The Future of Internet Security

Drupalcon 2017

Keeping up with the ever changing security threats to Drupal and the web

Lockr

Who is this guy?

Chris Teitzel
Founder / CEO Lockr

technerdteitzel

Cellar Door

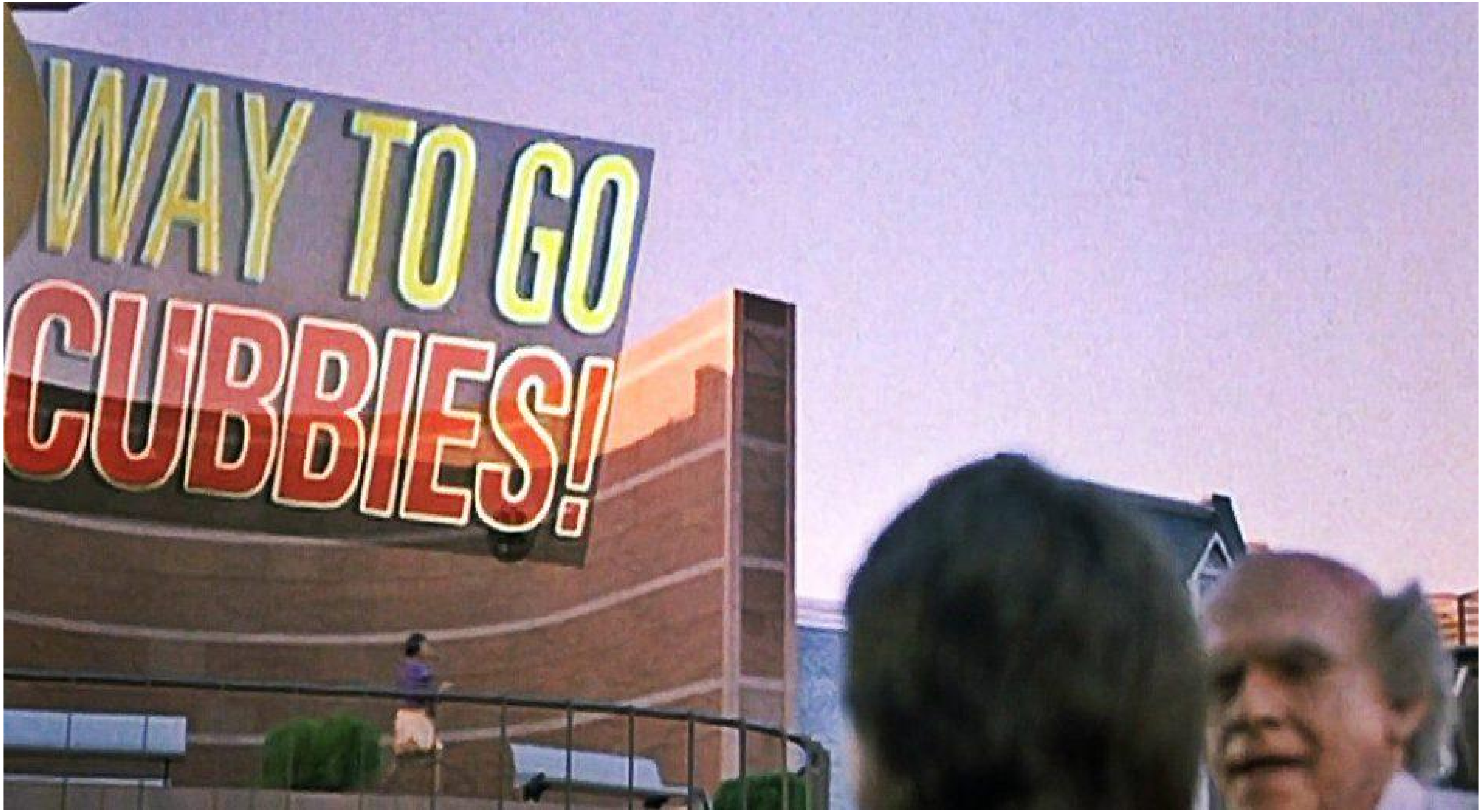
- 7 years 10 months in Drupal
- Omega, Encrypt, Key, File Encrypt, Field Encrypt...

