

APPLAND

# SPEED THE RIGHT WAY: DESIGN AND SECURITY IN AGILE

KEVIN GILPIN, CTO  
@kegilpin



# SPEEDING THE RIGHT WAY





# WHO AM I?

- Recently CTO, Conjur / CyberArk Fellow
- 20+ Years of Enterprise Software Engineering in healthcare, automotive, logistics, data science.
- Pioneer in DevOps, Cloud, and Containers
- MS Aerospace Engineering MIT
- Aviation enthusiast!



# "BLAME THE PROGRAMMER"

## Security

### 'Coding' cockup blamed for NHS cough-up of confidential info against patients' wishes

Another day, another UK public health data breach

By [Rebecca Hill](#) 3 Jul 2018 at 10:48

71 

SHARE ▼



## Cloudflare 'Cloudbleed' Flaw Leaks User Data from Millions of Websites



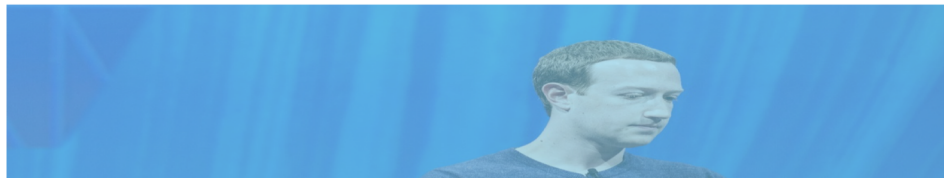
By [Jeff Goldman](#), Posted February 27, 2017

*The exposed data ranges from password manager data to hotel bookings and private messages.*

SHARE



## EVERYTHING WE KNOW ABOUT FACEBOOK'S MASSIVE SECURITY BREACH

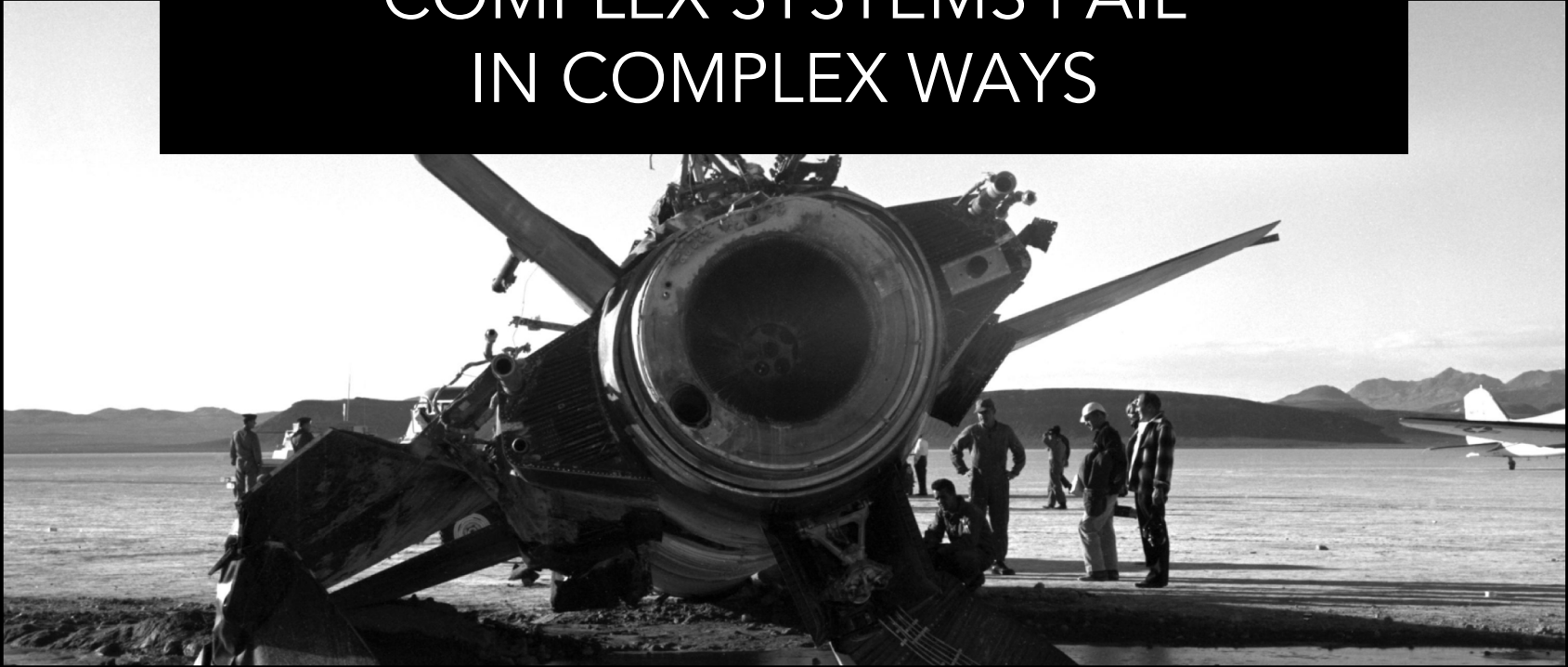


# AGENDA

- Discussion of breach examples
- How to review designs for security
- How to modernize design reviews



