



*Java
&
Security*

Romain



@rpelisse



Francois

5



@francoisledroff





Security Audit ?

Continuous Security



SEC-U.R.-IT-Y



Threat Modeling

Identify the threats

STRIDE

- **S**poofing Identity
- **T**ampering with Data
- **R**epudiation
- **I**nformation Disclosure
- **D**enial of Service
- **E**levation of Privilege

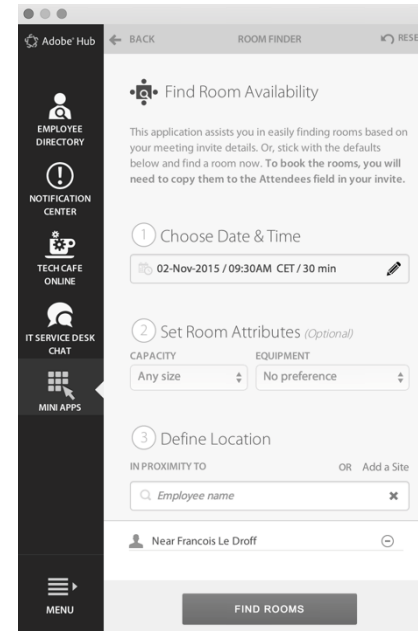
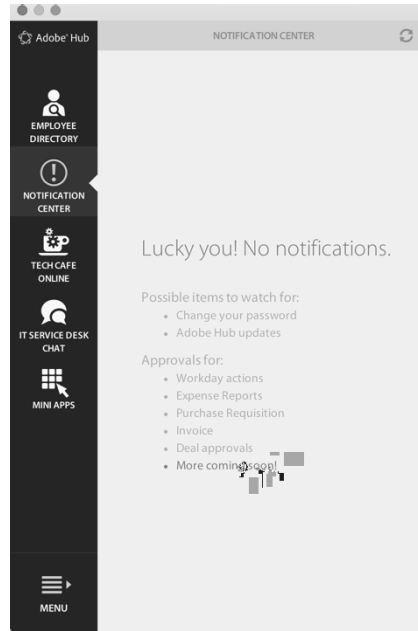
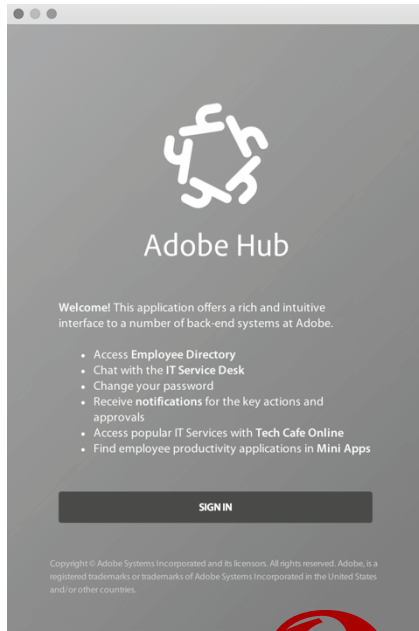
Assess the risk

DREAD

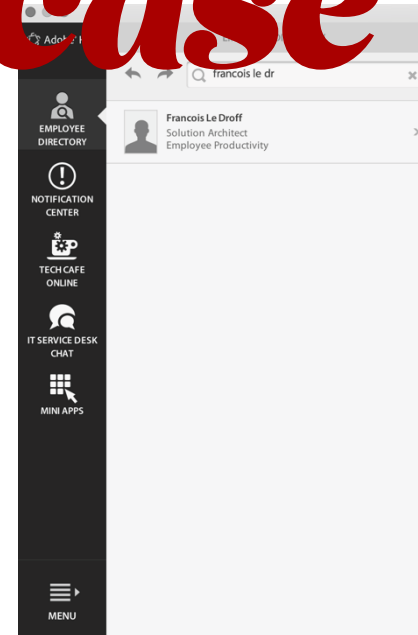
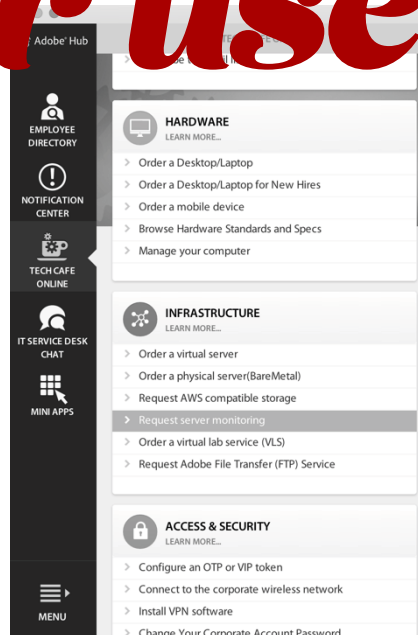
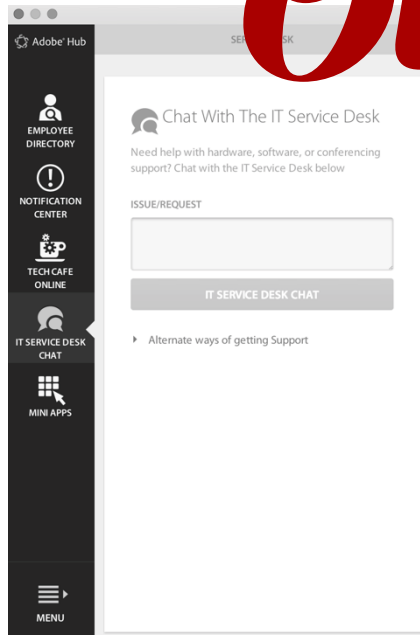
- *D*amage Potential
- *R*eproducibility
- *E*xploitability
- *A*ffected Users
- *D*iscoverability

A black and white photograph of a beach scene. In the foreground on the right, a young child with curly hair, seen from the back, wears striped shorts and holds a bowl of beach toys. In the middle ground, two people are swimming in the water. In the background, a large cable-stayed bridge with multiple arches spans across the water. The sky is filled with clouds.

