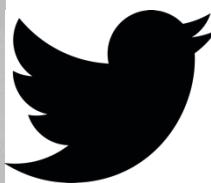
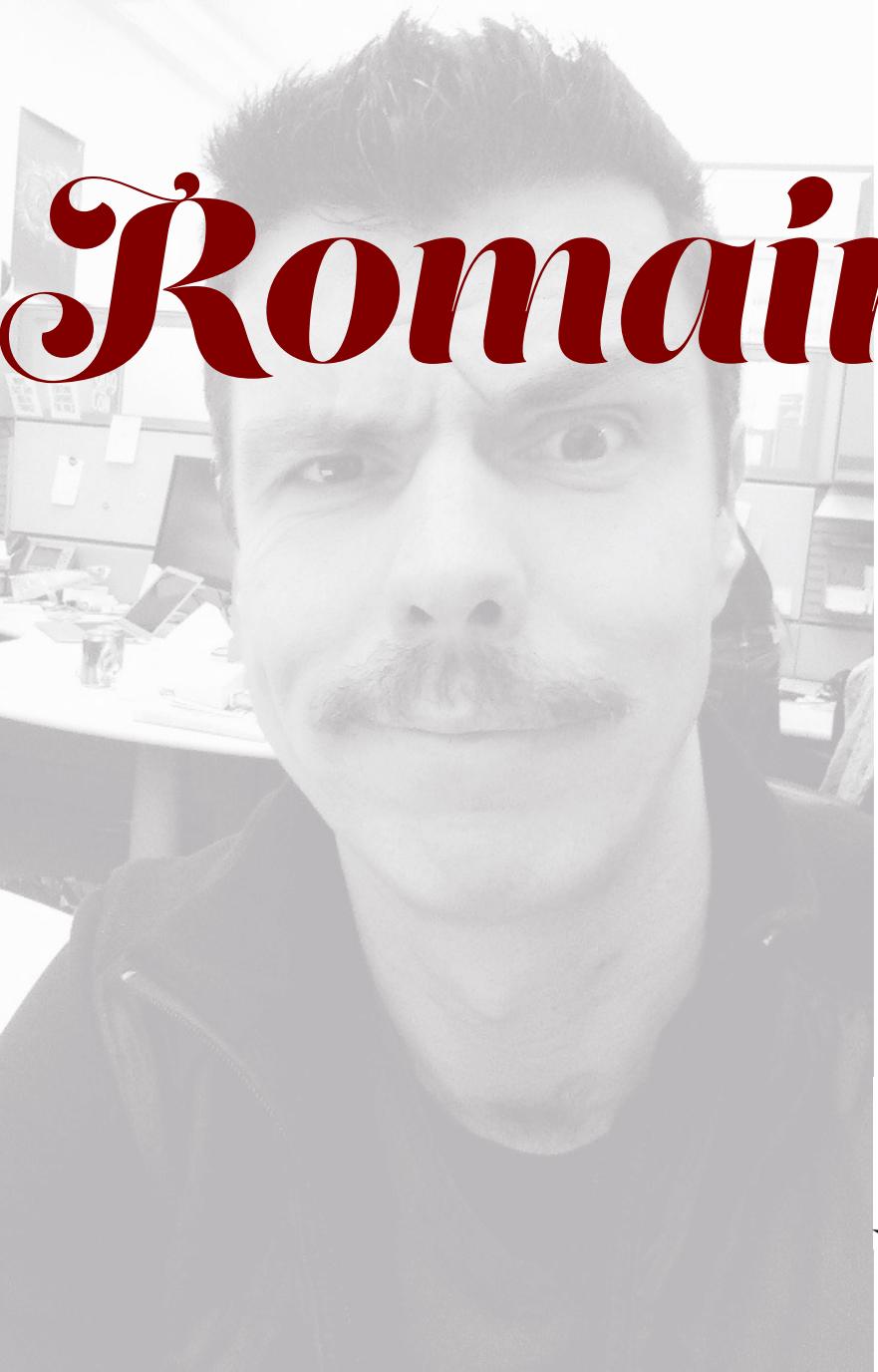