# COMPLEX SYSTEMS FAIL IN COMPLEX WAYS



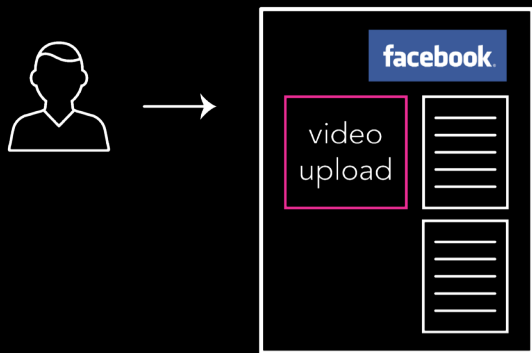
# SPEEDING THE **WRONG** WAY: FACEBOOK "VIEW AS"

Attackers carried out their attack with a series of steps that let them hop, skip and jump their way into generating access tokens for millions of Facebook users.



# SPEEDING THE **WRONG** WAY: FACEBOOK "VIEW AS"

"control who can  
see what you share"



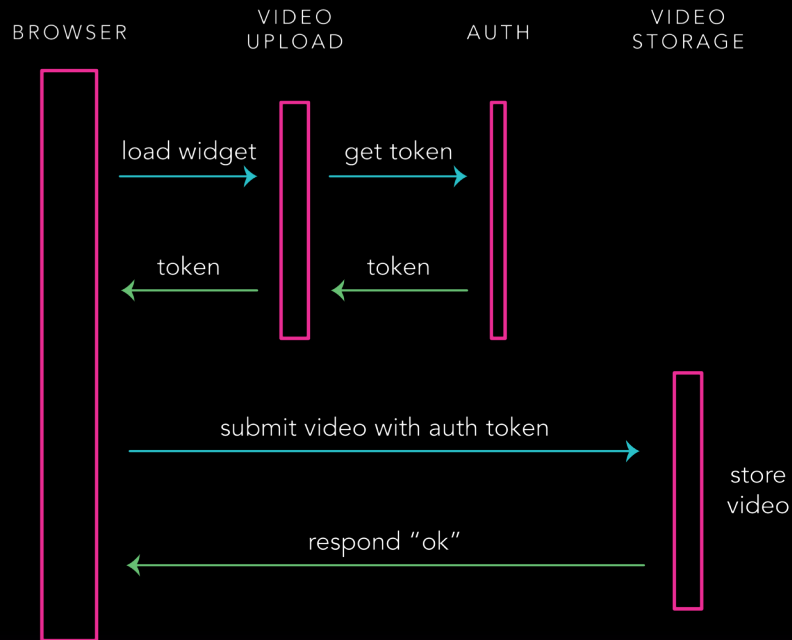
USER

BROWSER

auth

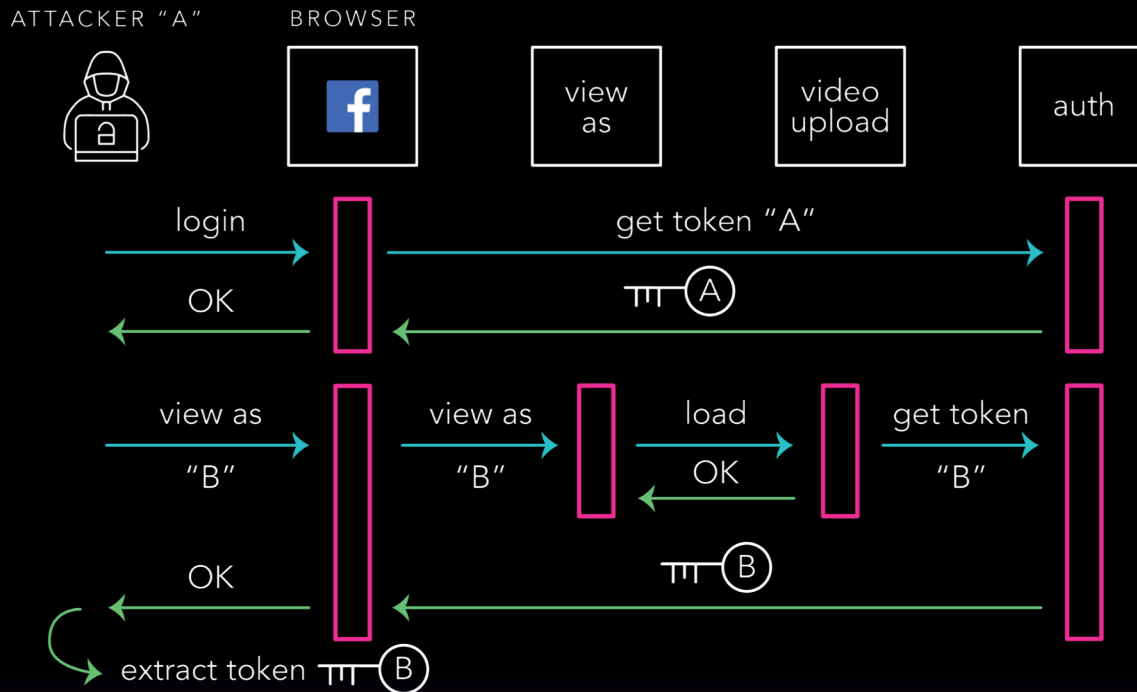
video  
storage

BACKEND





# SPEEDING THE **WRONG** WAY: FACEBOOK "VIEW AS"



# SUMMARY OF DESIGN FLAWS IN "FACEBOOK VIEW AS"

PROBLEM	EXAMPLE	IMPACT
Over-privileged service	"Video upload" service able to obtain a token for any user	"Video upload" service able to leak a token for the wrong user into the browser