Deep Dive
through our sample use case



Our use case



jHipster



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

Yo



```
~/workspace/github/devoxx2015 13:51:19
```

```
$ yo jhipster
```

```
███ J H I P S T E R S T A C K ██████████  
██████████  
██████████  
███ J A V A D E V S ██████████
```

Welcome to the JHipster Generator

```
? May JHipster anonymously report usage statistics to improve the tool  
? (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?  
    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



Encrypt at rest

- Application level encryption
- Storage encryption



Auth
Authentication &
Authorization

barbus

barbus.et.barbares.com:8080/#/login

Search

Home Account Language

Authentication

Login

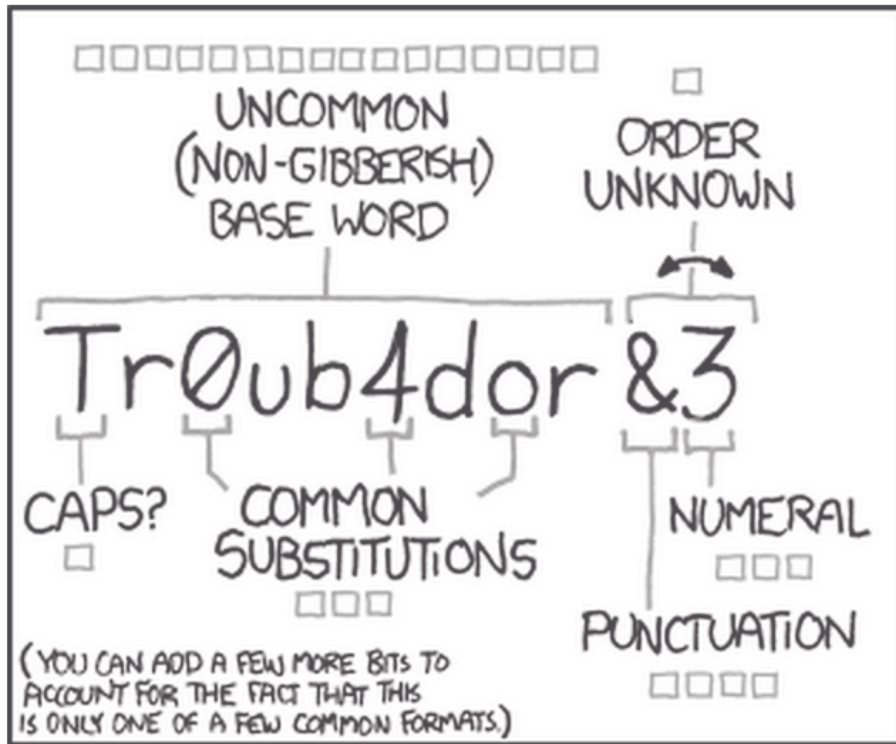
Password

Authenticate

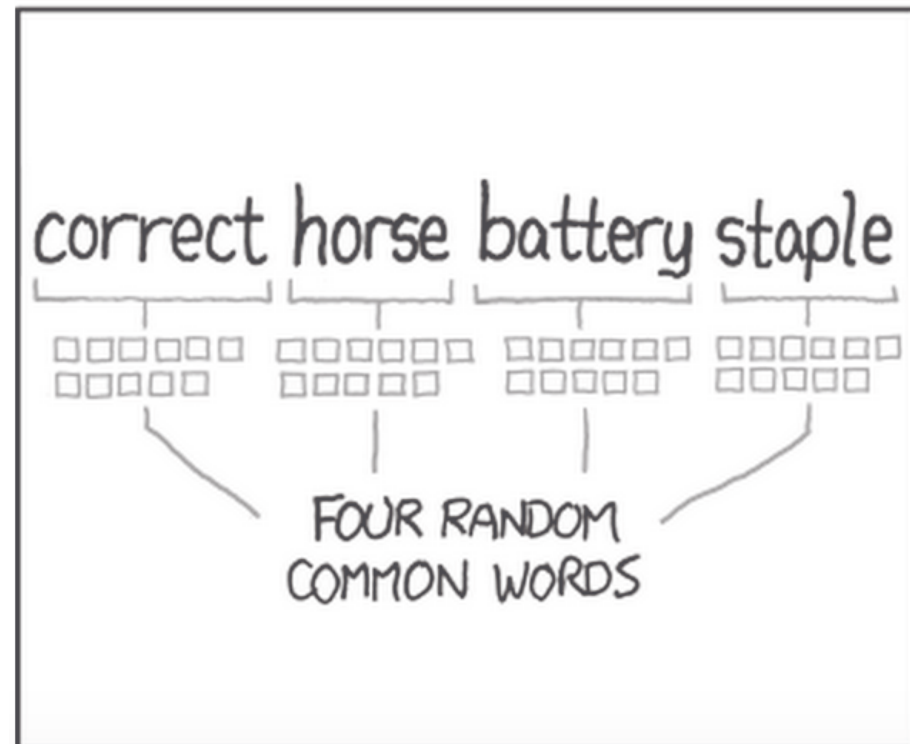
You don't have an account yet?
[Register a new account](#)

This is your footer

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/>

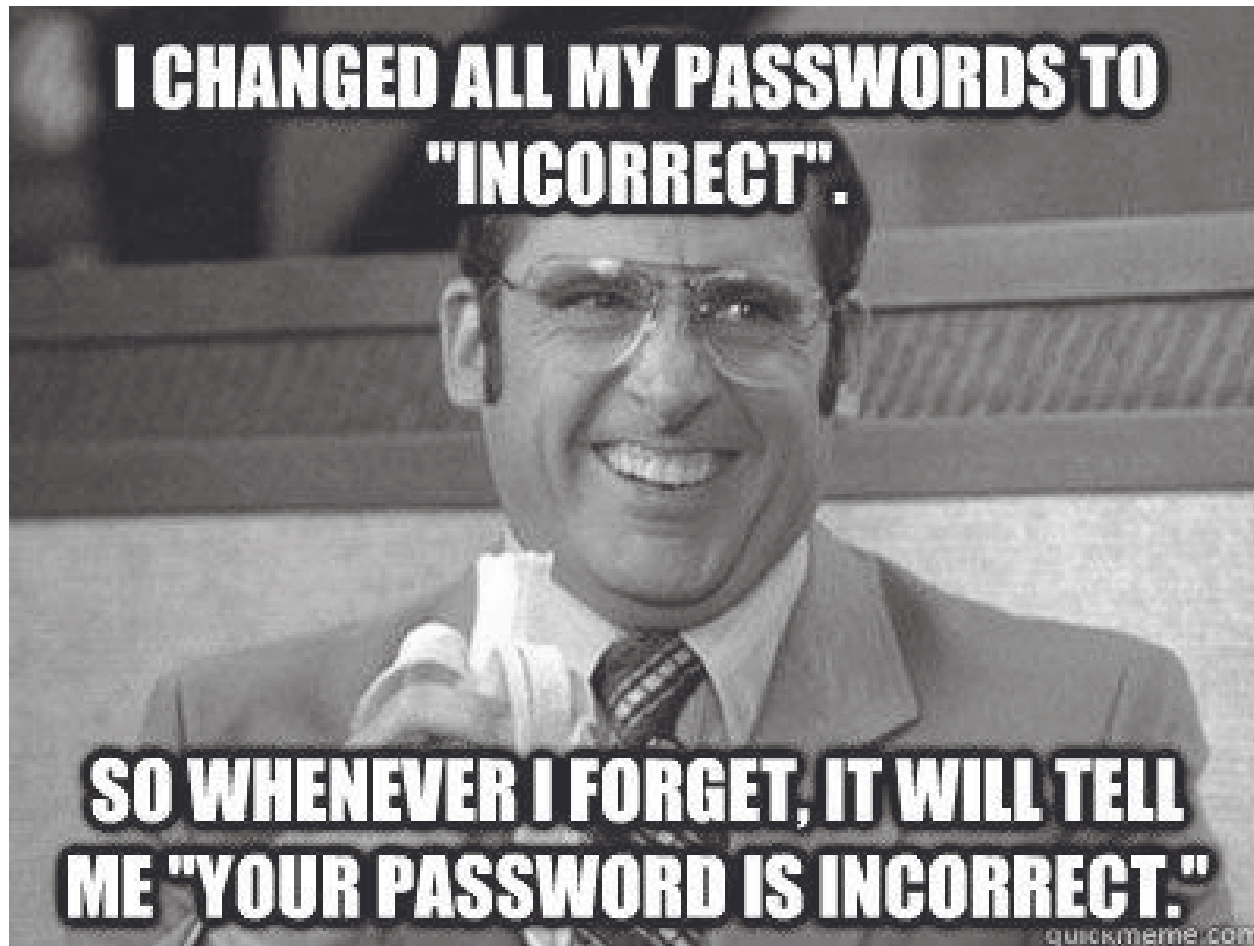
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.





















GLUI MGLW'
CTHULHU
R'LYEH
NGAH'NAGL
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 venliaeau

One dog



Secrets ?



Norse follows



