

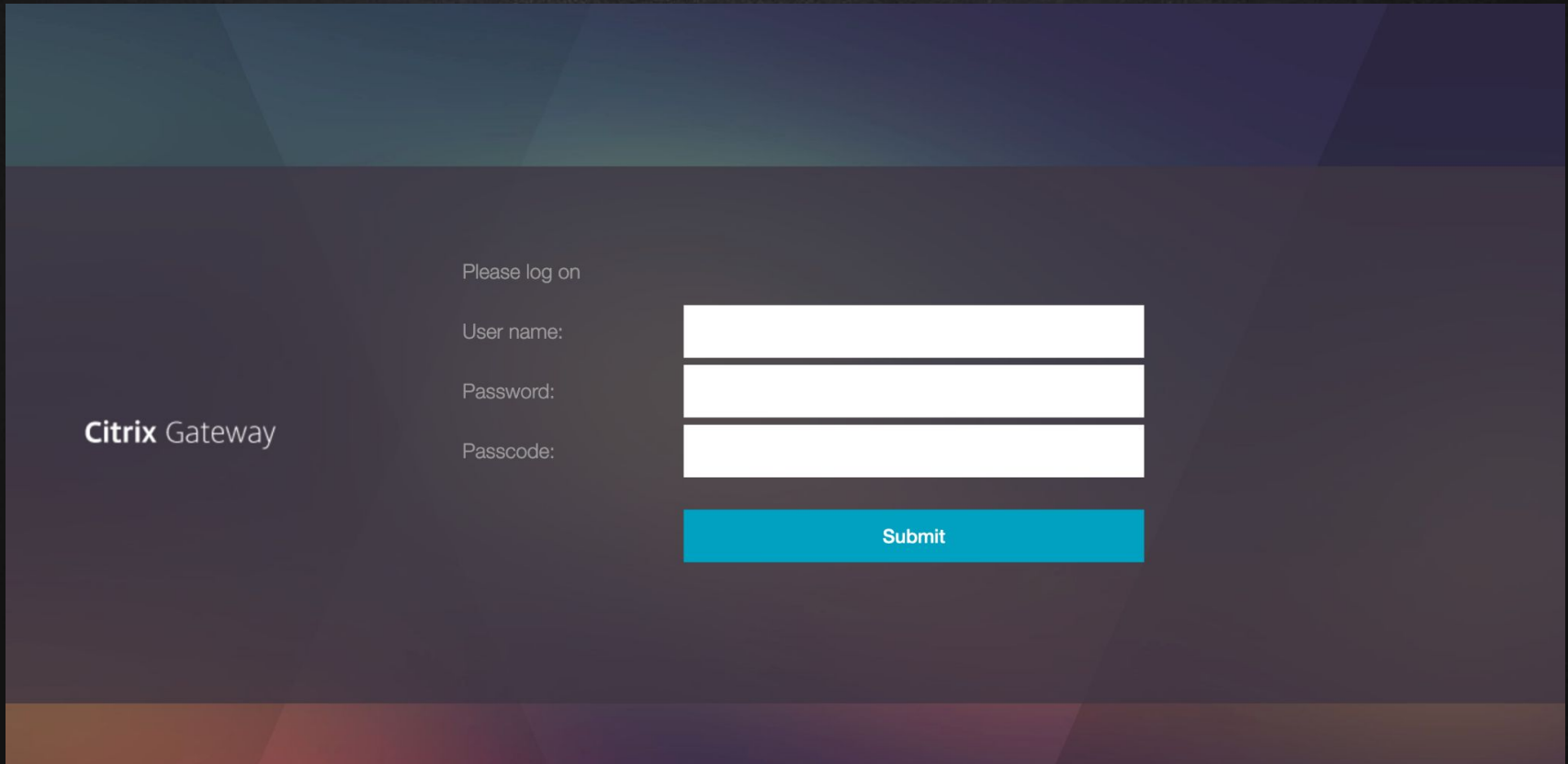
NOT SO SMART CARD

A TALE OF CERTIFICATES, MTLS AND
“BYPASSING” MULTI-FACTOR AUTHENTICATION

INTRO

- ✗ Task: Perform a pentest of customer's Citrix infrastructure
- ✗ Focus: Vulnerabilities regarding authentication and other potential initial access vectors
- ✗ I had valid credentials, so I could take a closer look at various steps involved when authenticating

THIS IS WHAT IT LOOKS LIKE



The image shows a login interface for Citrix Gateway. The background is a dark, textured surface with a horizontal band of lighter, geometric shapes in shades of blue and purple. On the left, the text "Citrix Gateway" is displayed in a white, sans-serif font. To the right of this, the text "Please log on" is centered. Below this, there are three input fields: "User name:", "Password:", and "Passcode:". Each field is represented by a white rectangular box. At the bottom of the input fields, there is a blue rectangular button with the text "Submit" in white.