Execution of untrusted code	"View as" did not whitelist the UI components which were trusted to operate correctly	"Video upload" widget was improperly loaded and executed in the UI
Lack of a secure sandbox	"View as" rendered untrusted code directly into the user's browser	Flaw in "Video upload" was exposed directly to the user rather than contained in a sandbox

# The "Swiss Cheese" model

... "likenes human systems to multiple slices of swiss cheese, stacked side by side, in which the risk of a threat becoming a reality is mitigated by the differing layers and types of defences which are "layered" behind each other"

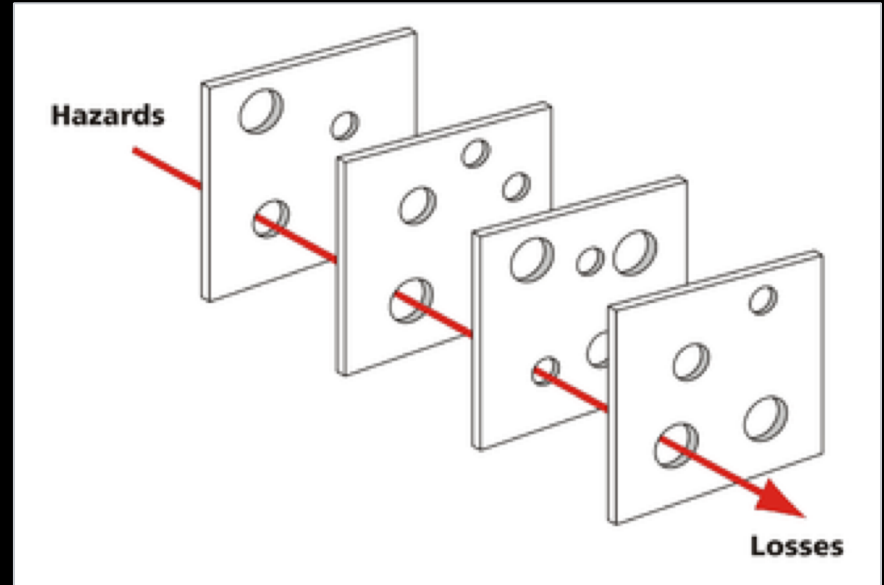


Image: [https://en.wikipedia.org/wiki/Swiss\\_cheese\\_model](https://en.wikipedia.org/wiki/Swiss_cheese_model)



