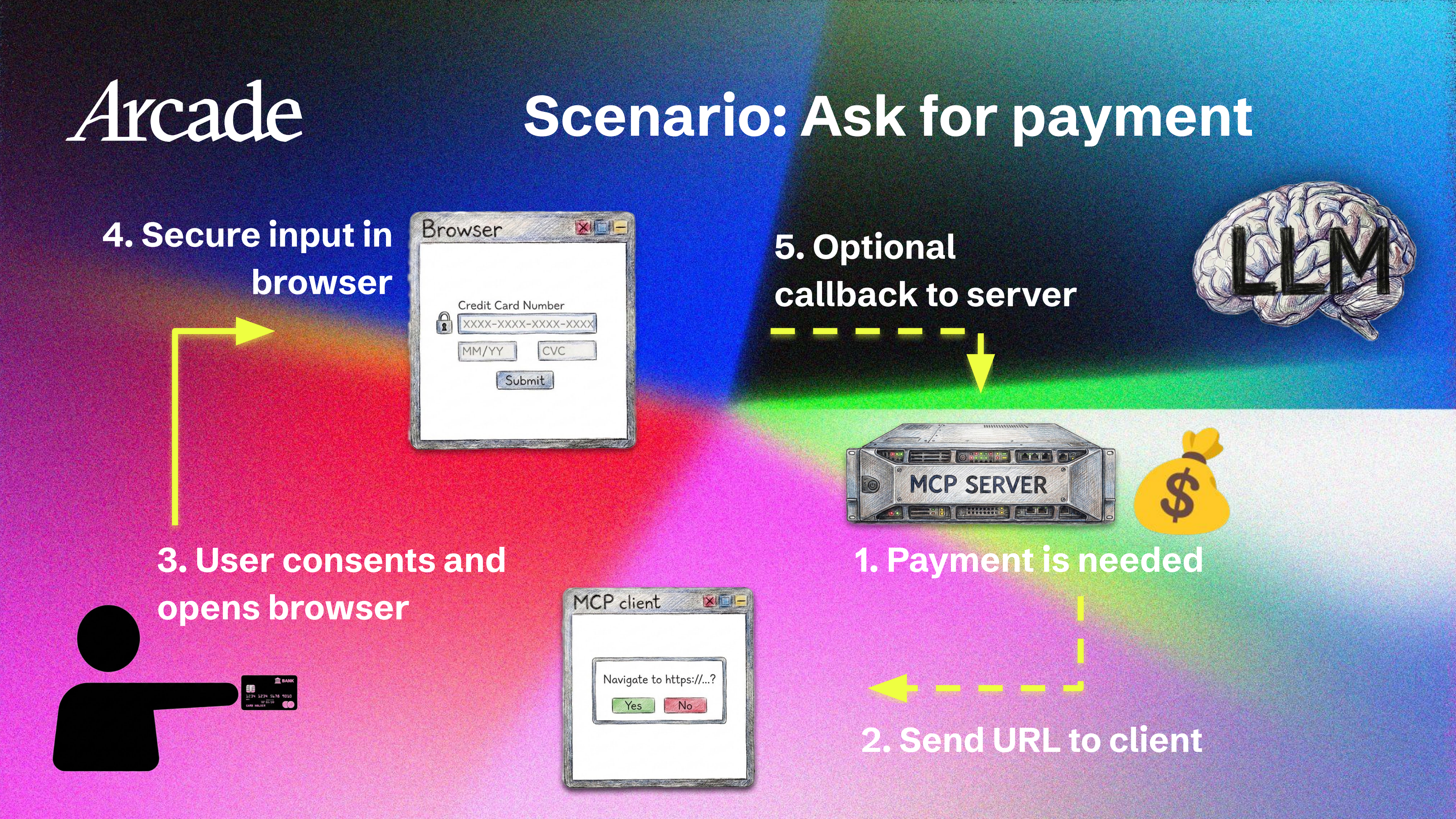
URL Elicitation gives MCP servers a safe way to cross trust boundaries.

Some interactions are too sensitive to be chat messages.

