Hairy Security - The many threats to your webapp

Damien Plard (Platform Engineer @solarisBank)
a security specialist who doesn't get Java

Romain Pelisse (Sustain Developer @Red Hat)
a so called Java developer who knows even less about security

Threats Modeling - STRIDE

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

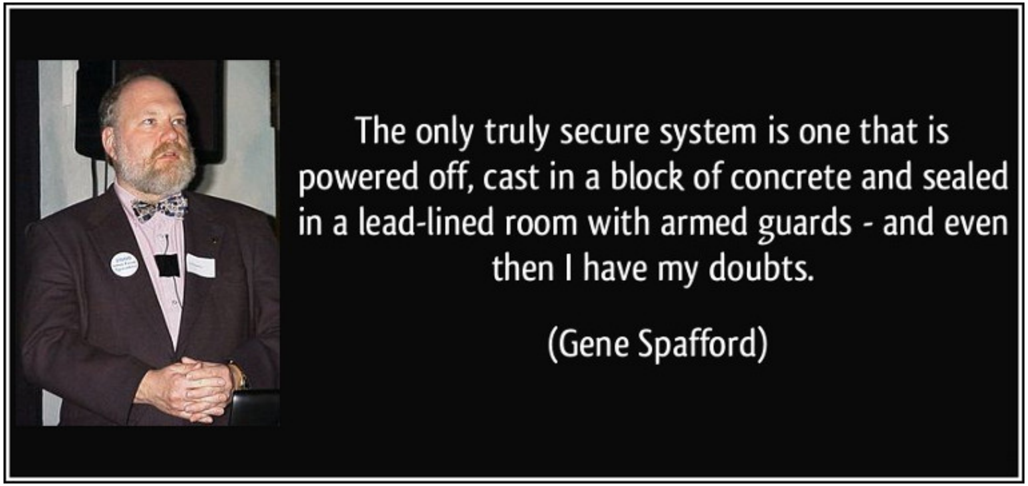
Threats Modeling - DREAD

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

Use Case - a simple WebApp

Frameworking your way out of security...

Safe(r?) Intranet

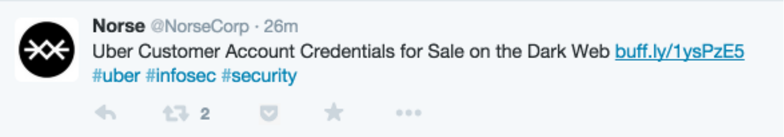


The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.

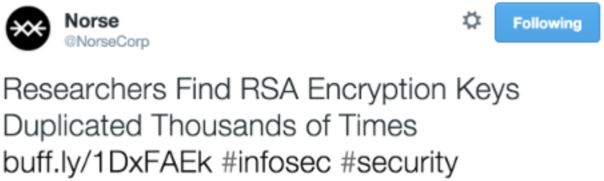
(Gene Spafford)

Reverse Proxy

Data

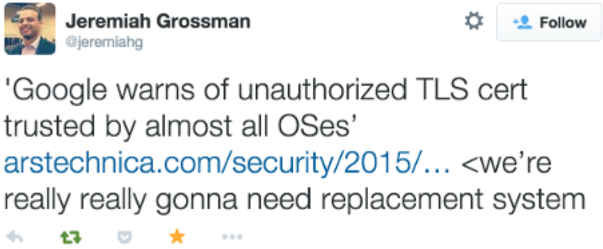


Norse @NorseCorp · 26m
Uber Customer Account Credentials for Sale on the Dark Web buff.ly/1ysPzE5 #uber #infosec #security



Norse
@NorseCorp

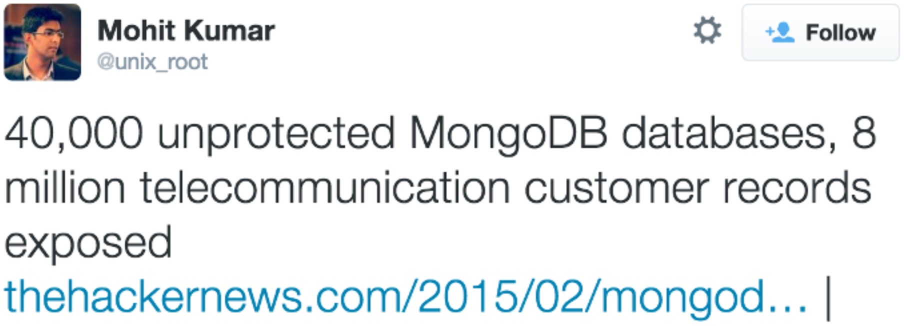
Researchers Find RSA Encryption Keys Duplicated Thousands of Times buff.ly/1DxFAEk #infosec #security