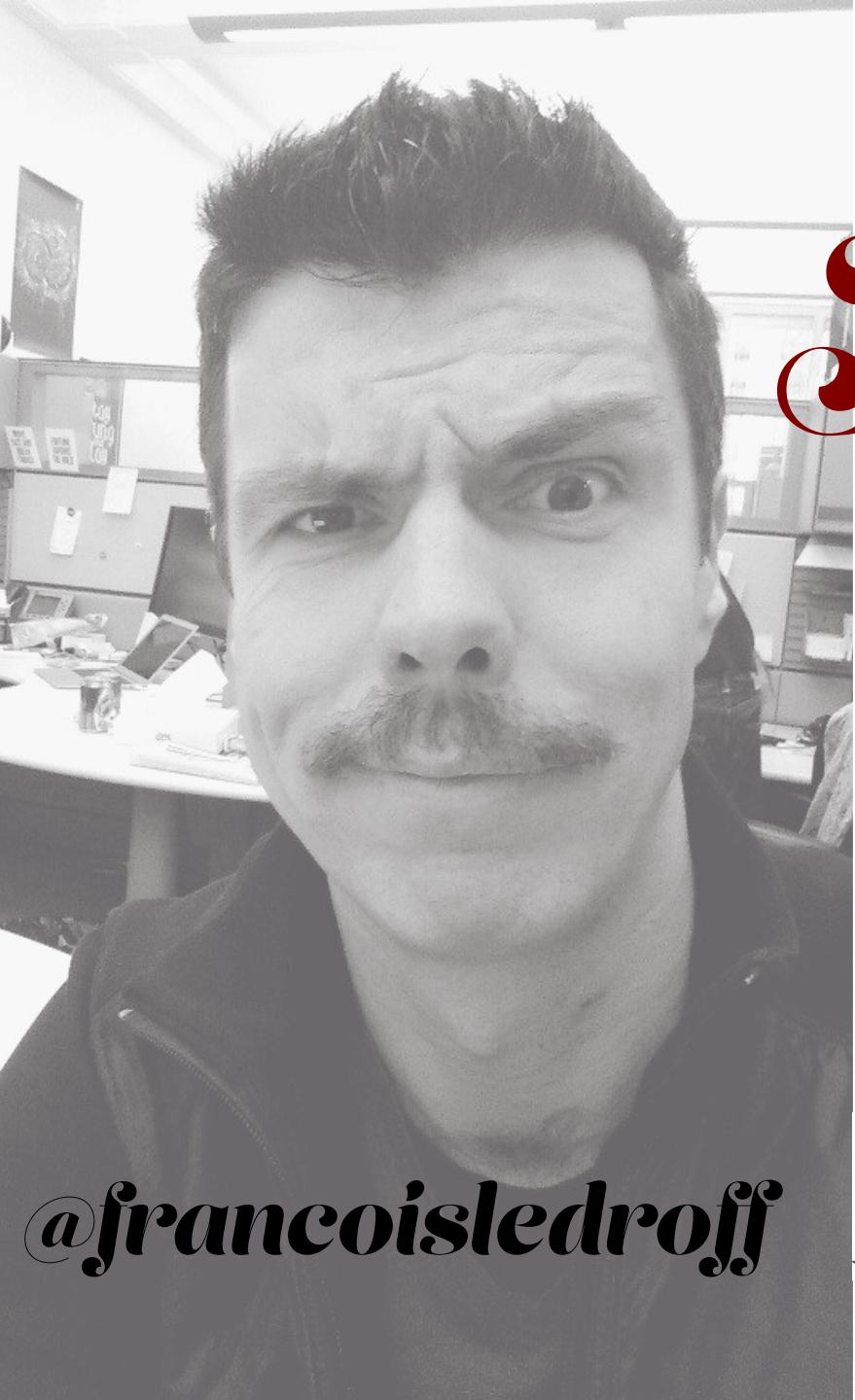
# Java & Security

# Romain



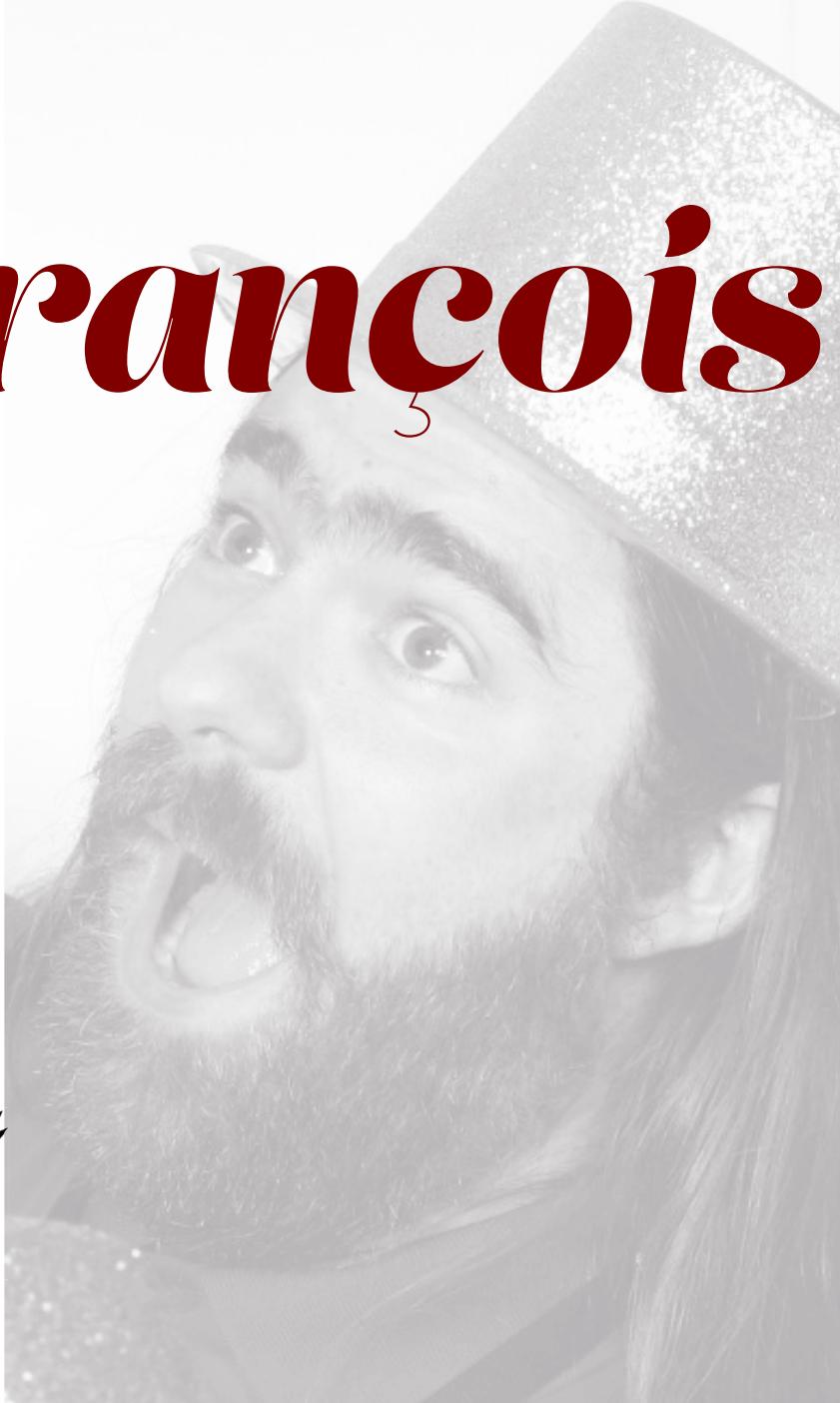
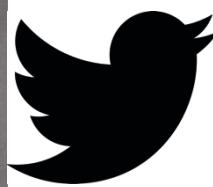
@rpelisse





@francoisledroff

# François





*Security Audit ?*

# Continuous Security



SEC-U.R.-IT-Y



# *Threat Modeling*

# Identify the threats

## STRIDE

- Spoofing Identity
- Tampering with Data
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

# Assess the risk

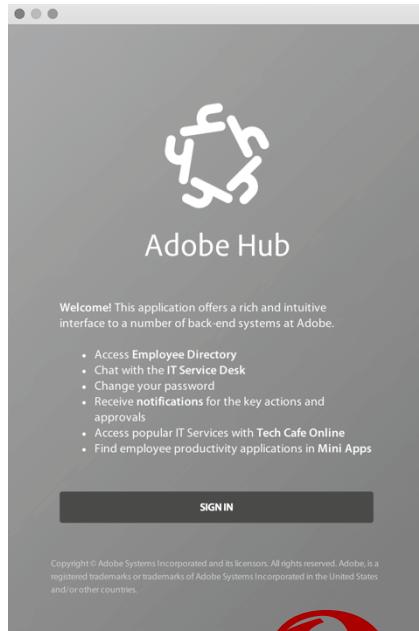
## DREAD

- *D*amage Potential
- *R*eproducibility
- *E*xloitability
- *A*ffected Users
- *D*iscoverability



# Deep Dive

through our sample use case



# Our use case

# jHipster



<https://jhipster.github.io/>

# Yo



```
~/workspace/github/devoxx2015 ⌚ 13:51:19
$ yo jhipster
```



```
Welcome to the JHipster Generator
```

```
? May JHipster anonymously report usage statistics to improve the tool? No
? (1/13) What is the base name of your application? barbus
? (2/13) What is your default Java package name? org.devoxx.barbus
? (3/13) Do you want to use Java 8? No (use Java 7)
? (4/13) Which *type* of authentication would you like to use? OAuth2
? (5/13) Which *type* of database would you like to use? NoSQL (MongoDB)
? (6/13) Which *production* database would you like to use? MongoDB
? (7/13) Which *development* database would you like to use? MongoDB
? (8/13) Do you want to use Hibernate 2nd level cache? No (this not p
? (9/13) Do you want to use clustered HTTP sessions? No
? (10/13) Do you want to use WebSockets? No
? (11/13) Would you like to use Maven or Gradle for building the back
? (12/13) Would you like to use Grunt or Gulp.js for building the fro
? (13/13) Would you like to use the Compass CSS Authoring Framework? I
  create package.json
  create bower.json
-----
```

# Spring Security

- Various Auth support
  - OAuth1 & OAuth 2
  - SAML
  - Kerberos
  - etc
- Role
- HSTS
- XFrame Option / XSS
- CSRF Protection
- Security Auditor

# Intranet

"The only secure computer is one with no power, locked in a room, with no user."

<http://www.arnoldit.com/articles/10intranetSecAug2002.htm>



# Firewall



Securing ?  
No!

# Reverse Proxy



The big clean

# *Our Data*

# Our Data?



- PII
- Internal
- Confidential
- Restricted

*Let's Encrypt!*

# Encrypt the front-end

https & SSL : good but ...

- the keys
  - must be
    - protected
    - big enough
  - can be
    - broken
    - Stolen
- pick the right algo
  - Heard of Heartbleed, bash or POODLE ?
- clients
  - Trustworthy ?