Arcade

Scenario: Ask for payment




Arcade
Scenario: Ask for payment
4. Secure input in browser
Browser
Credit Card Number
XXXX-XXXX-XXXX-XXXX
MM/YY
CVC
Submit
5. Optional callback to server
LLM
MCP SERVER
1. Payment is needed
3. User consents and opens browser
MCP client
Navigate to https://...?
Yes
No
2. Send URL to client

Arcade

URL Elicitation for sensitive input

✅ Server may send a URL to the client at any time, or in response to an action like a tool call

✅ Client must get consent from end-user to open browser

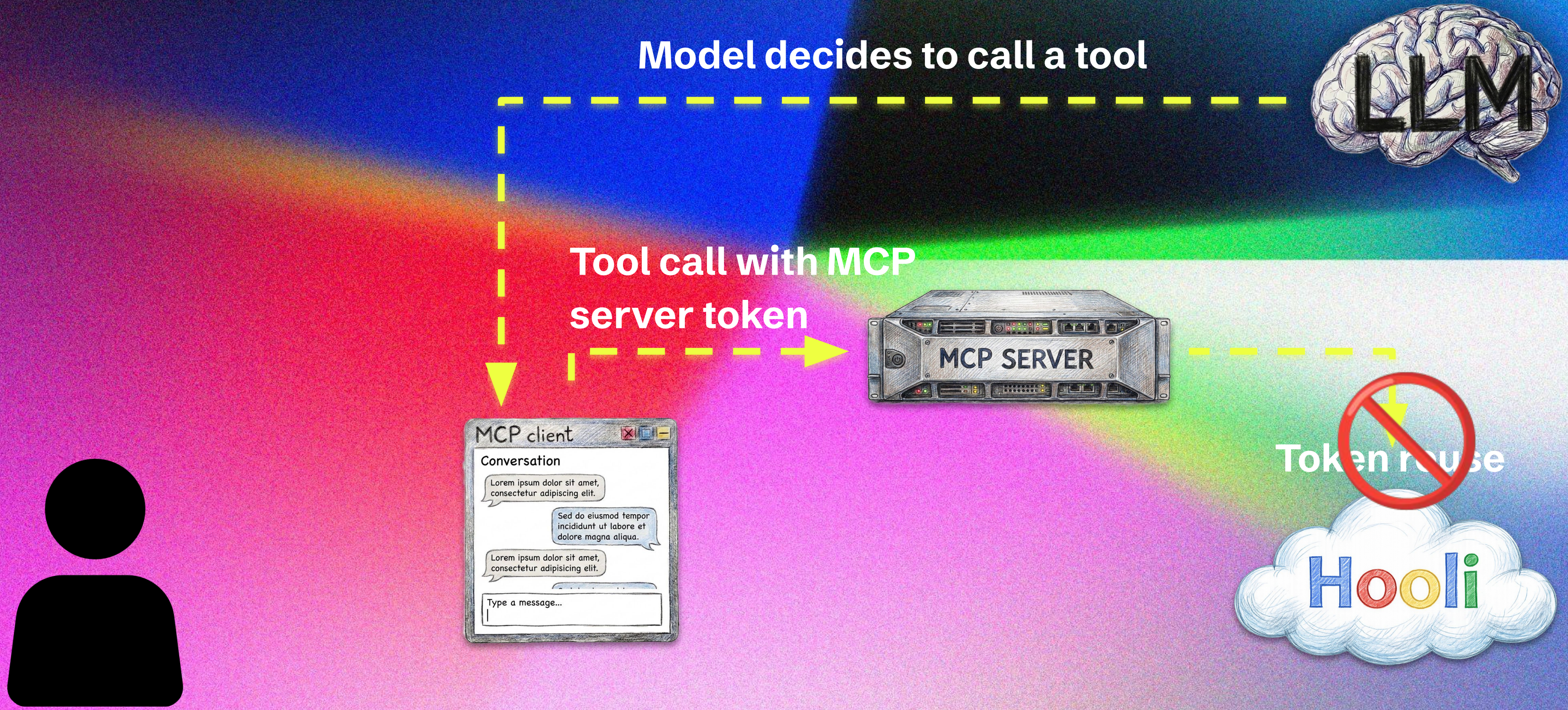
✅ User interaction is **out of band**, never exposed to the client or LLM