Jeremiah Grossman
@jeremiahg

'Google warns of unauthorized TLS cert trusted by almost all OSes' arstechnica.com/security/2015/… <we're really really gonna need replacement system

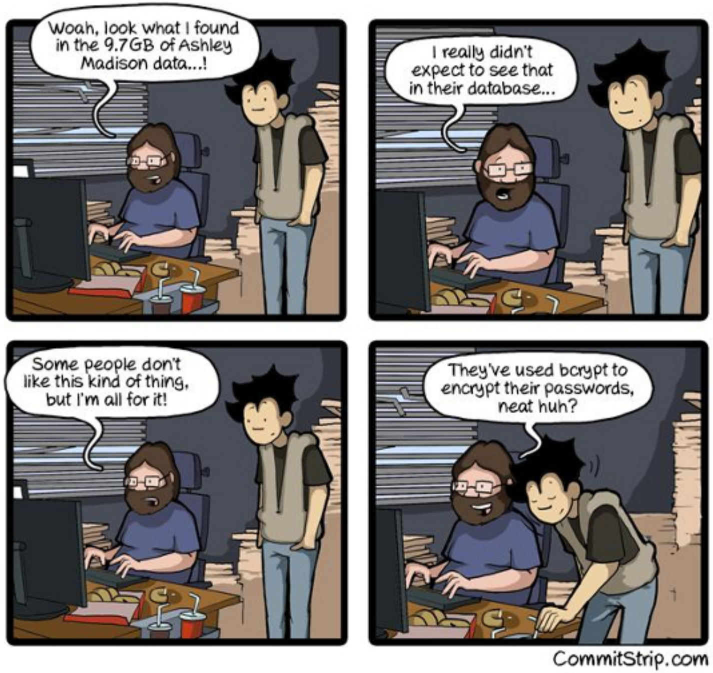
Data Storage



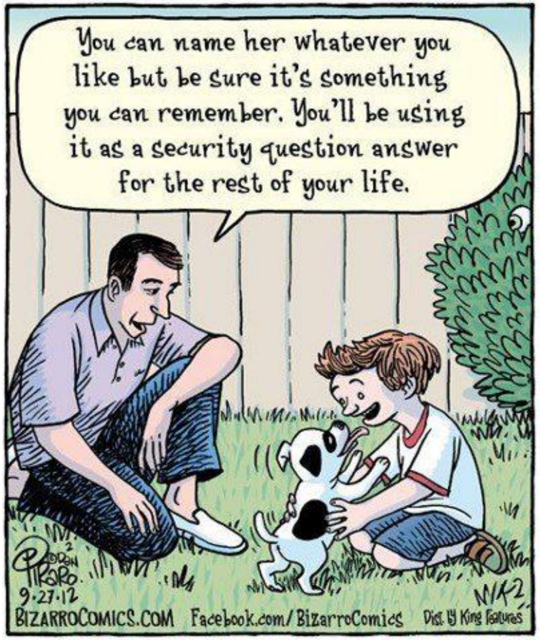
Mohit Kumar
@unix_root

40,000 unprotected MongoDB databases, 8 million telecommunication customer records exposed thehackernews.com/2015/02/mongod… |

Encrypt with care


Woah, look what I found in the 9.7GB of Ashley Madison data...!
I really didn't expect to see that in their database...
Some people don't like this kind of thing, but I'm all for it!
They've used bcrypt to encrypt their passwords, neat huh?
CommitStrip.com

