Getting Security Right the First Time

MacTech Conference 2014

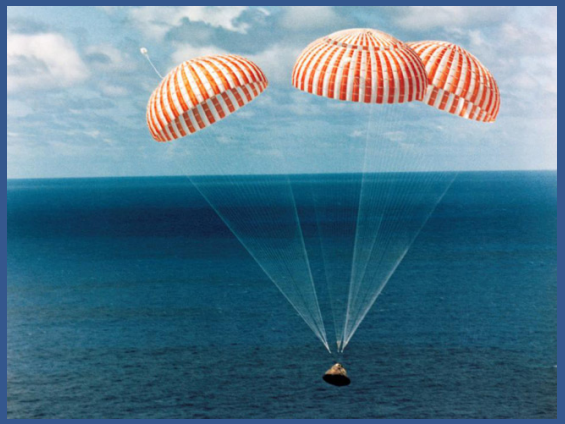
Andrew McDonnell

AsTech Consulting

Who cares?

How did we get here?

Engineering



Business

Security

One of these things is not like the others…

Let’s make an impregnable interplanetary conquest machine

But first…


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

Why do attackers have such an advantage?

How to be at every bank all the time

1. Security is an engineering problem
2. Misuse cases
3. Plan ahead, plan for failure

Building for Security

- What is at risk?
  - CIA
  - Reputation
- Cultivate security mindset
- Define problems narrowly
- “Why would anyone ever do that?”
  - Hackers
  - Griefers
- Training

Testing for Security

- Early and often
- SA with your QA
- Defect tracking and assignment

Hypothetical Example

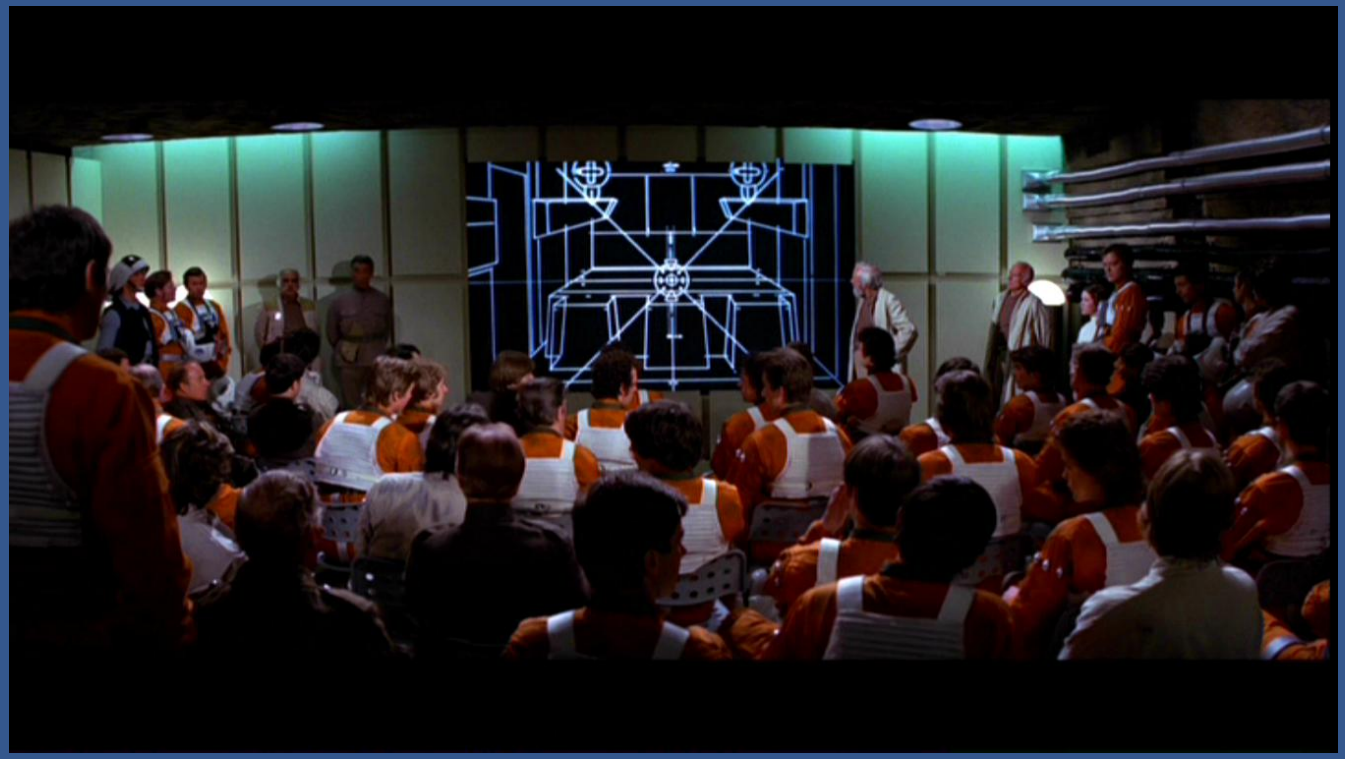
Planning to Fail

- Least privilege
- Decoupled functionality
- Encryption
- Tokenization
- Logging

Interstellar Vault Empires

- Tradeoffs
- Integrate processes, increase productivity
- Design it in
- Find, triage, fix, report
- Market your security

Questions?



Thank you

Andrew McDonnell
andrew.mcdonnell@astechconsulting.com
510.270.5551

ASTECH consulting