Cytegic @Cytegic · Mar 2

160,000 **#Facebook** pages are **hacked** a day **#infosec** **#privacy**
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 **#infosec**



[View summary](#)



Le Gorafi and 1 other follow



Alexandre Pouchard @AlexPouchard · Feb 23

Pourquoi la **#NSA** et le **#GCHQ** ont volé des clés de chiffrement de cartes SIM
lemonde.fr/pixels/article... **#Gemalto**

[View translation](#)

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
Ahal		✓	✓		✓	✓
Alibaba			TELL THEM TO SUPPORT 2FA			
aTech Media					✓	✓
Balsamiq			TELL THEM TO SUPPORT 2FA			
Bitbucket			TELL THEM TO SUPPORT 2FA			
Cloud9			TELL THEM TO SUPPORT 2FA			
Cofe Climate						✓
Codeskip			TELL THEM TO SUPPORT 2FA			
CompuLink		✓				✓
Docker			TELL THEM TO SUPPORT 2FA			
Esri						✓
GitHub		✓				✓

Finance	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
ADP			TELL THEM TO SUPPORT 2FA			
Check Inc			TELL THEM TO SUPPORT 2FA			
FreeAgent			TELL THEM TO SUPPORT 2FA			
HelloWaker			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			
Prokessmitt						✓
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
23andMe			TELL THEM TO SUPPORT 2FA			
23andMe						✓
Drugs.com			THANK THEM FOR WORKING ON 2FA			
Drugs.com			IN PROGRESS!			