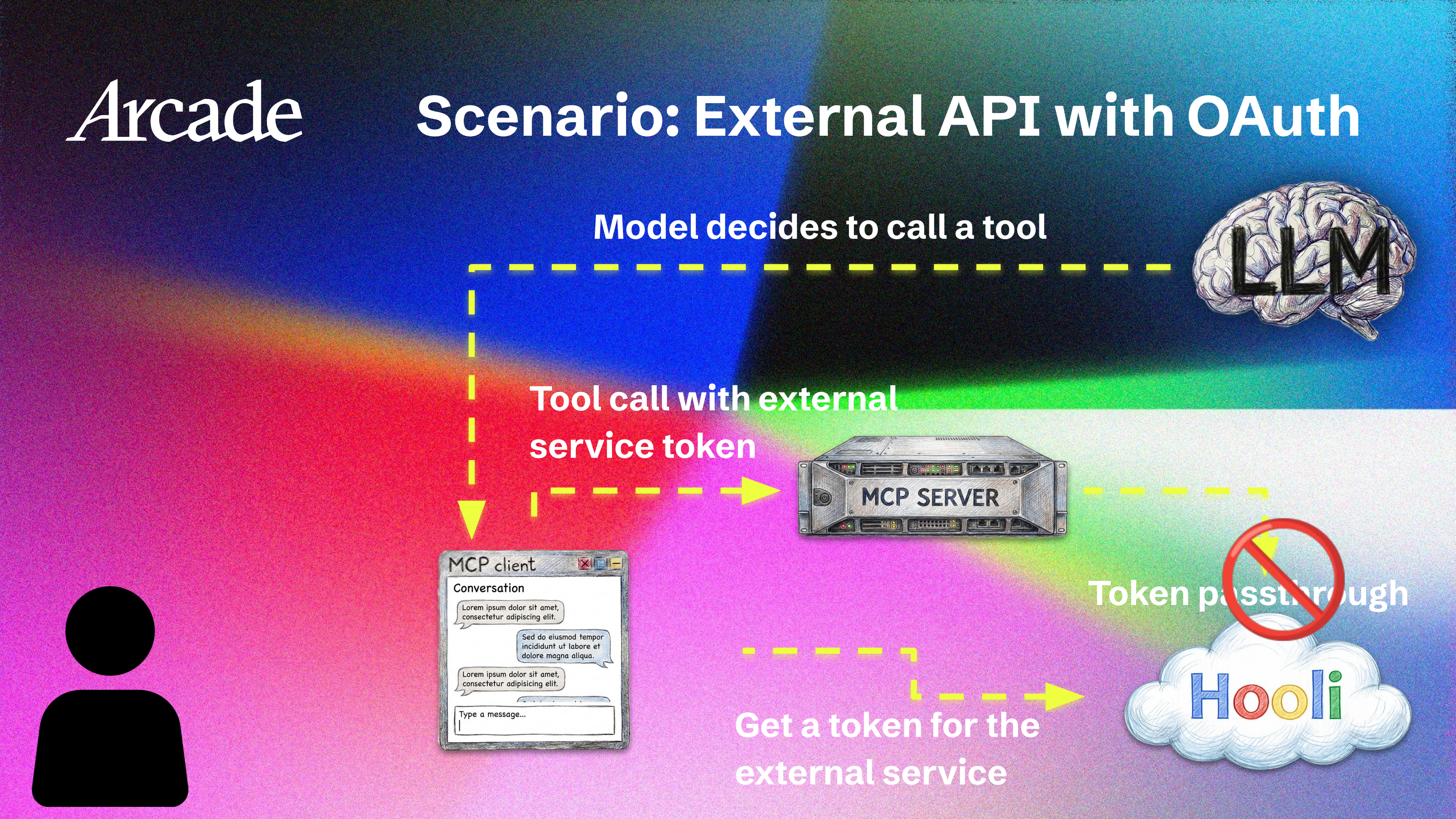
Arcade

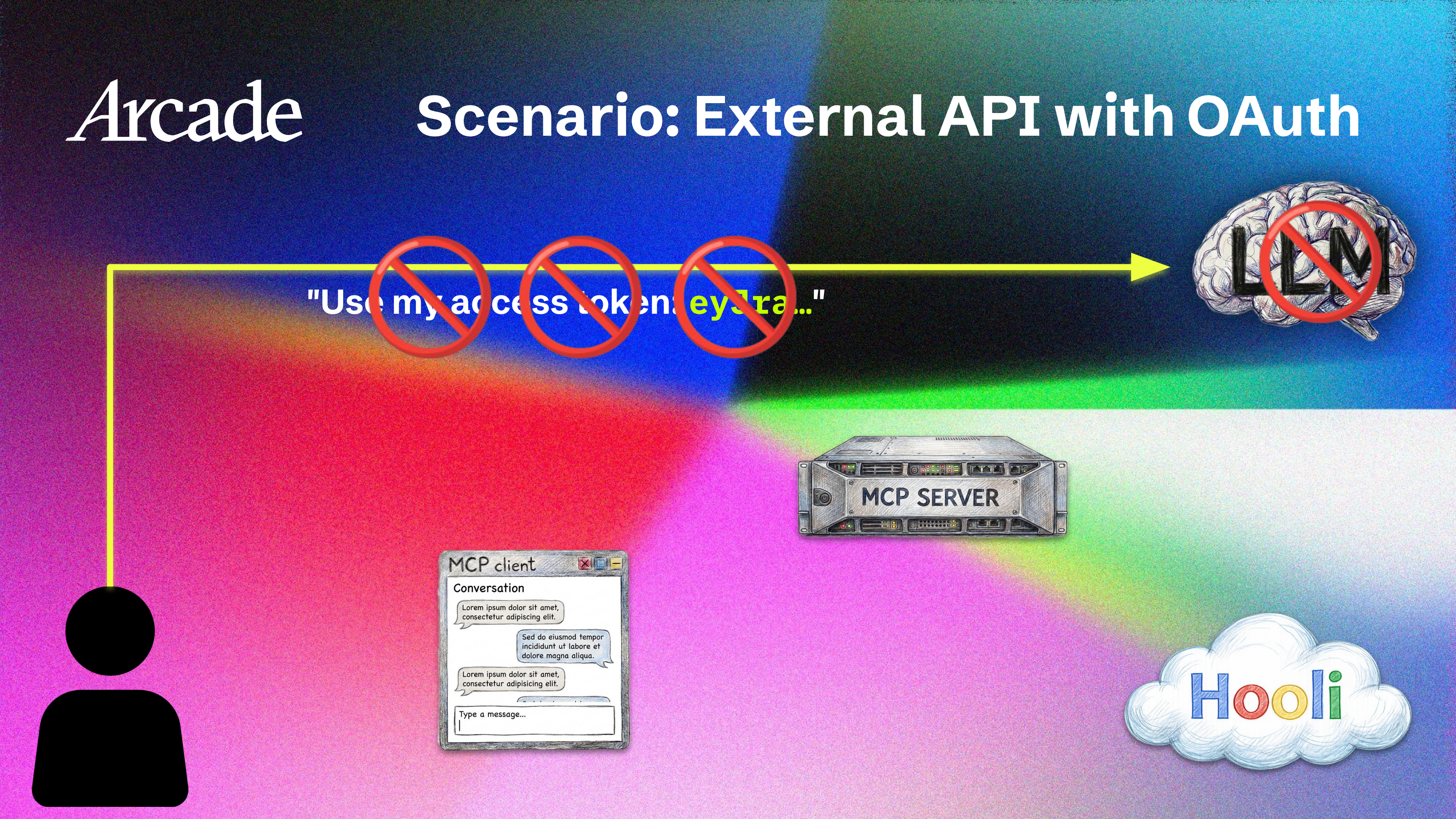
What about external OAuth?

Arcade

Scenario: External API with OAuth




Arcade
Scenario: External API with OAuth
Model decides to call a tool
LLM
Tool call with external service token
MCP SERVER
MCP client
Conversation
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Type a message...
Token passthrough
Hooli
Get a token for the external service