# UK NHS BREACH "TYPE 2 OPT-OUT"

Point of care system  
didn't send the "Opt-Out"  
election to the NHS


So the NHS used all the  
patient data for 700,000  
people against their wishes

## Security

### 'Coding' cockup blamed for NHS cough-up of confidential info against patients' wishes

Another day, another UK public health data breach

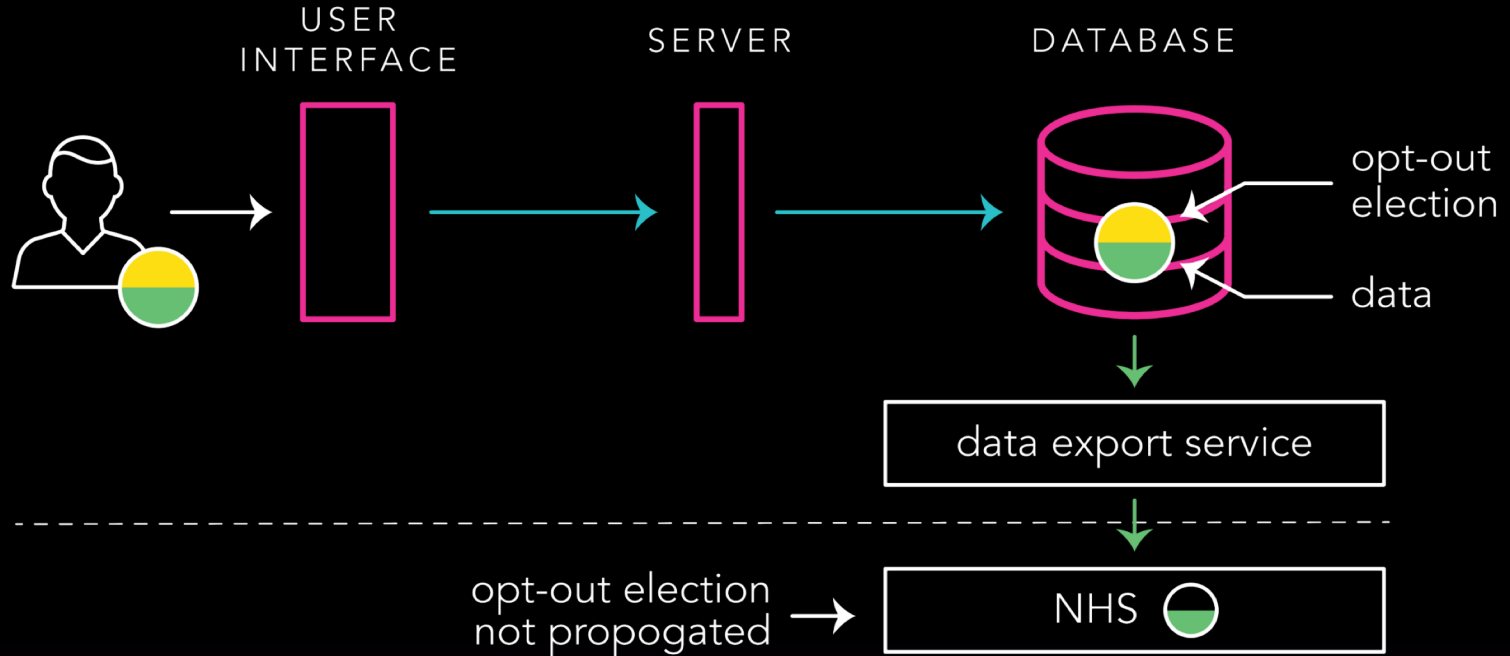
By [Rebecca Hill](#) 3 Jul 2018 at 10:48

71  [SHARE](#) ▼



# CASE STUDY

## "TYPE 2 OPT-OUT" NHS BREACH

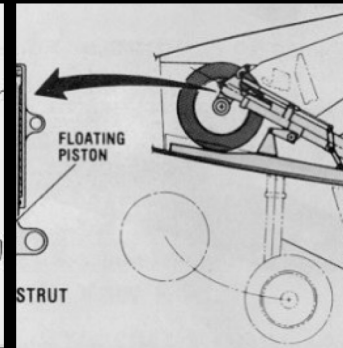
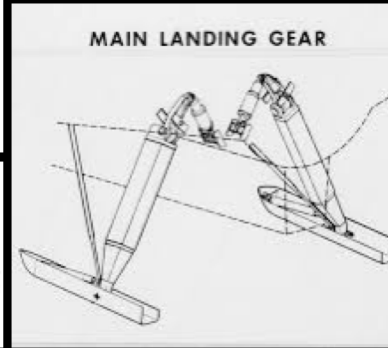
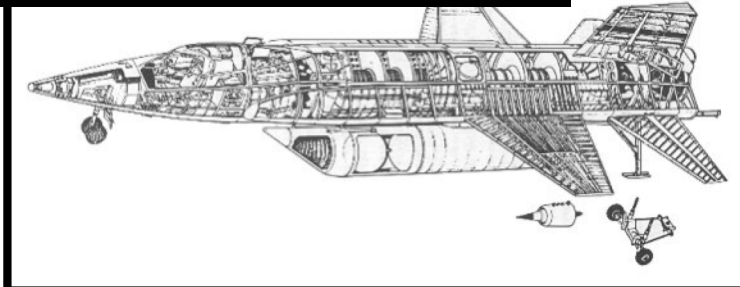
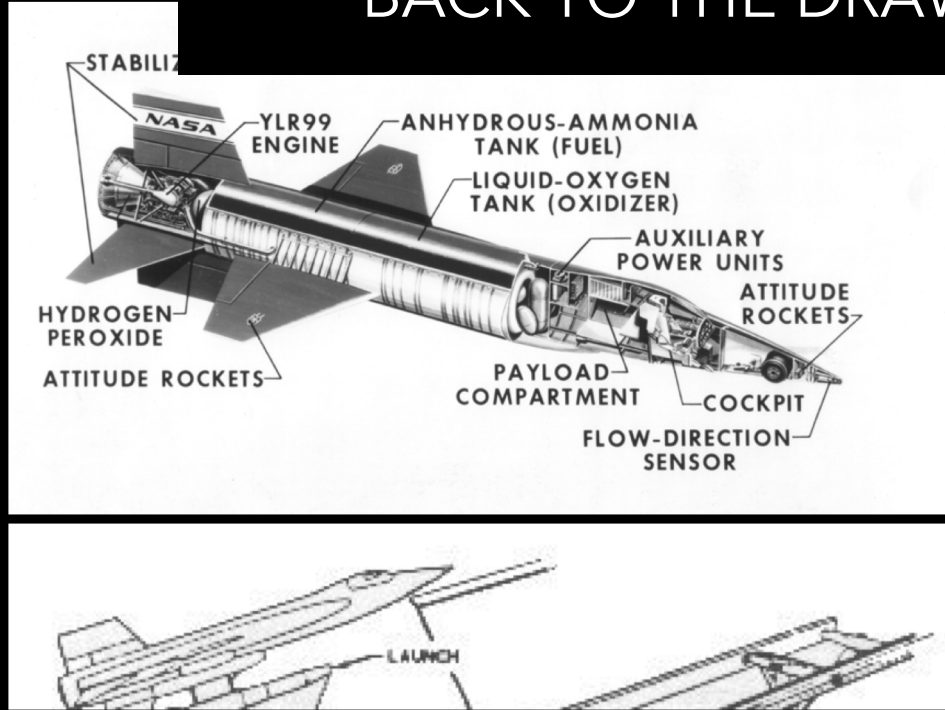