FitBit			TELL THEM TO SUPPORT 2FA			
Healthcare.gov			TELL THEM TO SUPPORT 2FA			
HealthVault (with Microsoft Account)		✓				✓
myFitnessPal			TELL THEM TO SUPPORT 2FA			
WebMD			TELL THEM TO SUPPORT 2FA			
Wotif			TELL THEM TO SUPPORT 2FA			

Payments	Docs	SMS	Phone Call	Email	Hardware Token	Software Implementation
Amazon Payments			TELL THEM TO SUPPORT 2FA			
Boycraft		✓				✓
Dynka			TELL THEM TO SUPPORT 2FA			
GoCardless			TELL THEM TO SUPPORT 2FA			
Google Wallet		✓	✓		✓	✓
Little & Co			TELL THEM TO SUPPORT 2FA			
Paycom			THANK THEM FOR WORKING ON 2FA			
Paycom			IN PROGRESS!			
PayPal		✓				✓
Skrill					✓	
Squares			TELL THEM TO SUPPORT 2FA			

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

Our Solution

Avoid the password/identity business :

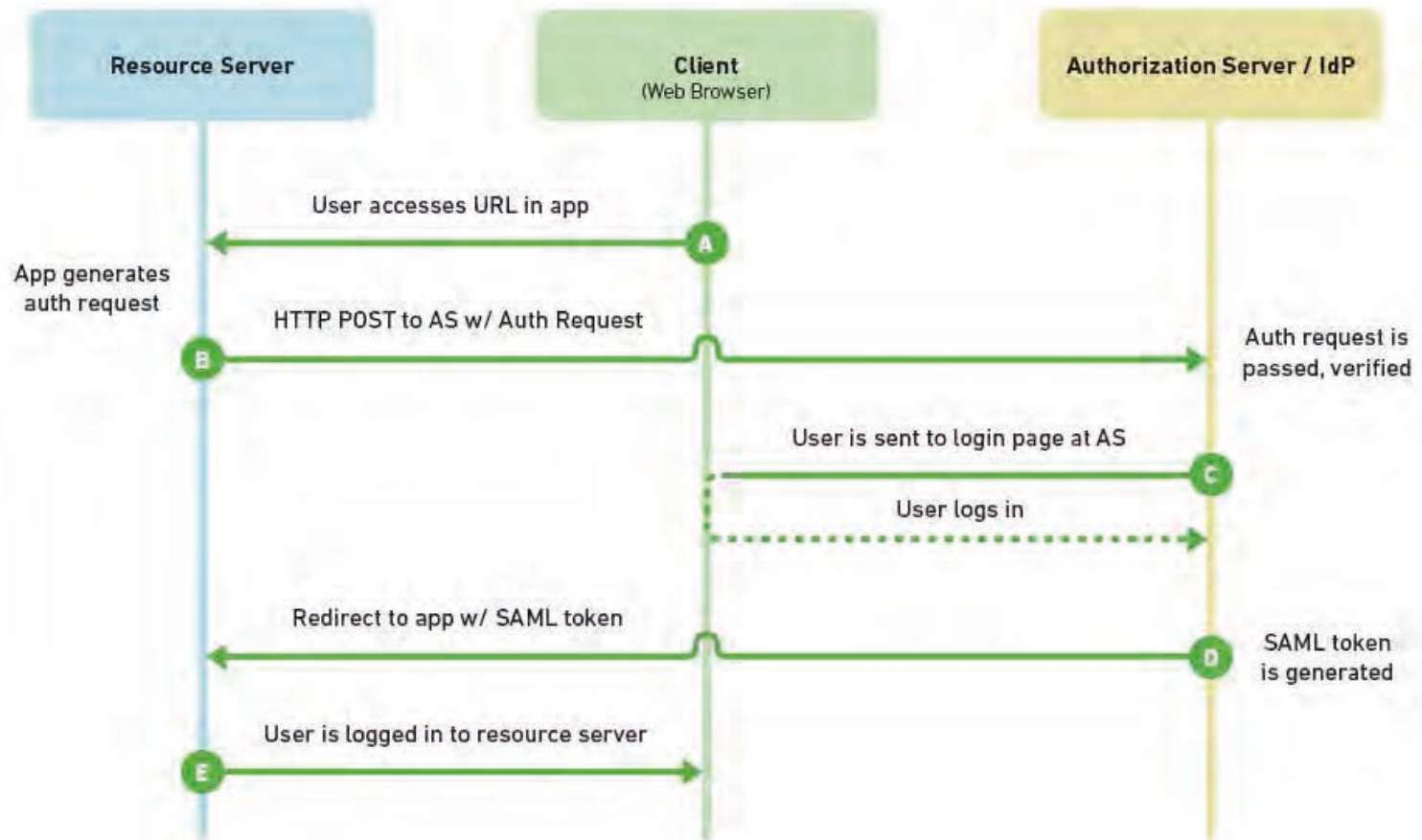
- Be a simple service provider
- Integrate with a trusted & trustworthy identity provider (IdP)
 - Enforcing two-factor authentication

SAML

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

SAML

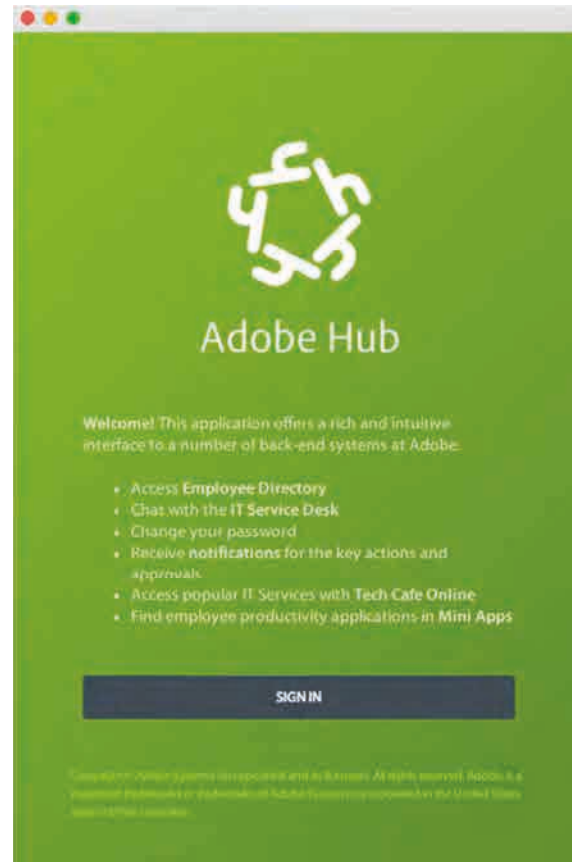
SAML 2.0 Flow



SAML & JHipster

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

Click?





Log on to this computer

Username

Password



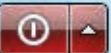
Use NMAP for Windows Logon