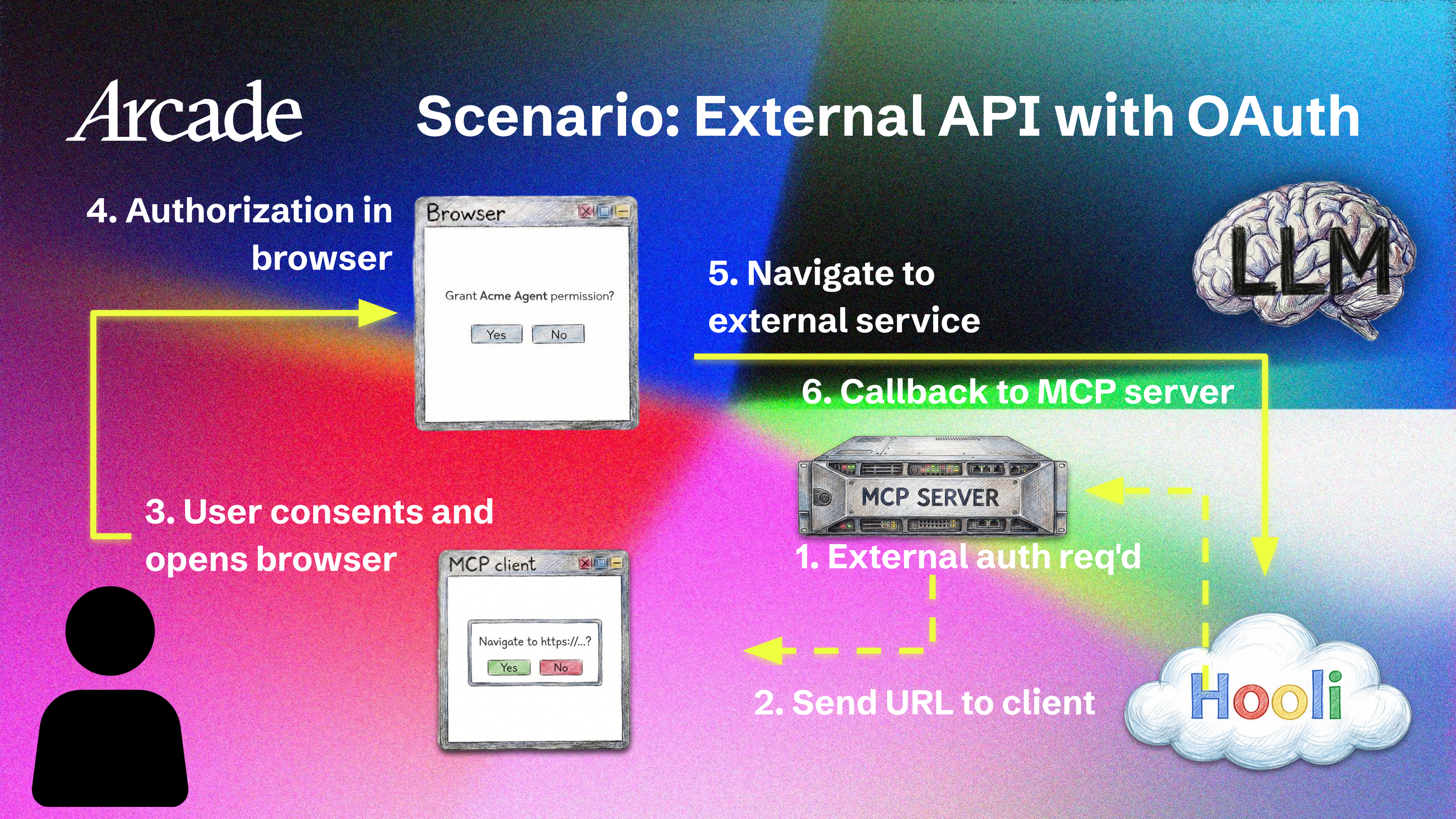

Arcade
Scenario: External API with OAuth
"Use my access token: eyJra..."
LLM
MCP SERVER
MCP client
Conversation
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.
Lorem ipsum dolor sit amet, consectetur adipiscing elit.
Type a message...
Hooli