Authentication & Authorization

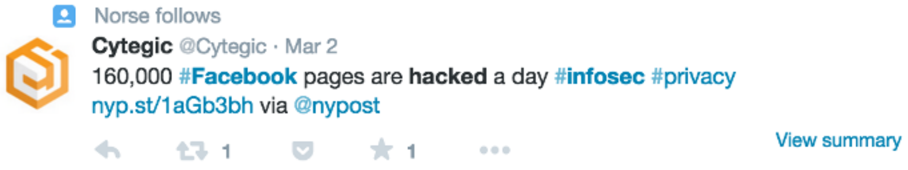

You can name her whatever you like but be sure it's something you can remember. You'll be using it as a security question answer for the rest of your life.
Piraro 9-27-12
BIZARROCOMICS.COM Facebook.com/BizarroComics Dist. by King Features

Strong Authentification

100% of security breaches implied stolen passwords in 2014

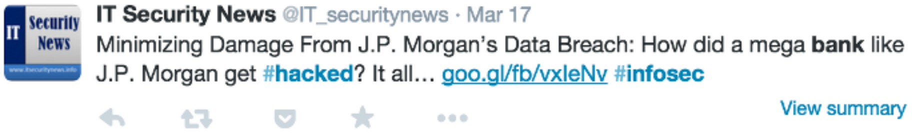
http://www.idtheftcenter.org/

Password can (and will) be stolen

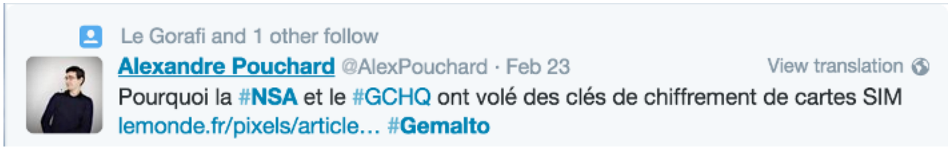

Norse follows

Cytegic @Cytegic · Mar 2

160,000 #**Facebook** pages are **hacked** a day #**infosec** #privacy nyp.st/1aGb3bh via @nypost


IT Security News @IT_securitynews · Mar 17

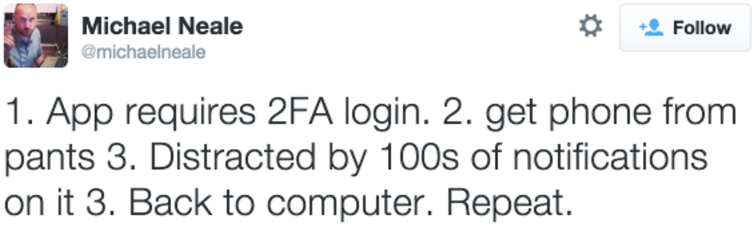
Minimizing Damage From J.P. Morgan's Data Breach: How did a mega **bank** like J.P. Morgan get #**hacked**? It all… goo.gl/fb/vxleNv #**infosec**


Le Gorafi and 1 other follow

Alexandre Pouchard @AlexPouchard · Feb 23

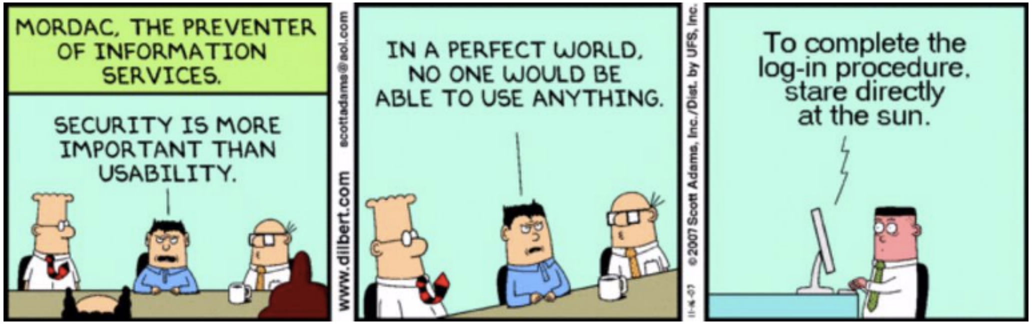
Pourquoi la #**NSA** et le #GCHQ ont volé des clés de chiffrement de cartes SIM lemonde.fr/pixels/article… #**Gemalto**

Security vs UX? Really?