Log on to: WIN-CLSSKORVKLB

[Log on to another domain](#)

[Novell Logon](#)

Switch User





Adobe Hub

Welcome! This application offers a rich and intuitive interface to a number of back-end systems at Adobe.

- Access **Employee Directory**
- Chat with the **IT Service Desk**
- Change your password
- Receive **notifications** for the key actions and approvals.
- Access popular IT Services with **Tech Cafe Online**
- Find employee productivity applications in **Mini Apps**

SIGN IN

© 2015 Adobe Systems Incorporated and its licensors. All rights reserved. Adobe is a registered trademark of Adobe Systems Incorporated in the United States and/or other countries.



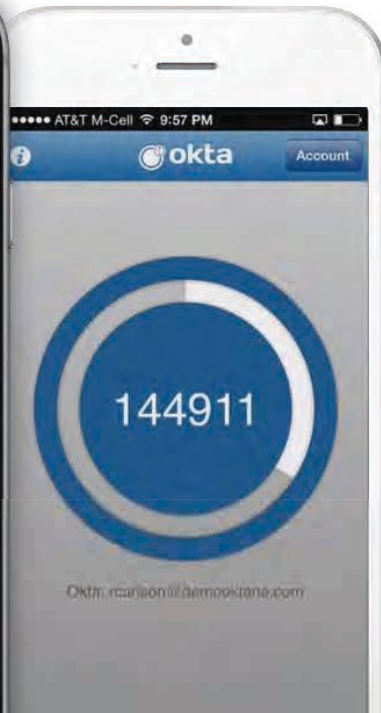
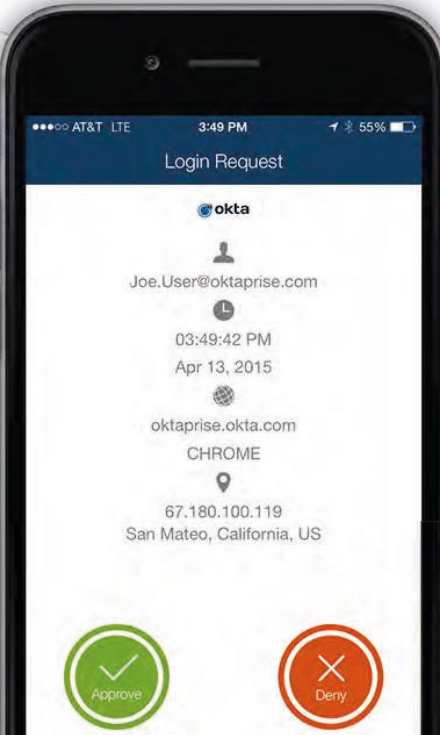
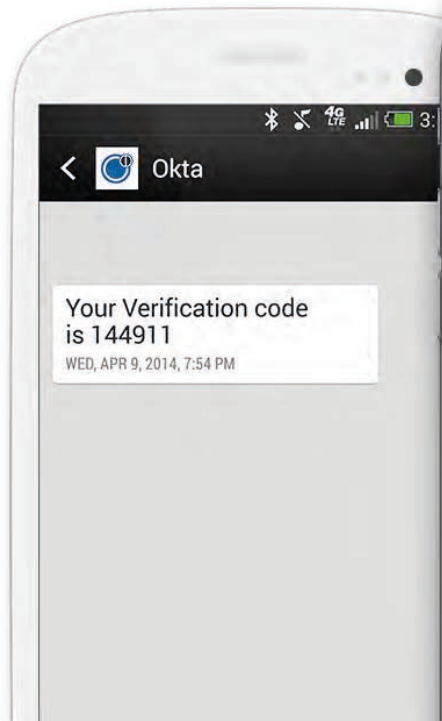
Sign In with Okta Verify

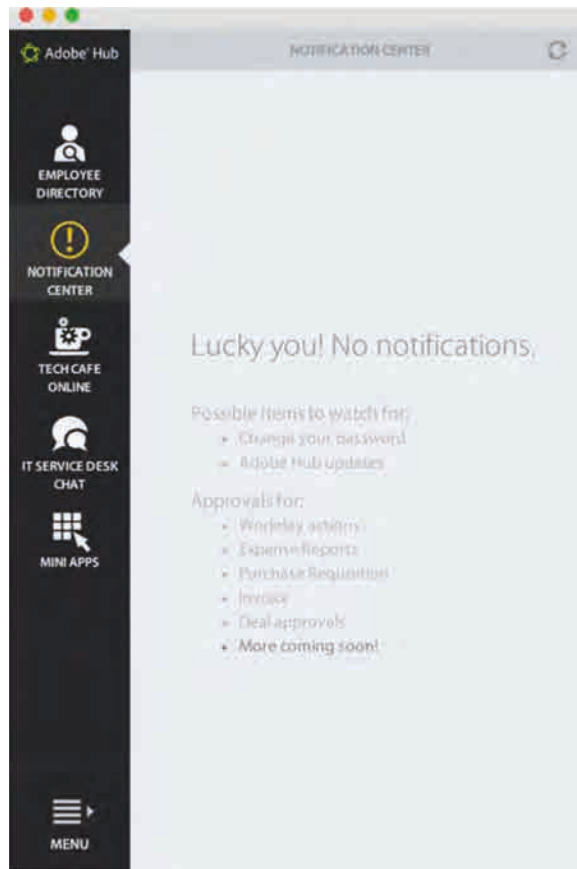
Your computer or mobile device has not been verified, or a previous verification has expired.

Push to device or  Enter code

Remember device









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 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>

Barbus & Barbares

https://barbus.et.barbares.com/index. Search

Barbus & Barbares devoxx 2015

oAuth Tokens for [ledroff]