# Encrypt the back-end

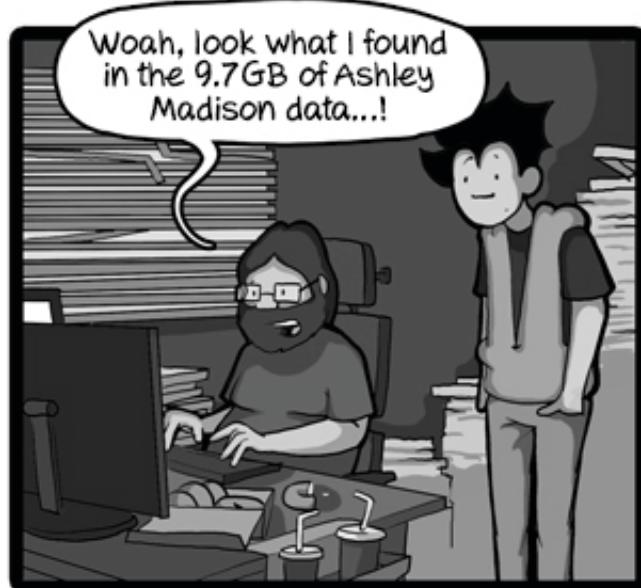
- Secure Mongo
  - Authentication
  - Role Based Access Control
    - <https://github.com/jhipster/generator-jhipster/issues/733>
  - Audit
- SSL with Mongo

Mohit Kumar (@unix\_root) posted a link to a news article about MongoDB security. The post includes a profile picture of Mohit Kumar, a gear icon, a 'Follow' button, and a link to the article.

40,000 unprotected MongoDB databases, 8 million telecommunication customer records exposed  
[thehackernews.com/2015/02/mongod...](https://thehackernews.com/2015/02/mongod...) |

# Encrypt at rest

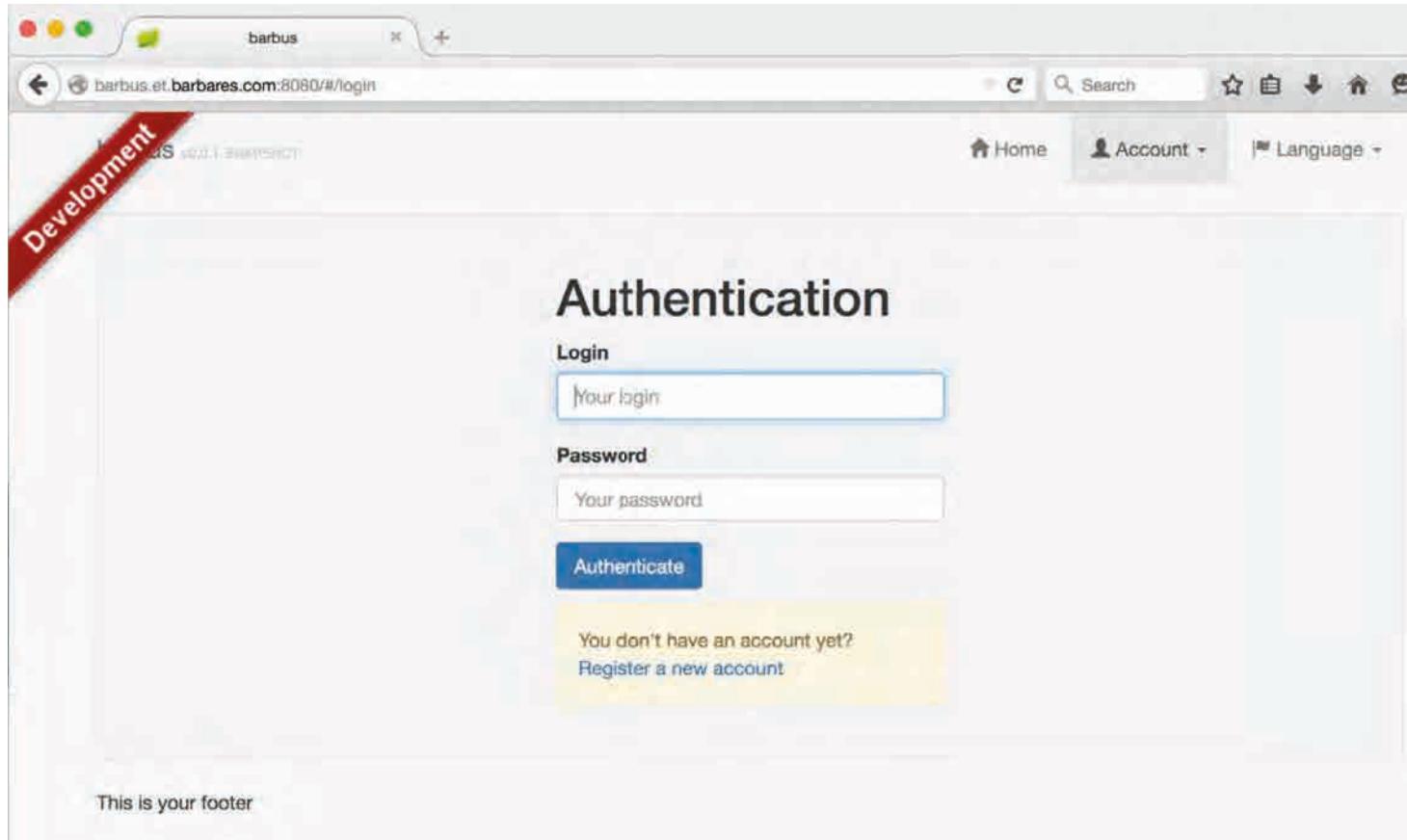
- Application level encryption
- Storage encryption



