Don’t Build “Death Star” Security

Maintaining agility and security in distributed and microservice architectures
About Me

- **Drupal**
  - Infrastructure (drupal.org)
  - Security
  - Performance/scalability, especially database

- **Systemd**
  - Committer
  - Scalable cgroups management
  - Structured logging integration
  - Launch-on-demand adapter maintainer

- **Pantheon**
  - CTO and Co-founder
  - Billions of monthly page views
  - Billions of monthly page views
Your infrastructure is the Empire...
...and Rebel scum from Tatooine threatens it.
“Death Star” security is reinforcing the edge...
...but suffering catastrophe when that’s breached.
We’re not here to talk about basics or your edge

- Layer 2 or 3 Firewalls
- Web Application Firewalls
- OWASP Top 10
- DDoS Controls

For the purposes of this presentation:

Your first line of defense is gone!
Where Do Attackers Go Next?

- Collecting authentication data
- Using the foothold behind the firewall
  - Attacking other internal systems
  - Exploiting the assumption of trust
- Collecting sensitive user, payment, and patient data
- Phishing attacks from privileged email accounts
Authentication Security
Challenge: Password Data Breach

827ccb0eea8a706c4c34a16891f84e7b

That's amazing! I've got the same combination on my luggage!

*President Skroob*
Password: 12345

Salt: 4c34a8371ce2d3116

Pepper: 27ccb0eea8a706c

HMAC SHA512

827ccb0eea891f84e7b8a7891f84e7b06c4c34a16891f84e7b

Pattern: Better Password Hashing
Pattern: Add in Password Stretching

Password: 12345
Salt: 4c34a8371ce2d3116
Pepper: 27ccb0eea8a706c

PBKDF2 (100k rounds)

84e7b8827ccba891f84e7b8a7891f84e7b06c4c34a16891
Pattern: Requiring Decent Passwords
Pattern: Multifactor Authentication

Something You Have
or
Something You Are
Pattern: Federated Authentication
Pattern: Authentication Before Application

Apache with SAML

Drupal or WordPress with PHP-FPM
Have You Met the Confused Deputy?
Challenge: Ambient Authority and Confused Deputies

How it’s supposed to work:

Set a course for Alderaan.

Governor Tarkin

Setting course, Governor.

Helm/Weapons

BOOM!

How it can fail:

Set a course for Coruscant.

Imposter Tarkin

Setting course, Governor.

Helm/Weapons

BOOM!
How it's supposed to work:

Set a course for ef28bc28 (signed token for Alderaan).

Governor Tarkin

Setting course, Governor.

Helm/Weapons

Attempted hack:

Set a course for, um, 3a2eb45a (invalid token).

Imposter Tarkin

Sorry, that code isn’t working in my helm system, Governor.

Helm/Weapons

Pattern: Capability-Based Security
Mandatory access control (MAC), like selinux

How it’s supposed to work:

Set a course for Alderaan.

Governor Tarkin

Setting course, Governor.

Helm/Weapons

BOOM!

Attempted hack:

Set a course for Coruscant.

Imposter Tarkin

Setting course, Governor.

Helm/Weapons

DENIED

Pattern: Mandatory access control (MAC), like selinux
Antipattern: Mandatory access control (MAC) as an afterthought
Better: Boundaries First, Container-Style
Staying Hands-Off Sensitive Data
Pattern: Delegated Handling of Sensitive Data

- Payments
  - chargify
  - Recurly
  - stripe

- Marketing
  - verticalresponse
  - MailChimp
  - Constant Contact

User Agent → HTTP GET → Your Application
HTTP POST → External Service → Sensitive Data
Don’t simply divide permissions into *read* versus *read+write*.

The ability to just *write* allows one side to irretrievably rid itself of access to sensitive information.
Protecting Data on the Move and Endpoints
Pattern: Key Management

- AWS Key Management System
- Alliance Key Manager by Townsend Security
  - Lockr (for Drupal and WordPress)
- Vault by HashiCorp
- Many more...

Lockr

- Audit Trail
- Alerts
Pattern: Anonymizing Data

sql-sanitize

Run sanitization operations on the current database.

```
drush sql-sanitize
```

Aliases

`sql-sanitize` has 1 alias/es:

```
drush sqlsan
```

Options

`sql-sanitize` accepts 4 option/s:

```
--sanitize-password : The password to assign to all accounts in the database.
```
Pattern: Smart Cards and Hardware Tokens
Preventing a Breach from Spreading
Pattern: Systems Isolation
Challenge: Shared Secrets (Including Passwords)
Anti-pattern: Security Through Obscurity

“An analysis of the plans found in their insecure git repository has demonstrated a weakness in the battle station.”
Pattern: Public Key Infrastructure
Creating a Local Certificate Authority (CA)

- **Once**: Create a certificate authority (CA):
  - Create a private key for the CA.
  - Create the certificate for the CA.
  - Distribute the certificate to your servers.

- **Every time**: Follow the normal certificate-creation steps:
  - Create a private key.
  - Create a certificate signing request (CSR).
  - Sign the certificate on the CA.
  - Deploy the certificate alongside the private key.
MySQL PKI: Server Side

```
[mysqld]
ssl-ca=ca.crt
ssl-cert=server.crt
ssl-key=server.key

CREATE USER 'backups'@'backup-host'
  REQUIRE SUBJECT '/C=US/ST=California/L=San Francisco/
      O=Pantheon/
    CN=backups.pantheon.io/emailAddress=hosting@pantheon.io';
```

Supports rolling secret rotation for multiple clients!
<?php

pdo = new PDO('mysql:host=ip;dbname=db', 'user', 'pass', array(
    PDO::MYSQL_ATTR_SSL_KEY => '/etc/mysql/tls/client.key',
    PDO::MYSQL_ATTR_SSL_CERT => '/etc/mysql/tls/client.crt',
    PDO::MYSQL_ATTR_SSL_CA => '/etc/mysql/tls/ca.crt'
));

statement = $pdo->query('SHOW TABLES;');
$row = $statement->fetch(PDO::FETCH_ASSOC);
echo htmlentities($row['_message']);

MySQL PKI: Client Side
Tomcat PKI: Server Side

<Connector port="443" protocol="HTTP/1.1" SSLEnabled="true" scheme="https" secure="true"
keystoreFile="/etc/tls/servlet.ks"
keystorePass="secret"
clientAuth="true" sslProtocol="TLS"
truststoreFile="/etc/tls/servlet.ks"
truststorePass="secret" domain="catalina" />
nginx PKI: Server Side

...

server {
    listen 443 ssl;
    ssl_certificate server.crt;
    ssl_certificate_key server.key;
    ssl_client_certificate ca.crt;
}

...
Python PKI: Client Side

```python
import requests

requests.get('https://api.pantheon.io',
              cert=('client.crt', 'client.key'),
              verify='ca.crt')
```
Questions?

@DavidStrauss
david@pantheon.io
linkedin.com/in/davidstrauss