# SUMMARY OF DESIGN FLAWS IN "TYPE 2 OPT-OUT"

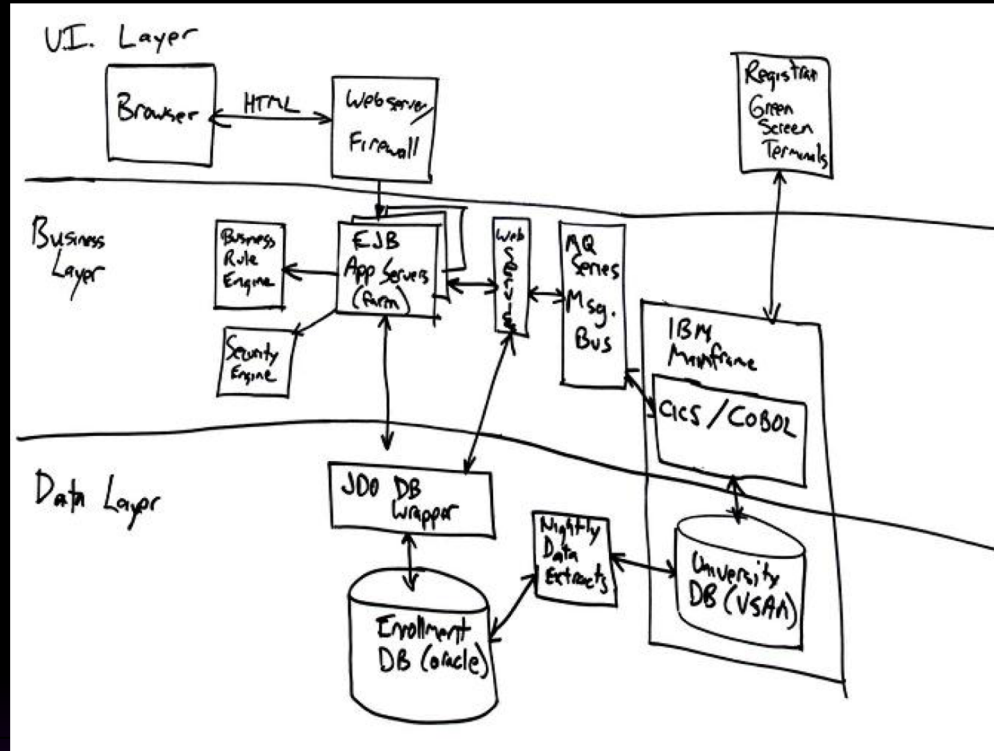
PROBLEM	EXAMPLE	IMPACT
Default allow	Data access allowed unless denied	Failure to propagate the opt-out election resulted in leaked data
Expiration	No time limit on opt-out election	Impact of the bug extended for an unlimited time
Lack of user notification	User not informed about how their data was being used	Failure to propagate the opt-out election was not reported by the users