STEVEN SPIELBERG PRESENTS
BACK TO THE FUTURE
PART II
A ROBERT ZEMECKIS FILM
OUTATIME

The mysterious future

174 50

Needles, Douglas J.
Food Preference: Steak, Mex
Food Disli


WAY TO GO
CUBBIES!

The mysterious future

amazon echo
Always ready, connected, and fast. Just ask.
music
tunein
iHeart RADIO
npr news
31
we mo
hue
PHILIPS
UBER
audible
IFTTT
amazon

nest
70

PHILIPS

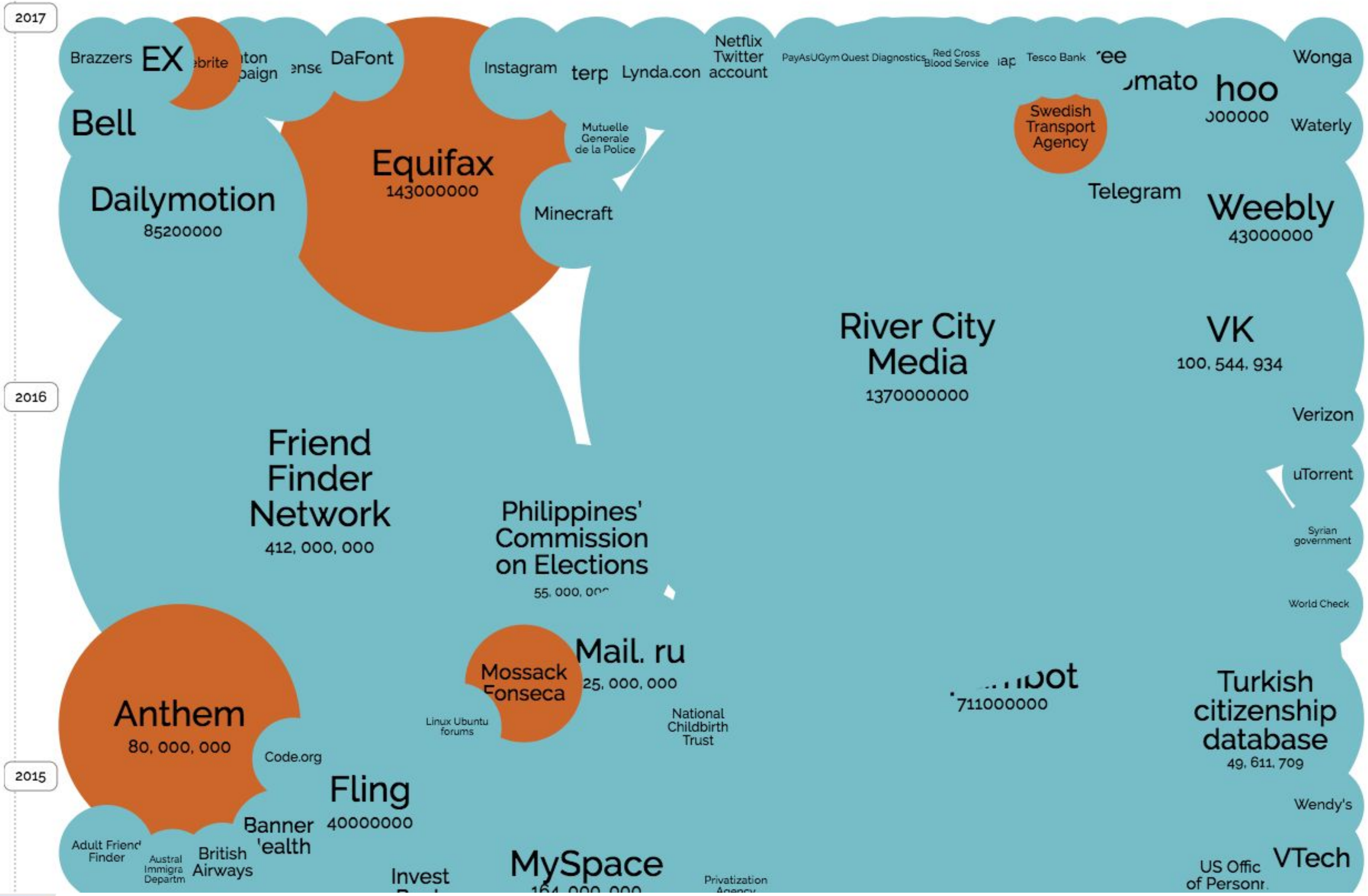
Front Door

wemo
Mr. Coffee
6:00
MR.COFFEE

Your entire life is connected…

As your digital footprint expands, so does the amount of personal data at risk

*I'm not inherently saying this is bad, but as developers we have a responsibility