Citrix Gateway

Please log on

User name:

Password:

Passcode:

Submit

HOW IT (USUALLY) GOES

- ✗ User enters username
- ✗ User enters password
- ✗ User enters another secret as well as a one-time password generated by a hardware token

this beautiful thingy
(thanks Wikipedia)



SAME FOR CUSTOMER... BUT

- ✗ They also run a PKI
- ✗ Each user has a smart card holding the user's certificate (they're mandatory to login on regular clients)
- ✗ If it works on a physical device, also securing remote access shouldn't be too hard, right?

RECAP: (M)TLS

Client

Server

ClientHello

ServerHello

Certificate

DemandClientCertificate

ServerHelloDone

ClientKeyExchange

ClientCertificate

ClientHelloDone

ChangeCipherSpec

Finished

ChangeCipherSpec

Finished

Both sides verify certificates after receiving them

ACTUAL IMPLEMENTATION

mTLS connection
successful?

no

Ask for username,
password and OTP

yes

Assume username
and ask for password

- ✗ This works seamless with any browser and doesn't require additional software
- ✗ It's completely transparent and without user's interaction
- ✗ Quality of life improvement for users holding a smart card
- ✗ No need to purchase RSA (\$\$\$) tokens for each employee

Citrix Gateway

Please log on

User name :

username@domain

Password :

|

Log On

IT'S HACKING* TIME!



*At least in Missouri, pressing F12 in your browser may be considered hacking:

<https://techcrunch.com/2021/10/15/f12-isnt-hacking-missouri-governor-threatens-to-prosecute-local-journalist-for-finding-exposed-state-data/>

Please log on

Citrix Gateway

User name :

username@domain

Password :

Log On

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

```
<div class="field CredentialTypeusername">
  <div class="left">
  <div class="right">
    <input id="login" class="editedCredential" name="login" type="text" autocomplete="off"
    spellcheck="false" disabled="true">
  </div>
</div>
<div class="field CredentialTypepassword">
<div class="field CredentialTypesavecredentials" style="display: none;">
```

Filter Styles

```
element {
}

.credentialform
input[type="text"]
[disabled], .credentialform
[disabled] {
  color: #666;
  background-color: #ccc;
}

.credentialform
input[type="text"],
.credentialform input[type="password"]
```

Please log on

Citrix Gateway

User name :

admin@domain

Password :

Log On

Inspector Console Debugger Network Style Editor Performance Memory Storage Accessibility Application

Search HTML

```
<div class="field CredentialTypeusername">
  <div class="left">
  <div class="right">
    <input id="login" class="editedCredential" name="login" type="text" autocomplete="off"
      spellcheck="false"> event
  </div>
</div>
<div class="field CredentialTypepassword">
<div class="field CredentialTypesavecredentials" style="display: none;">
```

Filter Styles

```
element {
}
.credentialform
input[type="text"],
.credentialform-input[type="text"],
.credentialform-pseudo-input
width: 385px;
font-size: 16px;
color: #666;
}
.credentialform
input[type="text"]
```

A man with long dark hair and glasses, wearing a dark jacket over a white t-shirt, stands in a cluttered office. He has his arms crossed and is looking directly at the camera. The office is filled with various items: a desk with a computer monitor, a printer, and a cup; a filing cabinet; a bulletin board with many papers; and a window with blinds. The lighting is dim, with a warm glow from the window.

HACKERMAN

HM

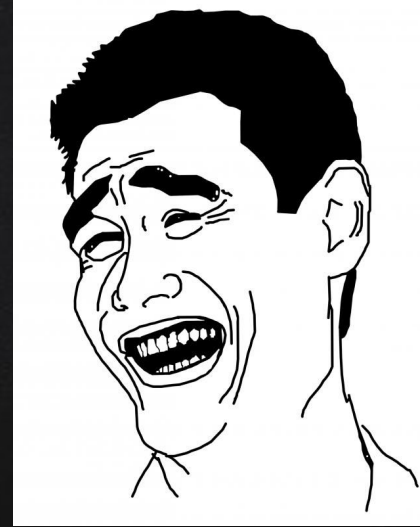
WHAT'S GOING ON?

- ✗ UPN is extracted from the certificate presented during client authentication and used for pre-filling the username field
- ✗ There is no check if the identity logging on afterwards matches the username in the previously presented certificate
- ✗ This can be abused without fancy hacking tools, just use the developer tools in your browser

You can authenticate with username + password of any user as long as you have any certificate issued by a trusted CA

MORE FUNSIES

- ✗ ANY certificate? What about computer certificates?
 - mTLS auth works, but there's no UPN, so fall back to "anonymous"
- ✗ How to obtain a computer certificate?
 - ~~Mimikatz?~~
 - ~~Fancy certificate extractor?~~
 - Just request a new one and make sure it's private key is marked exportable (follow me for more ghetto red team tips)
- ✗ Who logs and analyzes TLS handshakes to this detail level? Especially if there's a Load Balancer terminating TLS before forwarding packets to the Citrix backend?





THANKS!

<https://infosec.exchange/@edermi>

https://x.com/michael_eder_