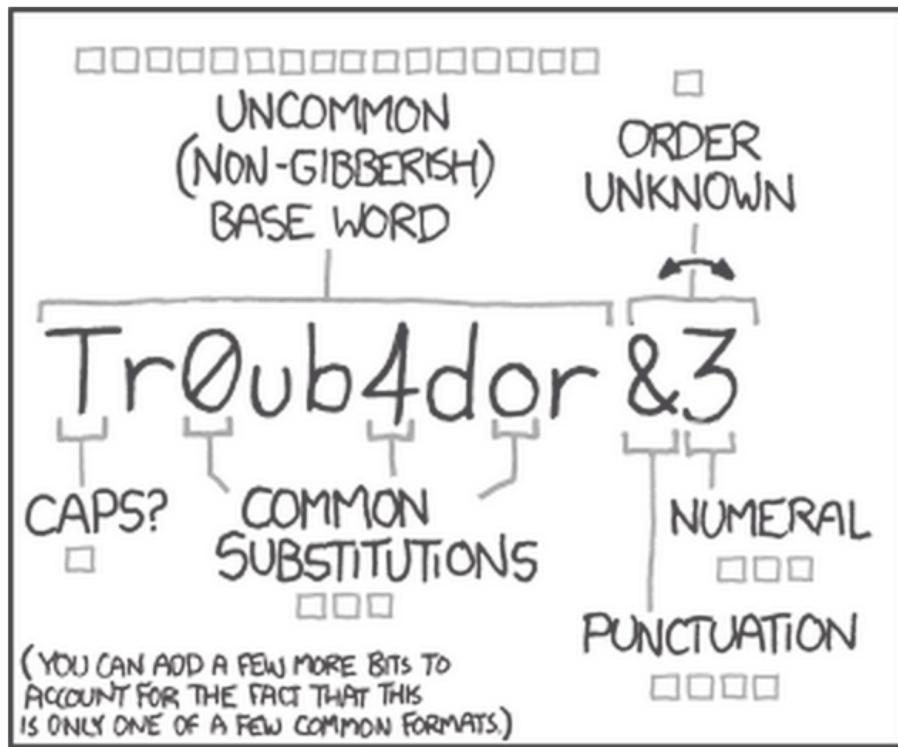
# *Auth*

## *Authentication &*

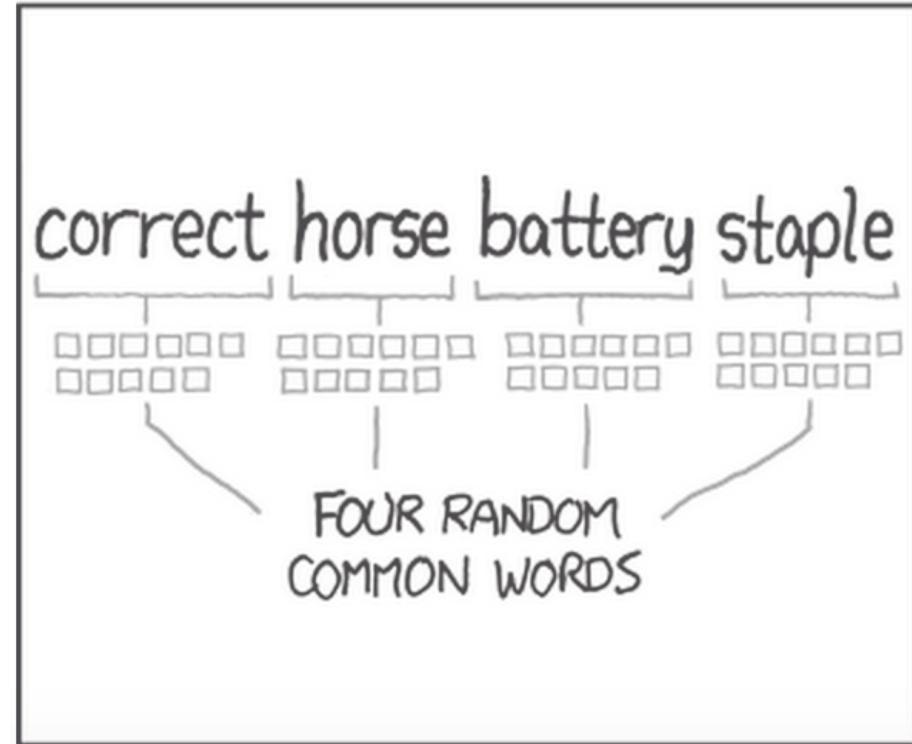
## *Authorization*



# Good ? passwords



$$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$$



$$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$$

<http://xkcd.com/936/>

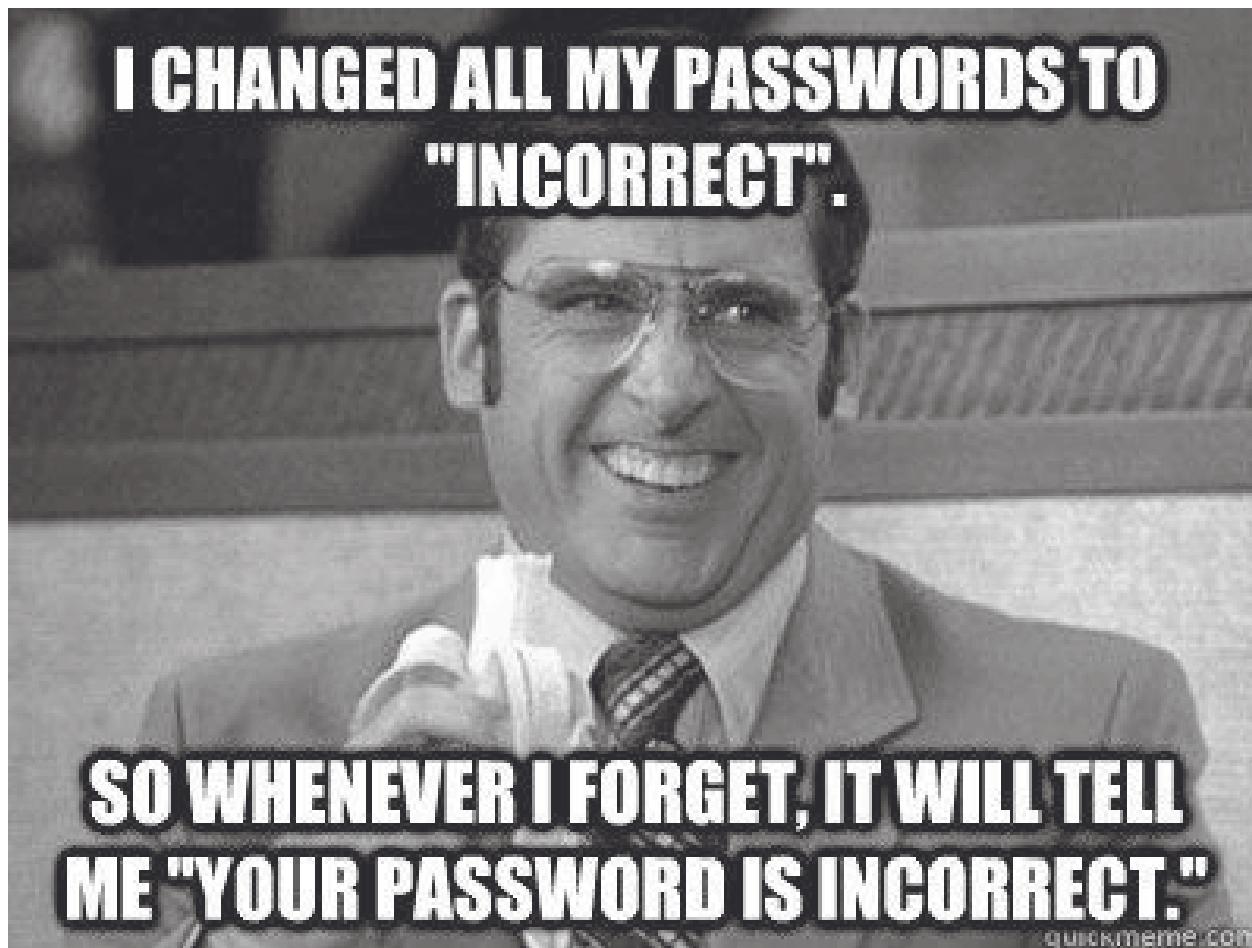
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.



**GLUI MGLW'I  
CTHULHU  
R'LYEH  
WGAH'NAGI  
FHTAGN**

<https://twitter.com/francoisledroff/status/643365403545219072>

# One ? password



# 156 ? passwords

 Files	1	 postman chrome extension
 Phone Numbers	2	 puk
 Serial Numbers	2	 rallydev
 Web Logins	156	 runkeeper
		 salesForce
		 salesforce poc renault
		 sap hx
		 sap-d2
		 sap-d4
		 sap-prod
		 sap-s2
		 sap-s4
		 scoleo.fr
		 sedif veoliaeau

# One dog



# Secrets ?



Norse follows

**Cytegic** @Cytegic · Mar 2

160,000 #Facebook pages are hacked a day #infosec #privacy  
[nyp.st/1aGb3bh](http://nyp.st/1aGb3bh) via @nypost



[View summary](#)



**IT Security News** @IT\_securitynews · Mar 17

Minimizing Damage From J.P. Morgan's Data Breach: How did a mega bank like J.P. Morgan get #hacked? It all... [goo.gl/fb/vxleNv](http://goo.gl/fb/vxleNv) #infosec



[View summary](#)



Le Gorafi and 1 other follow

**Alexandre Pouchard** @AlexPouchard · Feb 23

[View translation](#)

Pourquoi la #NSA et le #GCHQ ont volé des clés de chiffrement de cartes SIM  
[lemonde.fr/pixels/article...](http://lemonde.fr/pixels/article...) #Gemalto

# Two-Factor Authentication

*100% of security breaches  
implied stolen passwords in 2014*

<http://www.idtheftcenter.org/>



<http://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/>

# 2FA twofactorauth.org

Developer	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Atail	✓	✓	✓		✓	✓
Arbitrake				✗ TELL THEM TO SUPPORT 2FA		
atTech Media	✓				✓	✓
Balabit				✗ TELL THEM TO SUPPORT 2FA		
Bitticker				✗ TELL THEM TO SUPPORT 2FA		
Cloud9				✗ TELL THEM TO SUPPORT 2FA		
Code Climate	✓				✓	
Codewise				✗ TELL THEM TO SUPPORT 2FA		
Compositional	✓	✓			✓	
Docker				✗ TELL THEM TO SUPPORT 2FA		
Eshi	✓				✓	
Github	✓	✓			✓	