Breaches are not going away

Data is the most valuable asset in the world

The ability to collect, analyze, forecast and act upon data will drive the next decade of global business growth

We need to look no further than the acquisition of The Weather Channel by IBM. The ability to feed detailed weather data into Watson multiplies the inherent value of the data.

" Whether you are going for a run, watching TV or even just sitting in traffic, virtually every activity creates a digital trace... As devices from watches to cars connect to the internet, the volume (of data) is increasing: some estimate that a self-driving car will generate **100 gigabytes per second**. Meanwhile, artificial-intelligence (AI) techniques such as machine learning extract more value from data. Algorithms can predict when a customer is ready to buy, a jet-engine needs servicing or a person is at risk of a disease. Industrial giants such as GE and Siemens now sell themselves as data firms."

The Economist

https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource

Successful Companies Collect Data

- Whether you think the data is important at this time, data can have future value

- Use data to drive your decisions, back up your theories, and lead your company, product and team

IoT Turning into IoHT

- DDoS attack of orchestrated DVR and IoT devices took down Dyn
- Car computers programmed to stop and baby monitors being compromised are just the first wave
- Every connection to the web, creates a new surface for attack and data loss

Personal Data Everywhere

- Seemingly innocent data can be pieced into an identity
  - Quick survey
- Identity theft isn't the only goal for a breach
  - Corporate Espionage
  - Political gain
- Inform your users what you are collecting
  - It's not just the right thing to do, it's the law!

Regulations Increasing

- Poor security has become a “cost of business”
- Acronyms for every industry:
  - PCI
  - HIPAA, FERPA, FISMA in the U.S.
  - The GDPR in the EU (and U.K.)

GDPR Leading the way

- May 25, 2018 enforcement begins
- More than just a cookie warning
- Security by design
- Data portability and the right to be forgotten
- Protection of personal data
  - Anonymization
  - Pseudonymization
  - Encryption
- 4% of **global** revenue as a maximum fine