Two trust boundaries

MCP client <> MCP server

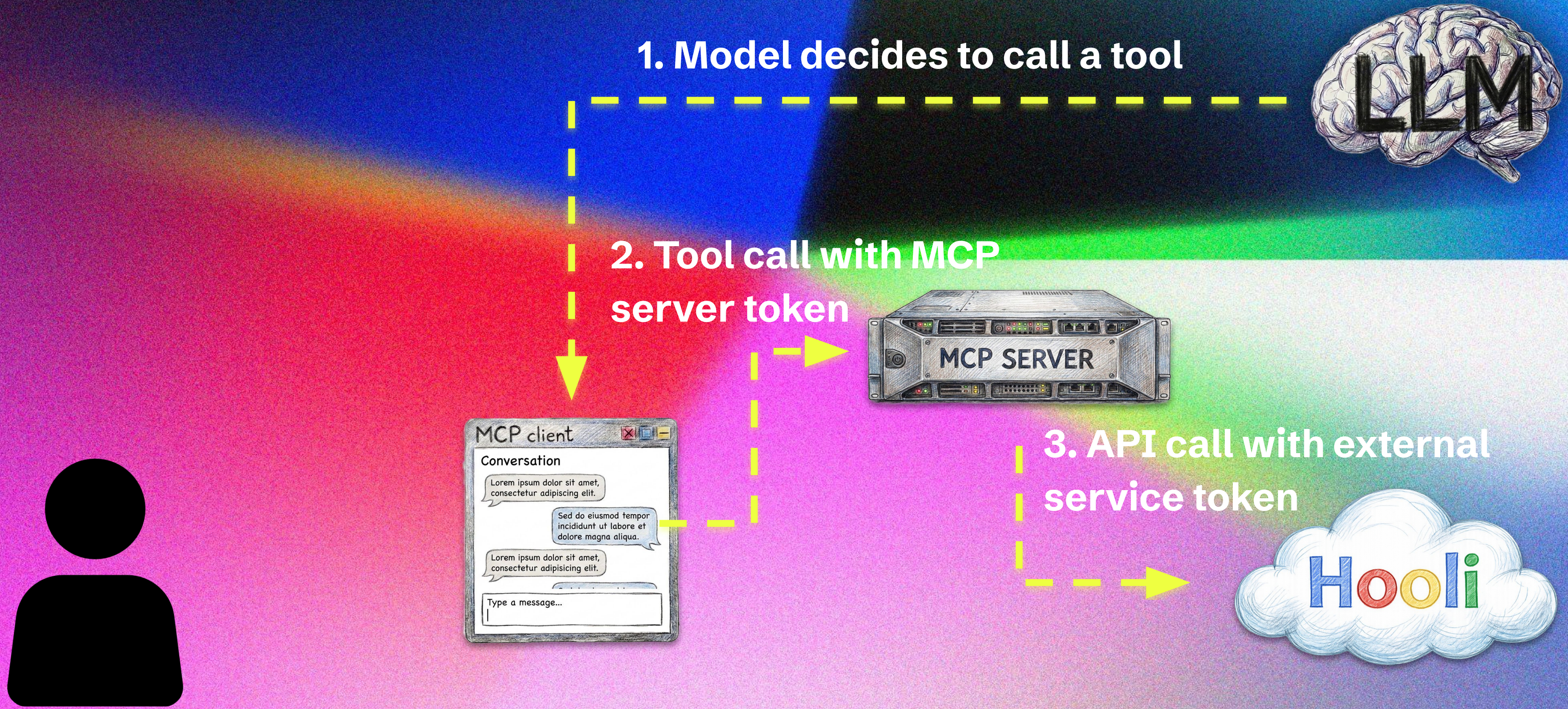
MCP server <> external service

The MCP server is not a magical tunnel!


Arcade
Scenario: External API with OAuth
4. Authorization in browser
Browser
Grant Acme Agent permission?
Yes
No
5. Navigate to external service
LLM
6. Callback to MCP server
MCP SERVER
3. User consents and opens browser
MCP client
Navigate to https://...?
Yes
No
1. External auth req'd
2. Send URL to client
Hooli

Arcade

Scenario: External API with OAuth



Arcade

URL Elicitation for external auth

✅ Plugs into the existing world of browser-based OAuth

✅ Correct trust boundary: MCP client has **only one** token, for the MCP server

✅ User interaction is **out of band**, never exposed to the client or LLM

Key takeaways

Arcade

- URL Elicitation gives MCP servers a way to trigger user interaction (a URL)
- User interaction occurs **out of band** of the client, LLM, and chat context
- Useful for payments and sensitive inputs like API keys
- Useful for preserving the **trust boundary** between the MCP server and an external OAuth API

Arcade

Thank you

Questions or comments?

Nate Barbettini Founding engineer, Arcade.dev
email nate@arcade.dev
X @nbarbettini