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 for the repository 'francoisledroff / devoxx2015'. The search query is 'secret'. The results are as follows:

- src/main/webapp/scripts/components/auth/provider/auth.oauth2.service.js** (JavaScript):
Showing the top match. Last indexed 2 minutes ago.
Line 7: `var data = "username=" + credentials.username + "&password="`
Line 8: `+ credentials.password + "&grant_type=password&scope=read%20write&" +`
Line 9: `"client_secret=mySecretOAuthSecret&client_id=barbusapp";`
Line 10: `return $http.post('/oauth/token', data, {`
- src/main/resources/config/application.yml** (YAML):
Showing the top three matches. Last indexed 2 minutes ago.
Line 8: `# security configuration (this key should be unique for your application, and kept secret)`
Line 9: `hipster.security.randomize.key: 5a57975ee65e8bda3dca253cd835dff90883a19d`
Line 27: `messageSource:`
Line 28: `cacheSeconds: 1`
Line 29: `authentication:`
Line 30: `auth:`
Line 31: `clientId: barbusapp`
Line 32: `secret: mySecretOAuthSecret`
- src/test/resources/config/application.yml** (YAML):
Showing the top match. Last indexed 2 minutes ago.
Line 6: `# security configuration (this key should be unique for your application, and kept secret)`