Drupal as a full stack website

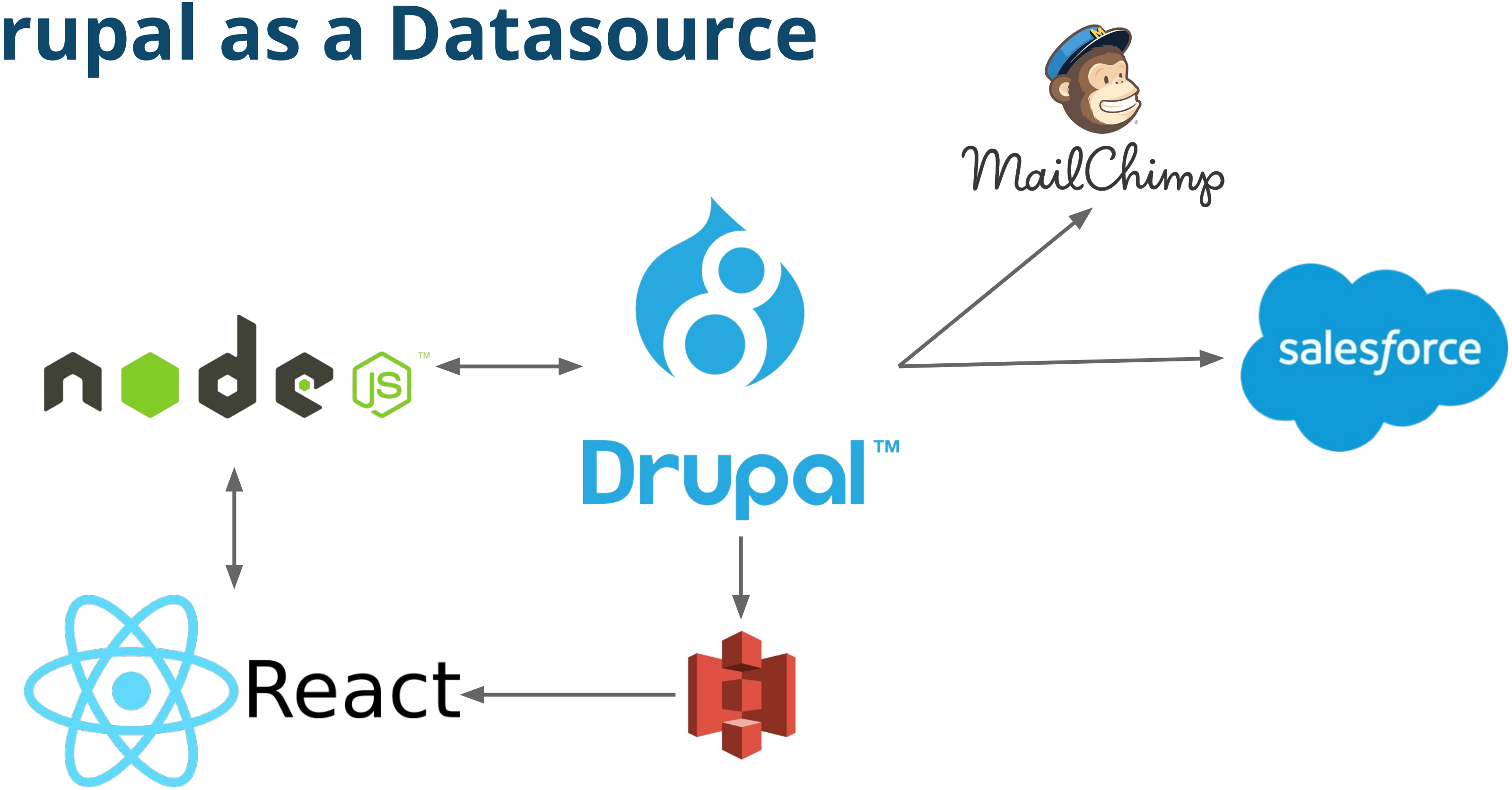
Drupal as a headless datasource

Drupal as a headless datasource

OWASP Top 10 2017 (not final)

- A1 - Injection
- A2 - Authentication and Session Management
- A3 - Cross-site Scripting
- A4 - Access Control
- A5 - Security Misconfiguration
- A6 - Sensitive Information Disclosure
- A7 - TBA (Insufficient Attack Protection?)
- A8 - Cross-site Request Forgery
- A9 - Using Components with Known Vulnerabilities
- A10 - TBA (Underprotetcted APIs?)

Drupal as a Datasource



Lockr

Drupal as part of the larger ecosystem

Drupal as a Datasource

- Arguably the best open-source CMS for complex data modeling and distribution
  - Entities in Drupal 7 led the way
  - API first design of Drupal 8 continues to grow
  - Inclusion of Media in core
- Tailoring the “Authoring experience” instead of the user experience