Finance	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
ASP				✗ TELL THEM TO SUPPORT 2FA		
Check Inc.				✗ TELL THEM TO SUPPORT 2FA		
Finra				✗ TELL THEM TO SUPPORT 2FA		
HelloWallet				✗ TELL THEM TO SUPPORT 2FA		
Intuit TurboTax				✗ TELL THEM TO SUPPORT 2FA		
Kiva				✗ TELL THEM TO SUPPORT 2FA		
LevelUp				✗ TELL THEM TO SUPPORT 2FA		
Mint				✗ TELL THEM TO SUPPORT 2FA		
Ticketmaster	✓				✓	
Quicken Online				✗ TELL THEM TO SUPPORT 2FA		

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Hot Mail				✗ TELL THEM TO SUPPORT 2FA		
FastMail	✓	✓		✓	✓	✓
Gmail	✓	✓	✓		✓	✓

Health	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
3bandMe				✗ TELL THEM TO SUPPORT 2FA		
anthonio		✓				✓
Drug.com				✗ IN PROGRESS		
HHS				✗ TELL THEM TO SUPPORT 2FA		
Healthcare.gov				✗ TELL THEM TO SUPPORT 2FA		
HealthVault (Microsoft Account)	✓	✓				✓
myfitnesspal				✗ TELL THEM TO SUPPORT 2FA		
WebMD				✗ TELL THEM TO SUPPORT 2FA		
Wink				✗ TELL THEM TO SUPPORT 2FA		

Payments	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Amazon Payments				✗ TELL THEM TO SUPPORT 2FA		
BuyCraft	✗	✓	✓			✓
Byndia				✗ TELL THEM TO SUPPORT 2FA		
GoCardless				✗ TELL THEM TO SUPPORT 2FA		
Google Wallet	✓	✓	✓		✓	✓
Lilith & Co				✗ TELL THEM TO SUPPORT 2FA		
Paytometer				✗ THANK THEM FOR WORKING ON 2FA		
PayPal	✗	✓	✓			✓
Skull	✓				✓	
Square				✗ TELL THEM TO SUPPORT 2FA		

Social	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
about.me				✗ TELL THEM TO SUPPORT 2FA		
App.net	✓					✓
Billy	✗	✓				
Buffer	✓	✓				✓
Facebook	✓	✓				✓
Google+	✓	✓	✓		✓	✓

# Our Solution

Avoid the password/identity business :

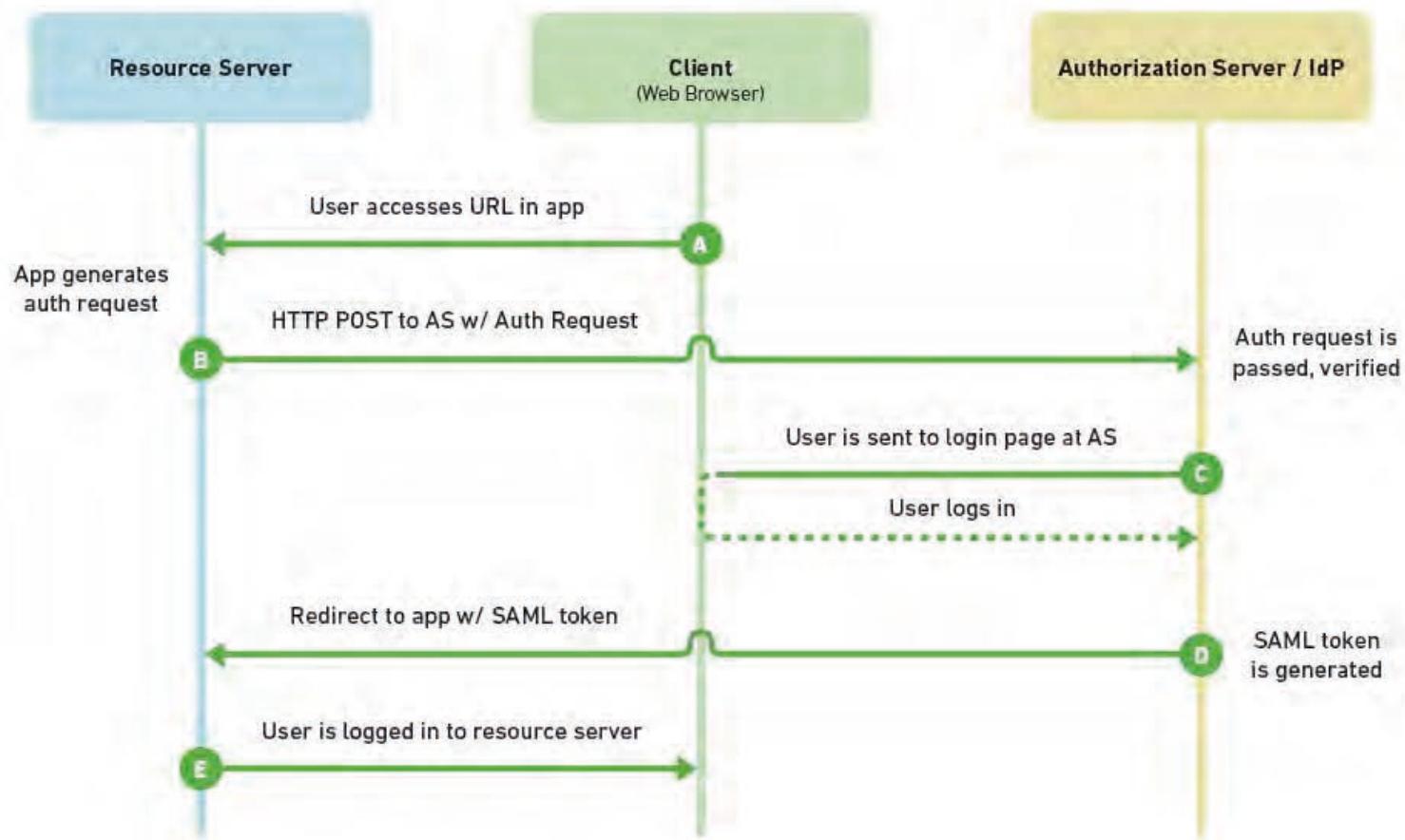
- Be a simple service provider
- Integrate with a trusted & trustworthy identity provider (IdP)
  - Enforcing two-factor authentication

# SAML

- SAML
  - un standard
    - SSO du navigateur
    - <http://www.ssocircle.com>
    - Juste un standard

# SAML

## SAML 2.0 Flow



# SAML & JHipster

- Spring Security Support
- Not in JHipster
  - Yet #695

# Click?





Log on to this computer

Username

Password



Use NMAS for Windows Logon

Log on to: WIN-CLSSKORVK1B

[Log on to another domain](#)

[Novell Logon](#)

Switch User

Windows 7 Professional





Francois Le Droff [Sign Out](#)



### Sign In with Okta Verify

Your computer or mobile device has not been verified, or a previous verification has expired.