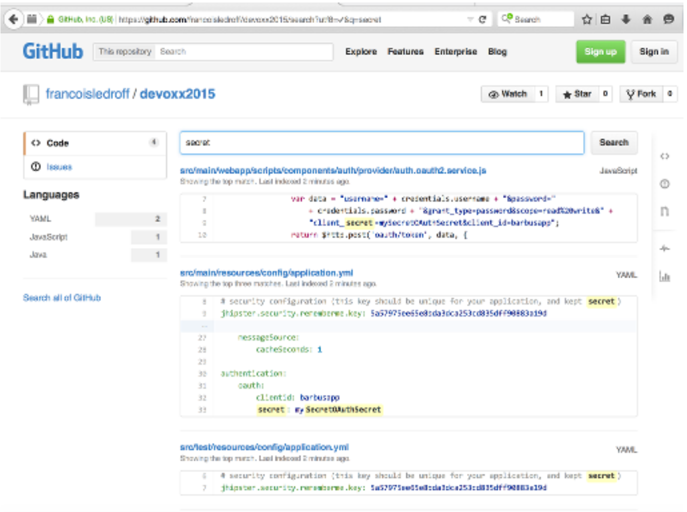


Michael Neale
@michaelneale

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


MORDAC, THE PREVENTER OF INFORMATION SERVICES.
SECURITY IS MORE IMPORTANT THAN USABILITY.
scottadams@aol.com
www.dilbert.com
IN A PERFECT WORLD, NO ONE WOULD BE ABLE TO USE ANYTHING.
©2007 Scott Adams, Inc./Dist. by UFS, Inc.
11-4-07
To complete the log-in procedure, stare directly at the sun.

Continus Integration - Handling secrets



https://github.com/francoisledroff/devoxx2015/search?utf8=✓&q=secret

francoisledroff / devoxx2015

secret

Languages

YAML	2
JavaScript	1
Java	1

Search all of GitHub

src/main/webapp/scripts/components/auth/provider/auth.oauth2.service.js

Showing the top match. Last indexed 2 minutes ago.

```
            var data = "username=" + credentials.username + "&password="
                + credentials.password + "&grant_type=password&scope=read%20write&" +
                "client_secret=mySecretOAuthSecret&client_id=barbusapp";
            return $http.post('oauth/token', data, {
```

src/main/resources/config/application.yml

Showing the top three matches. Last indexed 2 minutes ago.

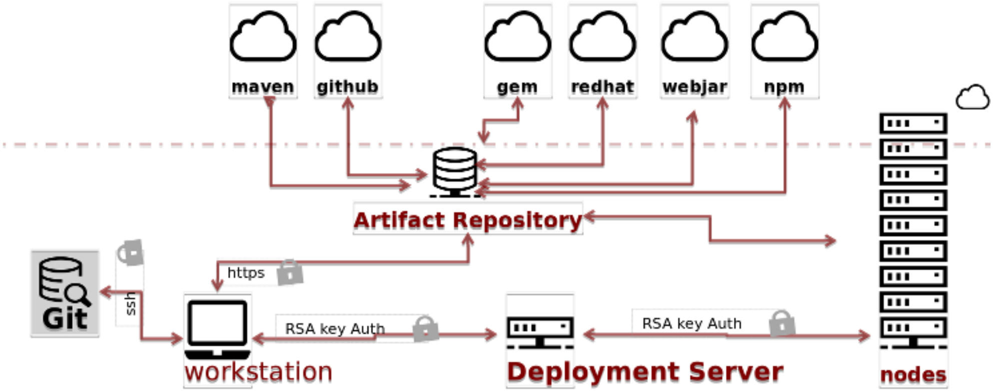
```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: 5a57975ee65e8cda3dca253cd835dff98883a19d
...
    messageSource:
        cacheSeconds: 1

authentication:
    oauth:
        clientid: barbusapp
        secret: mySecretOAuthSecret
```