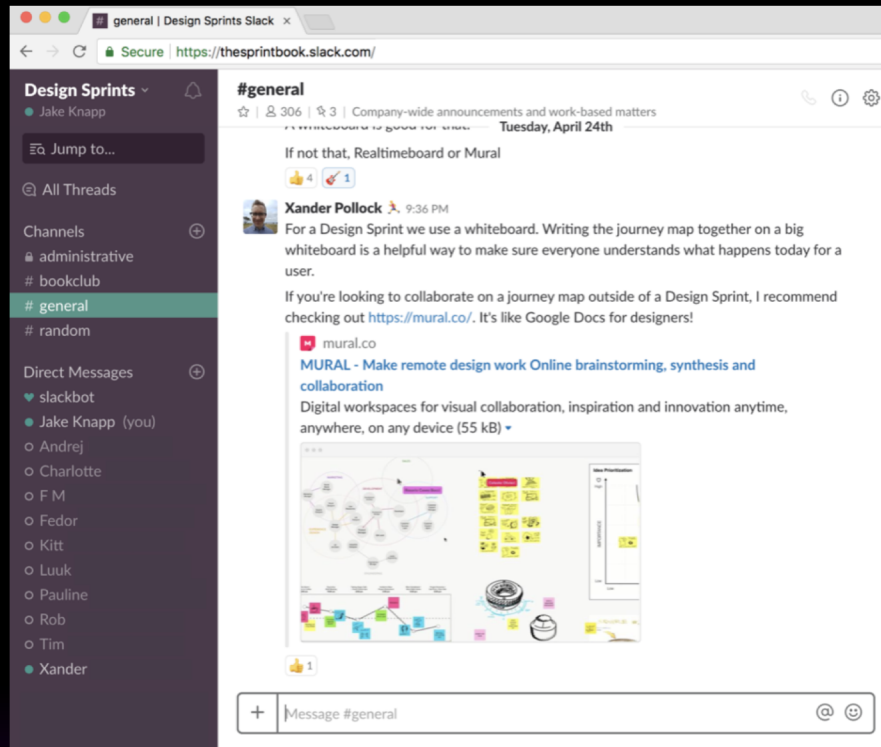
# BACK TO THE DRAWING BOARD



# HOW WE COMMUNICATE: WHITEBOARDS



# HOW WE COMMUNICATE: CHAT



# HOW WE COMMUNICATE: WIKI

The screenshot shows a Confluence page titled "Mobile Web Requirements" created by Mitch Davis. The page includes a sidebar with metadata and a main content area with a table of requirements. A tooltip titled "JIRA links" is visible, listing various JIRA items.

**Mobile Web Requirements**  
Created by Mitch Davis, last modified just a moment ago

Target release	1.0
Epic	<a href="#">MDT-18</a> - Mobile optimized web app
Document status	DRAFT
Document owner	@ Mitch Davis
Designer	@ Cassie Owens
Developers	@ Harvey Jennings
QA	@ Kevin Campbell

**Requirements**

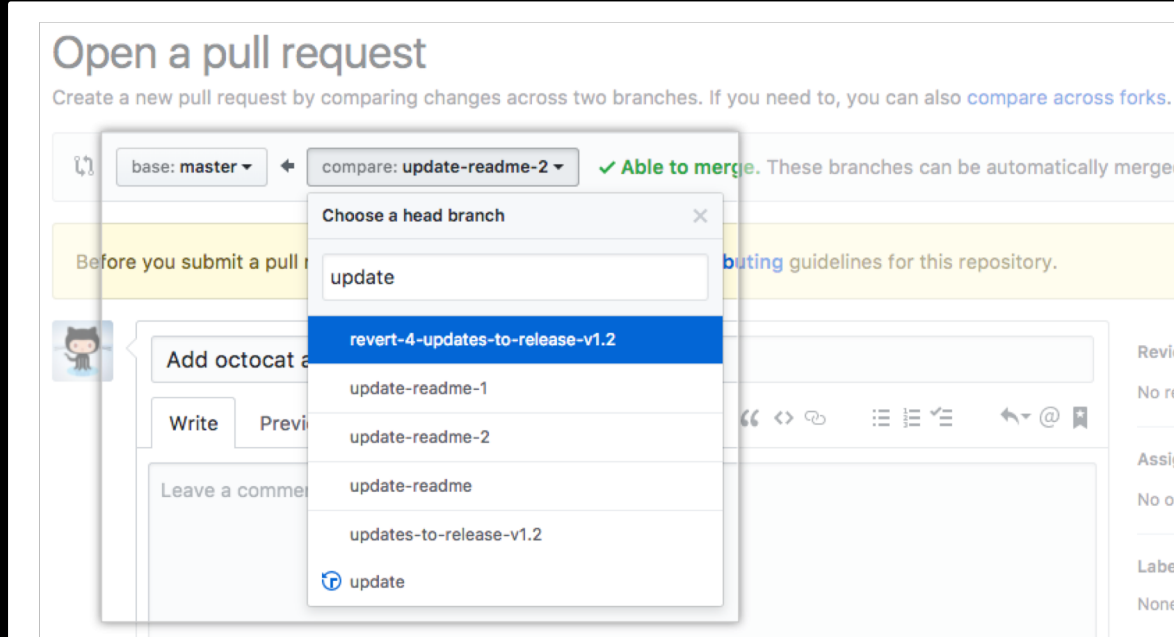
#	User story title	User story description
1	Facebook Integration	A user wants to sign up via Facebook