Push to device

or

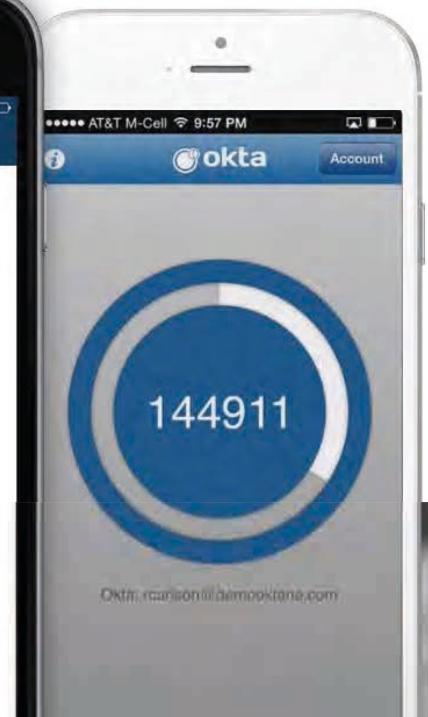
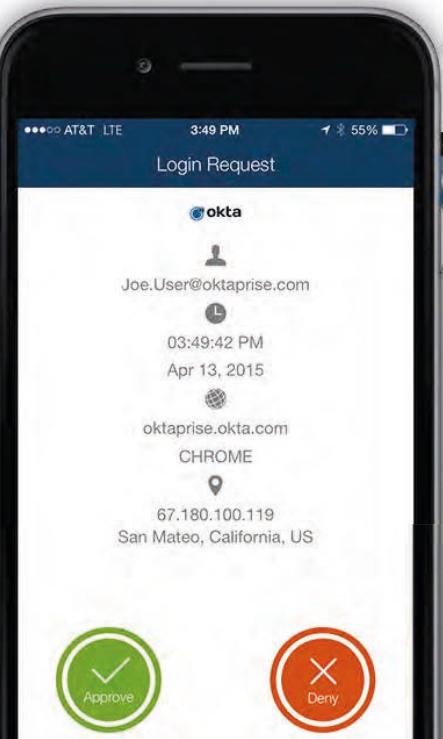
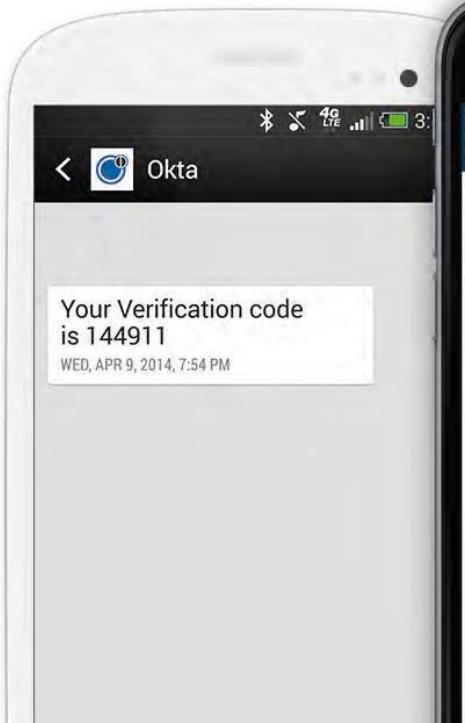


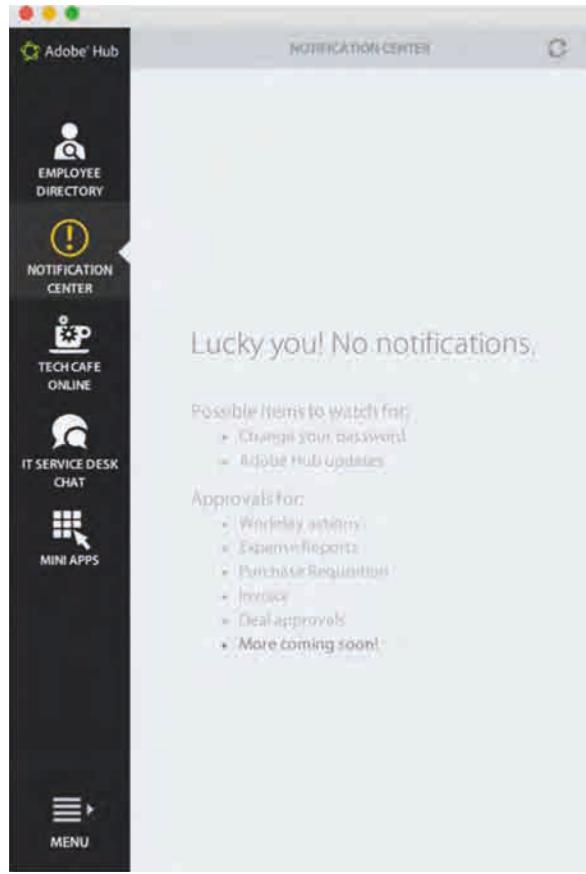
Enter code

Remember device

Verify with Okta Verify A small blue dropdown arrow icon.

Powered by Okta







**Michael Neale**  
@michaelneale



[Follow](#)

1. App requires 2FA login. 2. get phone from pants 3. Distracted by 100s of notifications on it 3. Back to computer. Repeat.



**Norse**  
@NorseCorp



[Following](#)

Executive Priorities: Balancing Security and Usability [bit.ly/1GNBN3x](http://bit.ly/1GNBN3x) via @Wh1t3Rabbit  
#infosec #security



# + OAuth2

- OAuth v2
  - Authorize data access to an API
  - Create a bond to trust between an application and a service provider
- OAuth2 threat model:
  - <http://tools.ietf.org/html/rfc6819>

A screenshot of a web browser window titled "Barbus & Barbares". The address bar shows the URL <https://barbus.et.barbares.com/index>. The main content area displays the heading "OAuth Tokens for [ledroff]" and a table with three columns: ClientId, User ID, and Scope. The table row shows "ledroff\_hub\_oauth\_client" in the ClientId column, "ledroff@adobe.com" in the User ID column, and "write read" in the Scope column. A blue "Revoke" button is located in the bottom right corner of the table row.

ClientId	User ID	Scope
ledroff_hub_oauth_client	ledroff@adobe.com	write read

Revoke

# Other options

- OAuth 1.0
- Radius
- X509 auth
- Combinations of the above
  - including Kerberos, SAML & OAuth 2.0

# *Continuous Integration & Secret Management*

# Secret Segregation

The screenshot shows a GitHub search interface with the query 'secret'. The results are displayed in three sections corresponding to different files:

- src/main/webapp/scripts/components/auth/provider/oauth.oauth2.service.js**:  
A JavaScript code snippet containing:

```
var data = "username=" + credentials.username + "&password=" + credentials.password + "&grant_type=password&scope=read%20write&client_secret=mySecretOAuthSecret&client_id=barbusapp";
```
- src/main/resources/config/application.yml**:  
A YAML configuration snippet containing:

```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: Sa57975ee65e8bda3dca253cd835dff90883a19d

messageSource:
  cacheSeconds: 1

authentication:
  auth:
    clientid: barbusapp
    secret: my SecretOAuthSecret
```
- src/test/resources/config/application.yml**:  
A YAML configuration snippet containing:

```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: Sa57975ee65e8bda3dca253cd835dff90883a19d
```

<https://github.com/francoisledroff/devoxx2015/search?utf8=%E2%9C%93&q=secret>

[https://www.google.ie/search?q=%22.git%22+intitle:%22Index+of%22&gws\\_rd=cr,ssl&ei=hTMRVfHtONbXapDogrgG](https://www.google.ie/search?q=%22.git%22+intitle:%22Index+of%22&gws_rd=cr,ssl&ei=hTMRVfHtONbXapDogrgG)

# Secret Segregation



**Marco Abis**

@capotribu



 Follow

My \$2375 Amazon EC2 Mistake  
[bit.ly/13RfcFI](http://bit.ly/13RfcFI) < "my key had been spotted by  
a bot that continually searches GitHub for  
API keys"

<https://twitter.com/capotribu/status/550079317368381441>

<http://www.devfactor.net/2014/12/30/2375-amazon-mistake/>

# Managing Secrets



Overheard By

@jtimberman



Follow

Managing secrets: still the hardest problem in operations.