Line 7: `hipster.security.randomize.key: 5a57975ee65e8bda3dca253cd835dff90883a19d`

<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

Secret Segregation



Marco Abis
@capotribu



 Follow

My \$2375 Amazon EC2 Mistake
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



The image shows a screenshot of a Twitter post. At the top, the user's profile is visible: a circular profile picture of a man, the name "Overheard By", and the handle "@jtimberman". To the right of the profile is a gear icon for settings and a "Follow" button. The main text of the tweet reads "Managing secrets: still the hardest problem in operations." Below the text are icons for retweeting, replying, favoriting, and a menu. A statistics bar shows "RETWEETS 2" and "FAVORITES 8", followed by a row of profile pictures of users who interacted with the tweet. The timestamp "8:07 PM - 18 Feb 2015" is at the bottom of the tweet. Below the tweet is a reply box with a profile picture of the user and the text "Reply to @jtimberman". Below the reply box is another tweet from "DiggityBiscuits @grubernaut · Feb 18" which says "@jtimberman doing it well is the biggest secret". This second tweet has one retweet and a star icon.

Overheard By @jtimberman

Managing secrets: still the hardest problem in operations.

RETWEETS 2 FAVORITES 8

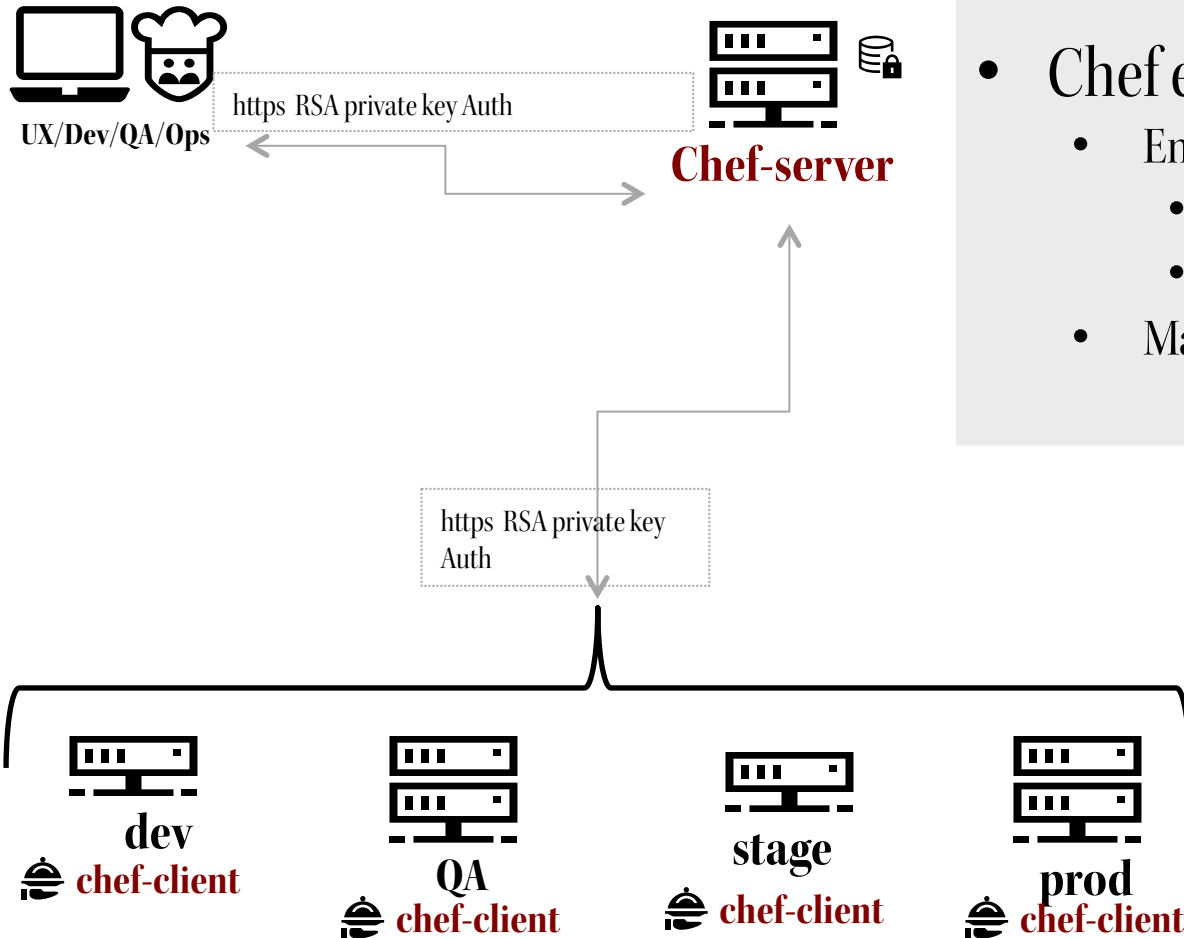
8:07 PM - 18 Feb 2015

Reply to @jtimberman

DiggityBiscuits @grubernaut · Feb 18
@jtimberman doing it well is the biggest secret

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

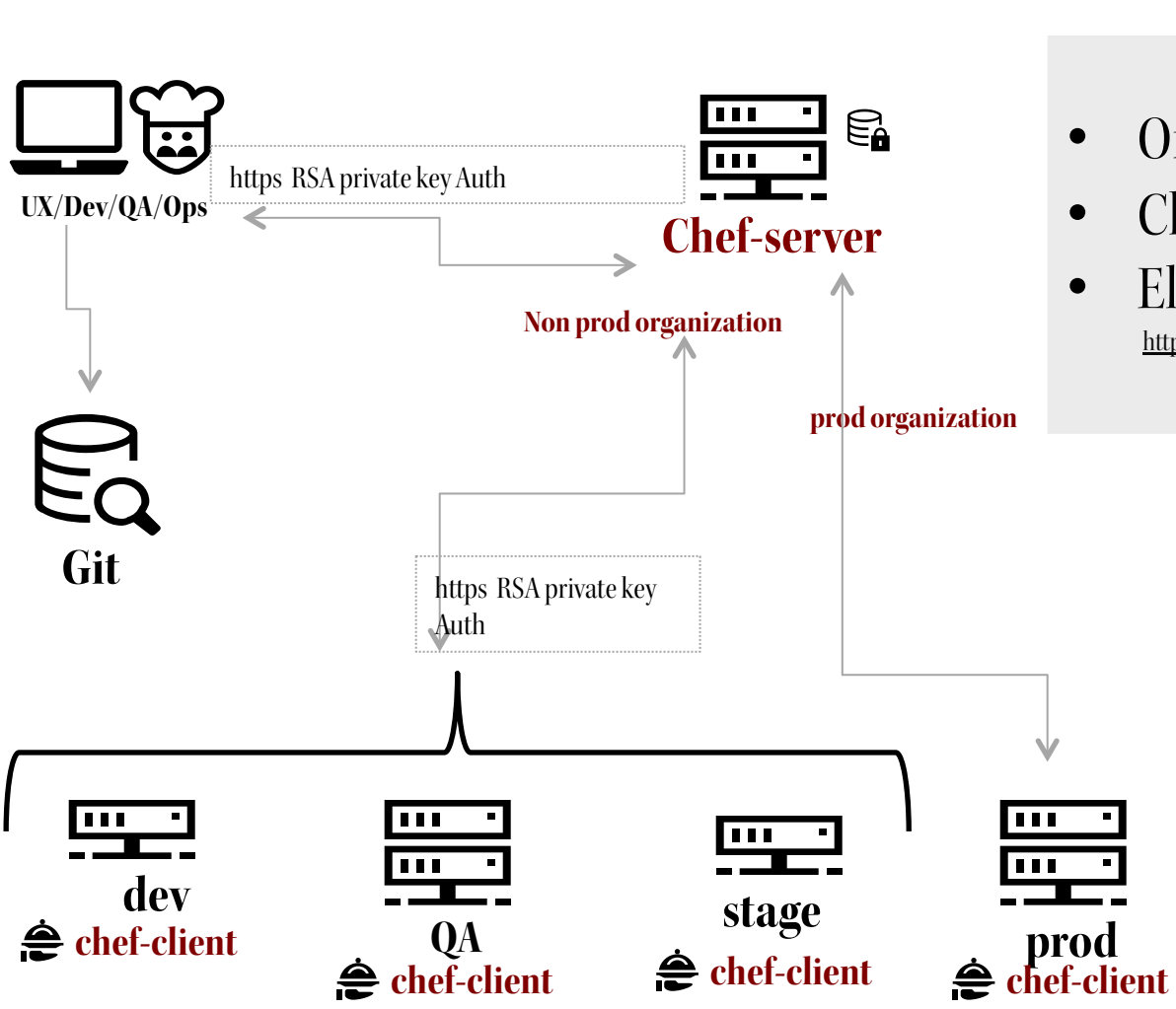
Chef-vault



- 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>



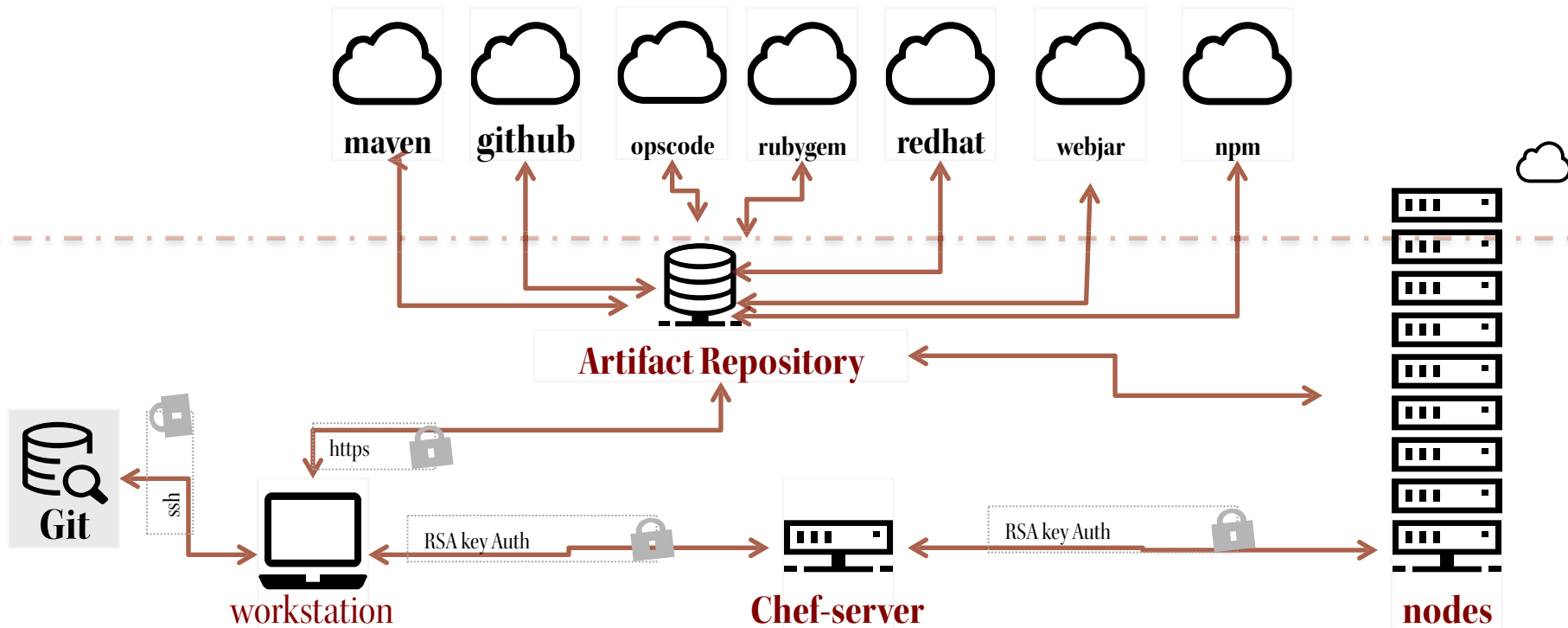
Securing Jenkins

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



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

Secure Dependency Management





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...

RETWEET

1



10:26 AM - 15 Jun 2015



NETFLIX
| ORANGE |
is the new BLACK |



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.

17 5

Oliver Bazoud and 8 others follow

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

19 6

Retweeted 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.

483 329

REAL API RESPONSE TIME

44ms



HTTP POST, 200, 204, 208, 212

288ms



PAGES BUILT FAILURE RATE

1.2966%



EXCEPTION PERCENTAGE

0.0%



HTTP 500, 502, 503, 504

1.06s



APP SERVER AVAILABILITY

99.9868%



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 ?