**JIRA links**

- Epics
  - [MDT-18](#)  
Mobile optimized web app
- Issues
  - [MDT-17](#) TO DO  
Twitter Integration
  - [MDT-16](#) TO DO  
API
  - [MDT-15](#) TO DO  
Post Updates
  - [MDT-14](#) TO DO  
Activity Stream
  - [MDT-13](#) TO DO  
Facebook Integration

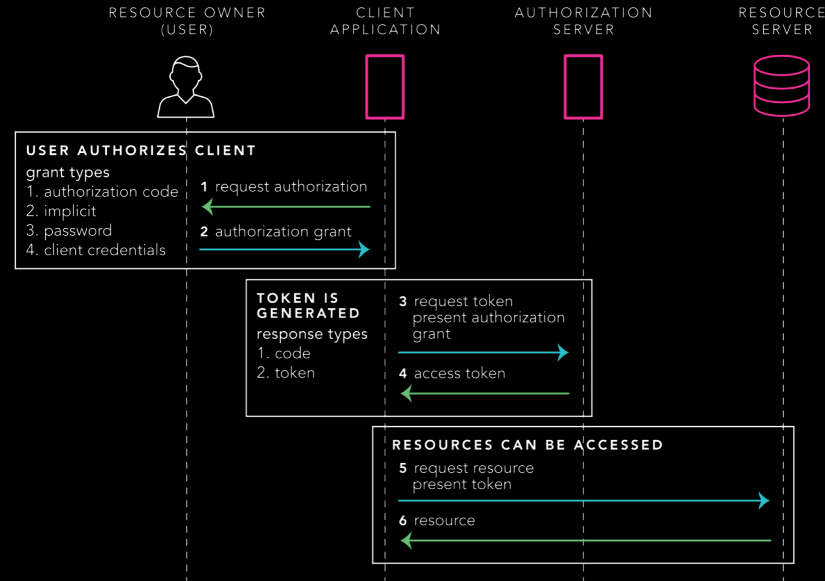
Image: <https://confluence.atlassian.com/doc/blog/2015/08/how-to-document-product-requirements-in-confluence>

# HOW WE COMMUNICATE: PULL REQUESTS



# THE COGNITIVE ARTIFACT – A FOCAL POINT FOR DISCUSSION

## OAUTH2 PROTOCOL FLOW



Source:

<https://www.onwebsecurity.com>

# PROPERTIES OF A GOOD COGNITIVE ARTIFACT

- **Big** enough and **expressive** enough for the design problem
- Built on a **collaborative** platform
- Lives **close** to the code
- The **quality** of the artifact becomes the quality of the product

# SIMPLE FORMULA FOR A DESIGN DOCUMENT

1. Overview
2. Diagram(s)
3. Design discussion
4. API specification
5. Q&A

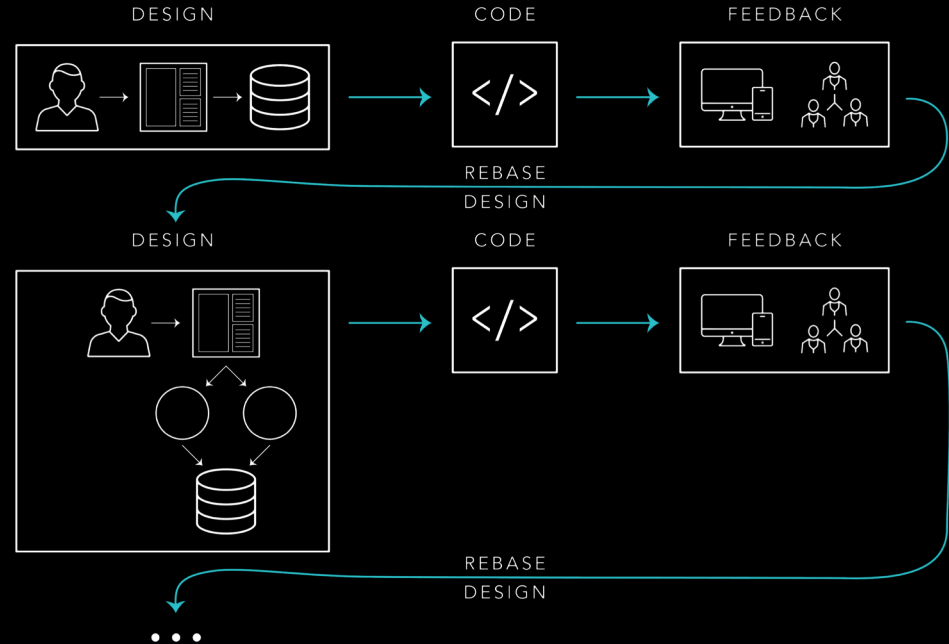


- You'll get feedback here
- Use RFCs as much as possible



# VISUALIZING “AS DESIGNED” VERSUS “AS BUILT”

- Design changes made during coding must be reflected back to the design artifacts
- Otherwise design artifacts get out of date



# GET MORE EYES ON THE PROBLEM



# WIDEN THE CIRCLE TO MAKE DESIGN MORE ACCESSIBLE

- A variety of people can add unique and valuable perspectives to the design review.
- To make design reviews more effective, make it clear to reviewers what's being asked of them.