RETWEETS

2

FAVORITES

8



8:07 PM - 18 Feb 2015



Reply to @jtimberman



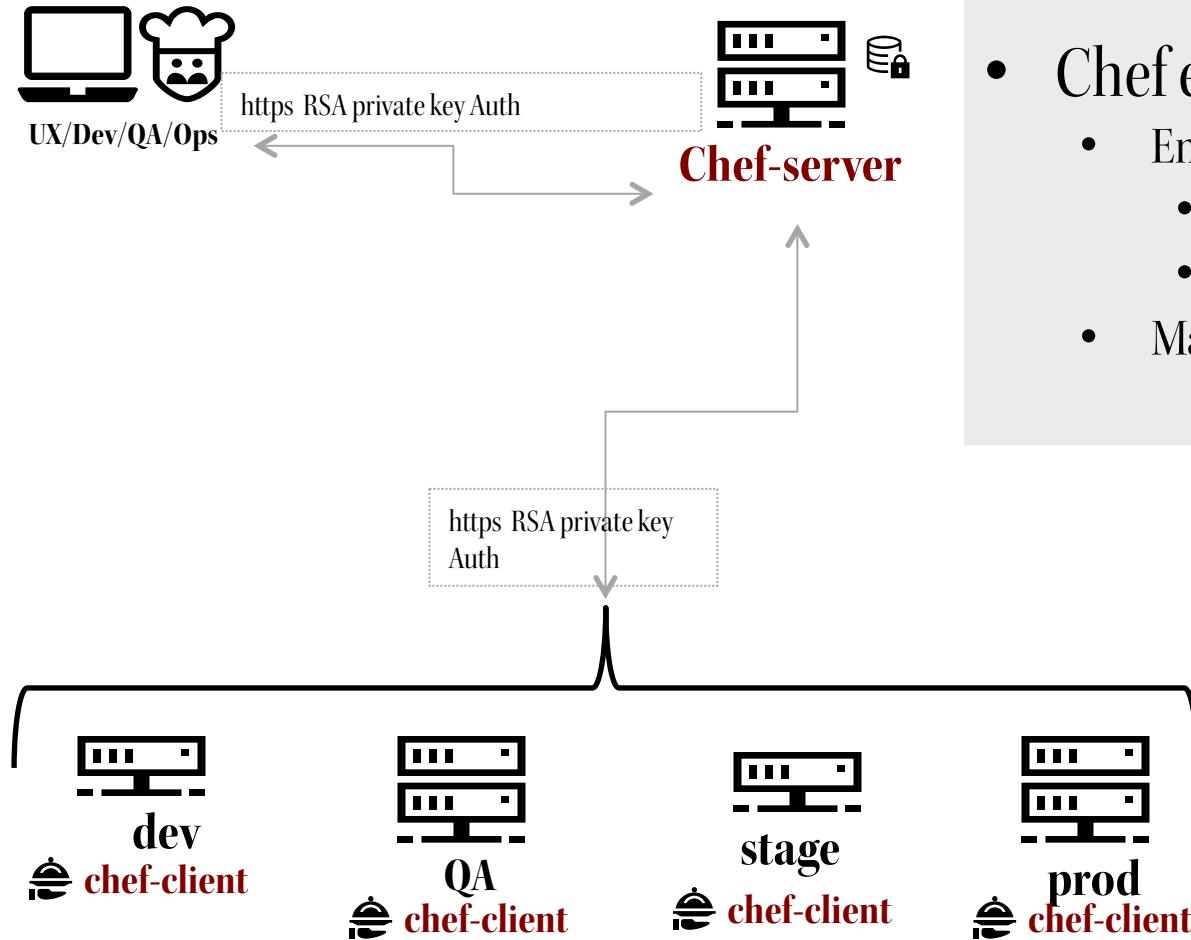
DiggityBiscuits @grubernaut · Feb 18

@jtimberman doing it well is the biggest secret



<https://twitter.com/jtimberman/status/568124542553423872>

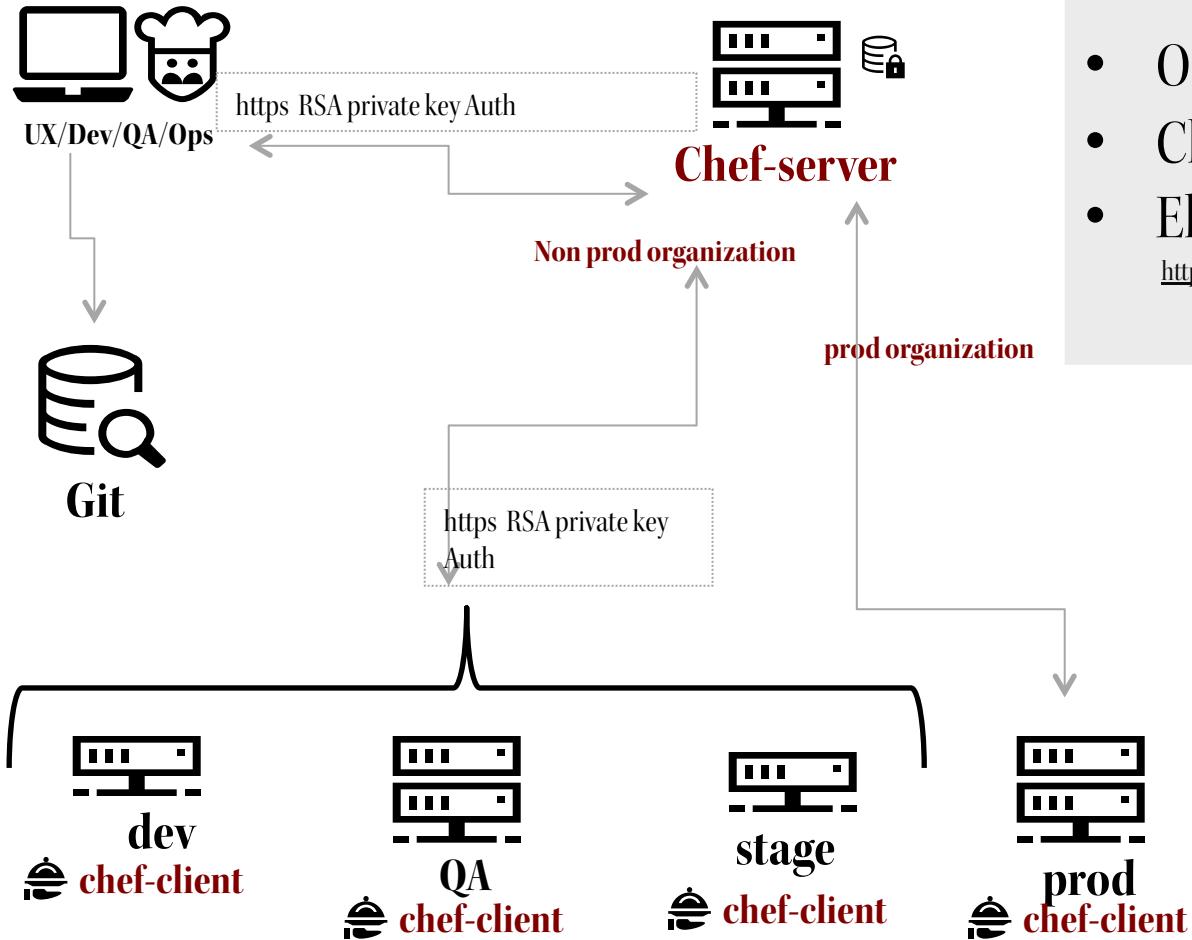
# Chef-vault



- Chef encrypted data bags
  - Encrypted for
    - admin users
    - whitelisted nodes
  - Managed by **chef-vault ruby gem**