src/test/resources/config/application.yml

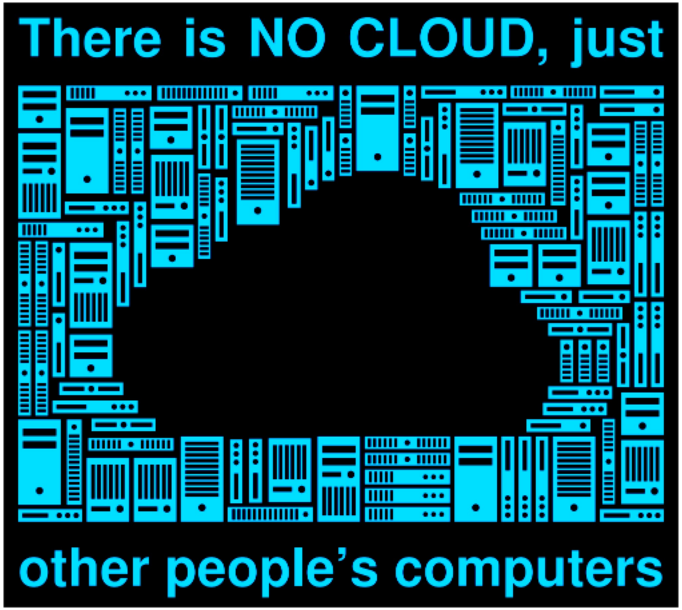
Showing the top match. Last indexed 2 minutes ago.

```
# security configuration (this key should be unique for your application, and kept secret)
jhipster.security.rememberme.key: 5a57975ee65e8cda3dca253cd835dff98883a19d
```

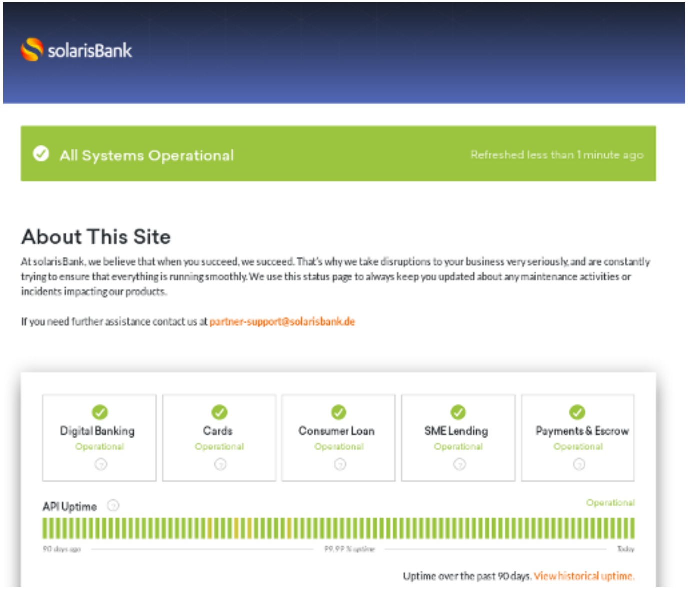
Artifacts - Don't trust the Internet



Safer in the clouds ?



Transparency is a thing



solarisBank

All Systems Operational

Refreshed less than 1 minute ago

About This Site

At solarisBank, we believe that when you succeed, we succeed. That's why we take disruptions to your business very seriously, and are constantly trying to ensure that everything is running smoothly. We use this status page to always keep you updated about any maintenance activities or incidents impacting our products.

If you need further assistance contact us at partner-support@solarisbank.de

Digital Banking	Cards	Consumer Loan	SME Lending	Payments & Escrow
Operational	Operational	Operational	Operational	Operational

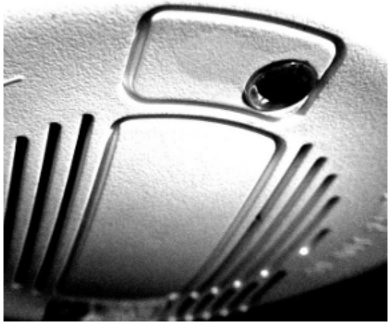
API Uptime

Operational

90 days ago — 99.99 % uptime — Today

Uptime over the past 90 days. View historical uptime.

Born to be Hacked!



So remember…

- Security is **your responsibility**, think about it!
- Use **Threat modeling**!
- You’ll never be safe, nor will your data
- so **Encrypt**, everything that needs to!
- Manage your secrets and use **strong authentification**!
- 2FA and SSO!
- Security is not an excuse for a **bad UX**
- Don’t forget continuous integration and the cloud
- Be ready to **firefight**!