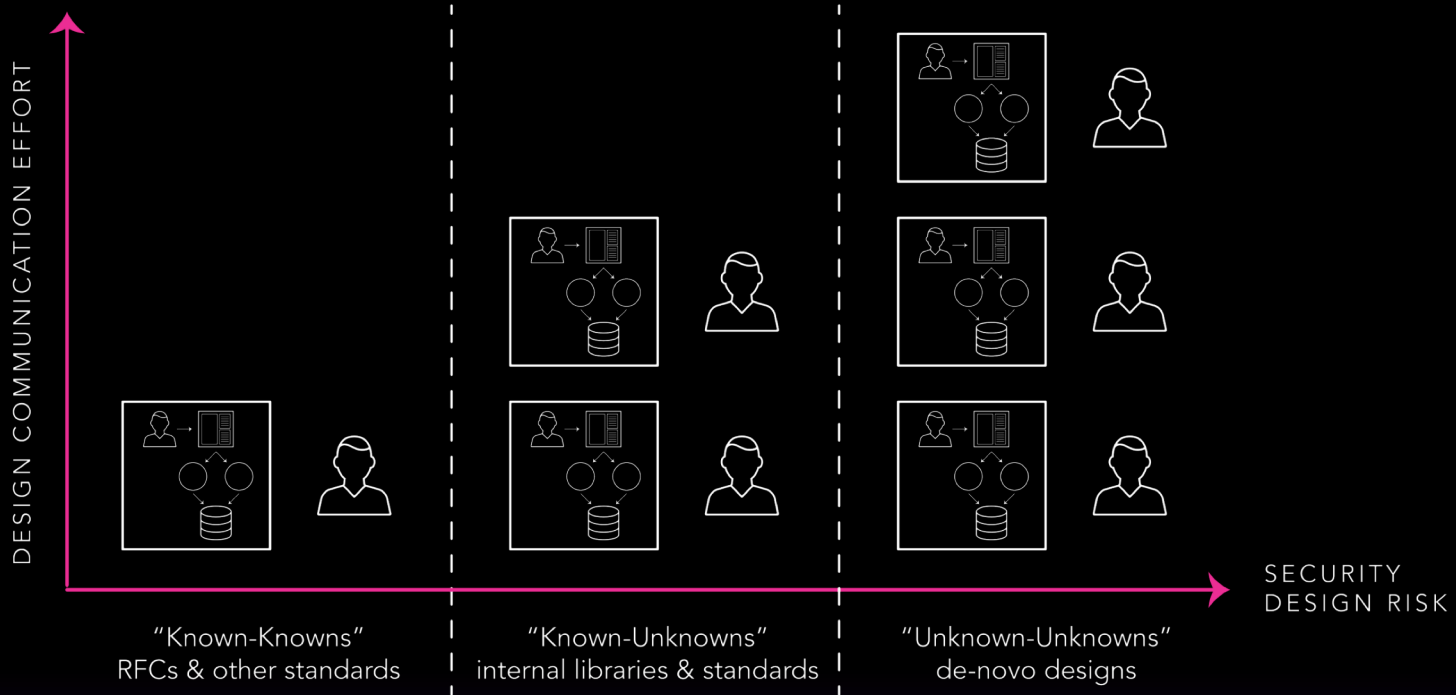


# ELEMENTS OF A DESIGN REVIEW

- Transforms *individual risk* into a *shared responsibility*.
- Like a pull request. Agile, but less technical.
- Performed upstream of the coding, and in parallel with prototyping.
- Importance and frequency of review is according to the risk.
- Microservice boundaries can be a helpful way to “tag” the code which needs extra design review attention.

Traditional test cases can verify that the code functions properly

# DESIGN REVIEW: WHO AND HOW MUCH?



# KEY TAKEAWAYS

- Security design flaws are not bugs... and flaws will be complex
- Invest in the right visual artifacts to get more eyes on the design
- Update the design artifact to accurately reflect "as built"
- Clearly indicate in code, READMEs, etc where a visitor can find the security design used in each project.
- For brand new designs, expect to invest heavily in design artifacts and design reviews in order to lower the risk

# DESIGN, A NOBLE PROFESSION

I took this photo-of-a-photo Sunday (March 3, 2019) at the RAF museum in Hanger 2 (World War I).





APPLAND

THANK YOU

@kegilpin

<https://www.linkedin.com/in/kegilpin/>

Further Reading

“Always Another Dawn” by Albert Scott Crossfield