Drupal gives powerful tools for data modeling

An API Driven World

Square

Payment Gateways

MailChimp

Email Marketing

SendGrid

SMTP Relays

OAUTH 2 OAUTH

Authentication

FedEx

Shipping

amazon web services

Cloud Providers

NIST

Encryption

{ api }

APIs

Multiple entry points for attack

Recent Attack

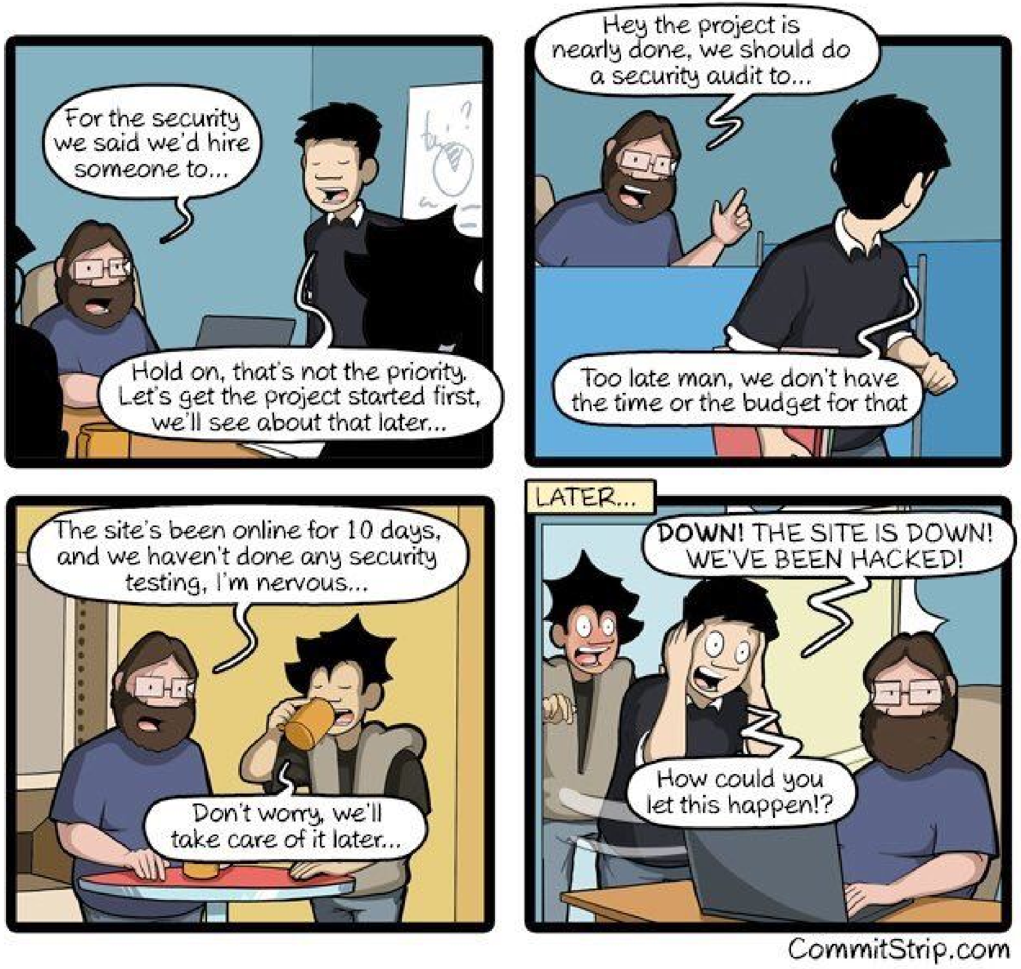
“...we know that a threat actor used one of our AWS keys to gain access to our AWS platform via API from an **intermediate host** with another, smaller service provider in the US.”

onelogin

Security starts at the top

Grow a team mentality of security in an ever changing online threat landscape

A little humor…
a lot of truth


For the security we said we'd hire someone to...
Hold on, that's not the priority. Let's get the project started first, we'll see about that later...
Hey the project is nearly done, we should do a security audit to...
Too late man, we don't have the time or the budget for that
The site's been online for 10 days, and we haven't done any security testing, I'm nervous...
Don't worry, we'll take care of it later...
LATER...
DOWN! THE SITE IS DOWN! WE'VE BEEN HACKED!
How could you let this happen!?
CommitStrip.com

Security as an afterthought

Team Security Best Practices

- Don’t discount security concerns
- Always ask: What if this information gets out?
- Use tools and services to protect before an attack
  - Password vaults
  - WAF/CDN
- If an incident occurs:
  - Breath - staying calm avoids poor decisions
  - Backup - You want to know why it occurred
  - Post-Mortem - Don’t blame, learn

Drupal Modules for Security

- Encrypt (Real AES)
- Key
- Password Policy
- TFA (Two Factor Authentication)

Just a sampling - many many more exist

Guardr - Secure Drupal Distribution

- Distribution with modules and settings
- Helps Drupal meet today's enterprise and regulatory needs
- https://drupal.org/project/guardr

The Price of DevOps

“If your website is worth more than $5…
Pay more than $5 for hosting it.”

Don’t Do Security Alone

- Open source does not make software less secure
  - Do update your software
- Focus on what you do best as a team/company and let the experts do their job
- Continually re-evaluate your data decisions

I get by with a little help from my friends

Security Doesn’t Kill the Fun

- The future of the web, and Drupal, is an exciting new frontier
- Use Drupal to create the next generation of IoT and connected deviceS

Thank You!

Drupalcon 2017 | Slides will be up shortly

Lockr