# Chef-vault



- Org Segregation
- Chef Server Security
- Elasticity

<https://wiki.jenkins-ci.org/display/JENKINS/chef-identity+plugin>



# Securing Jenkins

- Authentication
  - SAML is an option
- Cloudbees
- Automate
  - Short live*



Jean-Laurent Morlhon

@morlhon

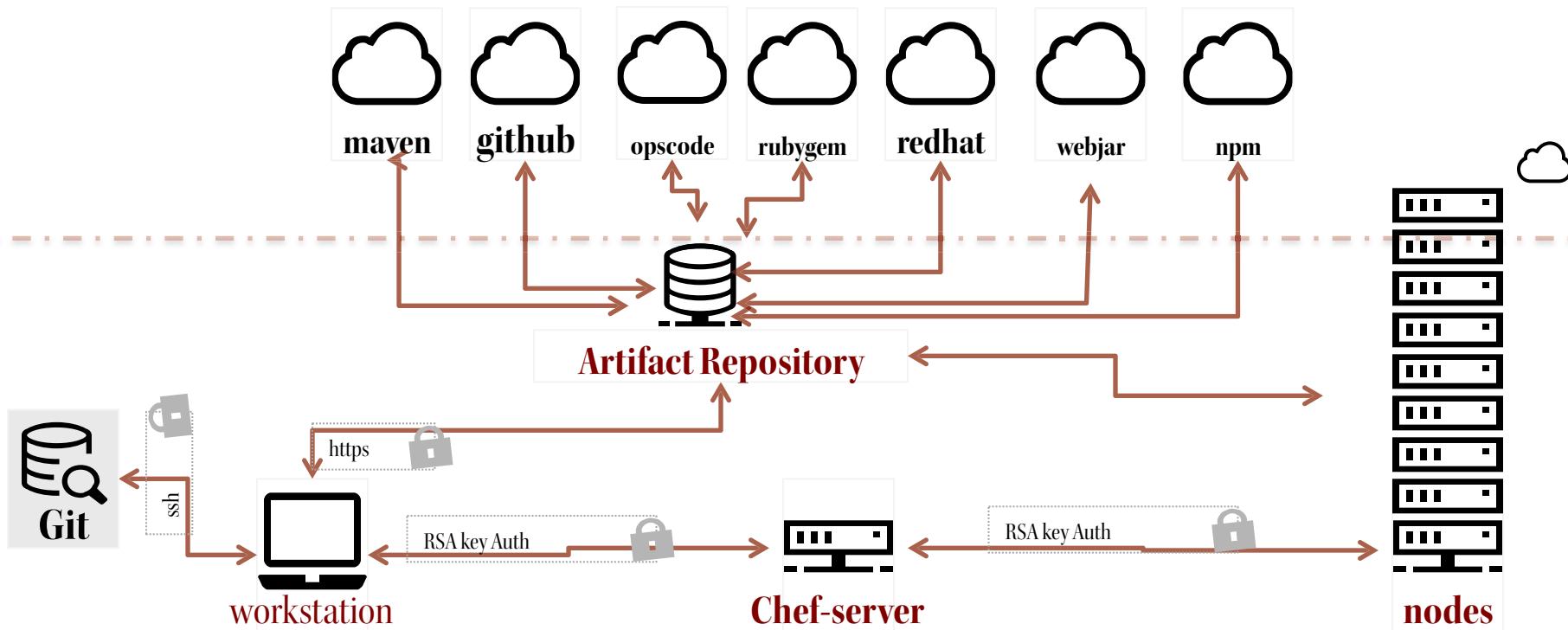


Following

A must-read : [@paulgreg](#): interesting slide on security of your webapp "DevOoops" by [@carnalOwnage](#) #devops #hacking [slideshare.net/chrisgates/las...](https://slideshare.net/chrisgates/las...)"

<https://twitter.com/morlhon/status/554899543150850048>

# Secure Dependency Management



A black and white photograph of a vast, calm body of water under a dramatic, cloudy sky. The clouds are thick and white, creating a sense of depth and texture. The horizon line is visible in the distance, where the water meets the sky.

*In the Cloud ?*

# There is NO CLOUD, just



## other people's computers





**francoisledroff**

@francoisledroff

Crazy number: one guy for 25000 servers

**Antony Slumbers** @antonyslumbers

Facebook has one technician per 25,000 servers in a data centre. That, my friends is the future of work. [hbr.org/2015/06/an-ins...](http://hbr.org/2015/06/an-ins...)

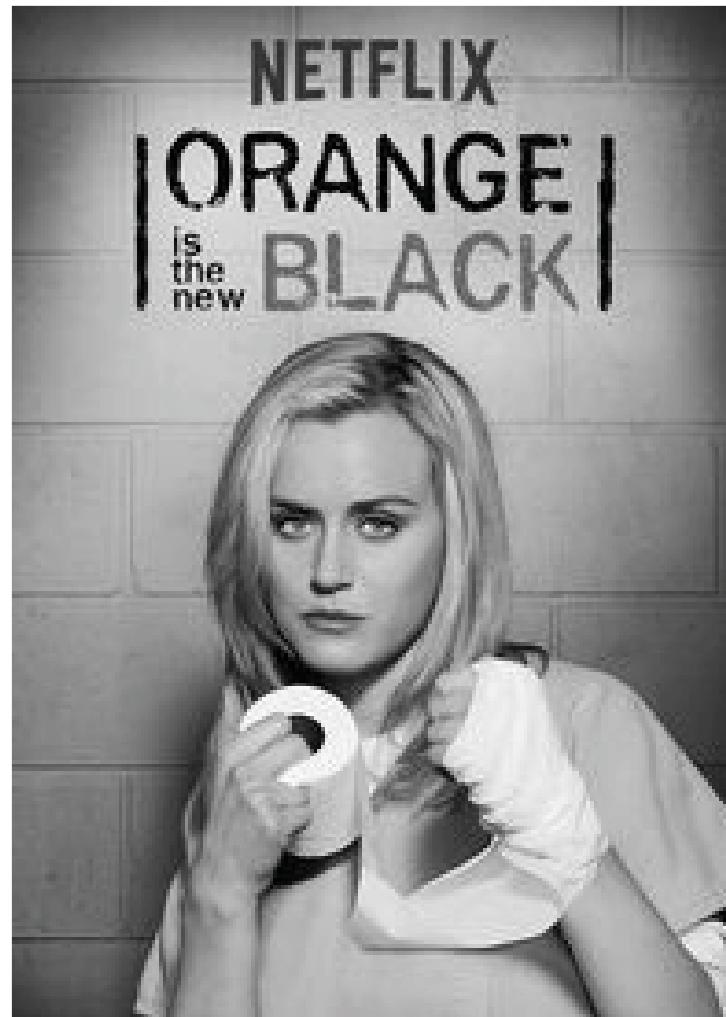
RETWEET

1



10:26 AM - 15 Jun 2015





*Ready to be hacked?*

# The House is on fire



- Smoke detectors
  - HSM
  - IDS
- Fire Doors
  - SELinux
  - SecurityManager

# Firefighters ?



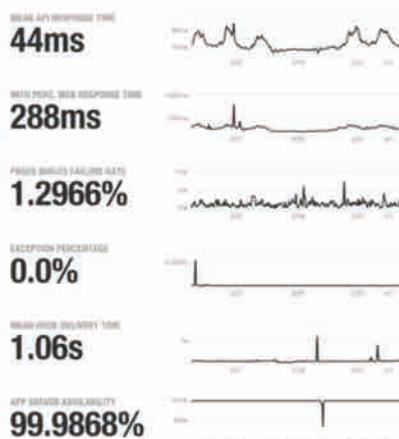
**GitHub Status** @githubstatus · Mar 26  
We are currently experiencing some minor service outages.

Olivier Bazoud and 8 others follow

**GitHub Status** @githubstatus · Mar 27  
We are investigating increased error rates as an incoming DDoS amplifies their attack.

Rewritten 483 times.

**GitHub Status** @githubstatus · 13h  
After 113 hours of sustained DDoS attacks our defenses are holding. We will keep our status at yellow until the threat has subsided.



*What to take away*

# Take away

- Security is your responsibility
- Think about it, Threat model
- You'll never be safe
  - nor your data
  - Encrypt!
- Manage your secrets
- Switch 2FA/strong authentication on

# Take away

- UX is not an excuse for a lack of security
- Security is not an excuse for a bad UX
- Don't forget continuous integration
- Treat your servers like cattle
- Be ready to firefight

# Questions ? Really?

It was clear, wasn't it ?



**@francoisledroff**



**@rpelisse**