Building secure software and keeping it secure in the face of changing requirements
This guidance is in alpha
I am a civil servant
I work for the Government Digital Service
Publishing
Transactions
API's
Agile
Security vs Information Risk
Why bother?
What are the threats?
Data loss and theft
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
http://www.nbcnews.com/id/8985989/#.VQgdgWSsU8Z
http://news.bbc.co.uk/1/hi/uk/7103911.stm
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
Criminal users on the internet
GameOver/Zeus Banking Malware
Figure 16: The webinject file is used by attackers to customize attacks for specific sites and applications

1. Malware coder writes malicious software to exploit a computer vulnerability and installs a trojan

2. Victim infected with credential-stealing malware

3. Banking credentials siphoned

4. Hacker retrieves banking credentials

5. Remote access to compromised computer

6. Hacker logs into victim’s online bank account

7. Money transferred to mule

8. Money transferred from mule to organizers

Victims are both financial institutions and owners of infected machines.

Money mules transfer stolen money for criminals, shoving a small percentage for themselves.

Criminals come in many forms:
- Malware coder
- Malware exploiters
- Mule organization

"FBI Fraud Scheme Zeus Trojan" by FBI. Licensed under Public Domain via Wikimedia Commons - http://commons.wikimedia.org/wiki/File:FBI_Fraud_Scheme_Zeus_Trojan.jpg
<table>
<thead>
<tr>
<th>Bin</th>
<th>Card</th>
<th>Debit/Credit</th>
<th>Mark</th>
<th>Expired</th>
<th>Track 1</th>
<th>Code</th>
<th>Country</th>
<th>Bank</th>
<th>Base</th>
<th>Price</th>
<th>Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>651686</td>
<td>MASTERCARD</td>
<td>DEBIT</td>
<td>STANDARD</td>
<td>11/14</td>
<td>Yes</td>
<td>101</td>
<td>United States, MI, GRAND RAPIDS, 49512</td>
<td>CHEMICAL BANK</td>
<td>Tortuga-6</td>
<td>26.6$</td>
<td>+</td>
</tr>
<tr>
<td>414709</td>
<td>VISA</td>
<td>CREDIT</td>
<td>SIGNATURE</td>
<td>02/16</td>
<td>Yes</td>
<td>101</td>
<td>United States, PA, HARRISBURG, 17111</td>
<td>CAPITAL ONE BANK (USA) N.A. Dump or use of this particular bank (BIN) cannot be replaced or refunded</td>
<td>Tortuga-6</td>
<td>39.2$</td>
<td>+</td>
</tr>
<tr>
<td>512107</td>
<td>MASTERCARD</td>
<td>CREDIT</td>
<td>GOLD</td>
<td>02/10</td>
<td>Yes</td>
<td>101</td>
<td>United States, AZ, MESA, 85208</td>
<td>CITIBANK N.A. Dump or use of this particular bank (BIN) cannot be replaced or refunded</td>
<td>Tortuga-6</td>
<td>44.8$</td>
<td>+</td>
</tr>
</tbody>
</table>

http://www.theverge.com/a/anatomy-of-a-hack
Advanced Persistent Threats
## 100+ Targets

Since mid-2013, FIN4 has targeted over 100 organizations, all of which are either publicly traded companies or advisory firms that provide services such as investor relations, legal counsel, and investment banking. Approximately two-thirds of the targeted organizations are healthcare and pharmaceutical companies.

FIN4 knows their targets. Their spearphishing themes appear to be written by native English speakers familiar with both investment terminology and the inner workings of public companies.

FIN4 does not infect their victims with malware, but instead focuses on capturing usernames and passwords to victims’ email accounts, allowing them to view private email correspondence.

FIN4 uses their knowledge to craft convincing phishing lures, most often sent from other victims’ email accounts and through hijacked email threads. These lures appeal to common investor and shareholder concerns, enticing the intended victims into opening the weaponized document and entering their email credentials.

On multiple occasions, FIN4 has targeted several parties involved in a single business deal, to include law firms, consultants, and the public companies involved in negotiations. They also have mechanisms to organize the data they collect and have taken steps to evade detection.

https://www2.fireeye.com/fin4.html
Watering Hole Attacks

http://www.invincea.com/2015/02/chinese-espionage-campaign-compromises-forbes/
THE DARKHOTEL APT ATTACKS

DARK HOTEL

http://securelist.com/blog/research/66779/the-darkhotel-apt/
http://blog.kaspersky.co.uk/darkhotel-apt/

Michael Brunton-Spall
The state of information security
BS7799-1:1999
ISO27001:2005
Accreditation  
Certification  
Approval to operate
PCI
How do we deal with this?
Traditional model
How do we deal with changes?
Agile changes everything
Only do what's needed now
Release It!
MVP and iterate
A security nightmare!
How can we deal with it?
Investigated projects across government
Variety of approaches
... and that's ok
A new world of security
Principles over rules
The UK Government published 8 principles
Accept uncertainty
Security as part of the team
Understand the risks
Trust decision making
Security is part of everything
User experience is important
Audit decisions
Understand big picture impact
But what do they mean?
Let's get practical
National Insurance Claim
User submits their details and claim
Company confirms details via 2\textsuperscript{nd} channel
User gets paid
System is currently paper based for users
mainframe based for staff
This team is going to digitise the service
Embed security on the team
Choose security model that's appropriate
Understand the threats
Hackers break in and steal data from database
Fraudsters submit false claims
Educate decision makers to risks
Make risk decisions on a per story basis
Example
“Allow user to enter bank details to be paid by bank transfer”
Add risk
“Add 2 factor authentication to staff login system”
Counters risk
“Allow user to enter multiple holiday periods”
Risk neutral
What do you do about the risk?
“Allow user to enter bank details to be paid by bank transfer”
Avoid
Don't do it, use cheques instead
Transfer
Use a banking third party
Accept
Just do it
Mitigate
Encrypt bank details on submission using public key cryptography
How much extra work is that?
Accept for now, add a story to backlog to mitigate
Feature flags and feature releases
Risk evaluation
R = Impact * Likelihood
What does it cost to lose data/customers etc
How likely is it to happen
Is the business owner willing to take the risk?
How long for?
What sorts of mitigations might we use?
“Allow user to enter bank details to be paid by bank transfer”
Against hackers stealing the data
“Encrypt the data” - Prevent
“Transaction monitoring” - Detect
“Store data only while session is live” - Compensate
Against fraudsters inputing false data
“Check bank details against claim details” - Detect
“Only pay the same account once a year” - Prevent
“Don't pay until second channel supplies details”
Deter, Prevent, Correct, Recover, Detect, Compensate
Record decision in a log
… probably a wiki
What about big picture impact?
Most information disclosure risks are business process
Can a case worker add/replace bank account details with their own details
... without getting caught?
Can we automate this?
Ideas
Connect the risk log to the story tracker
When a story is played, the risks get updated
It's clear what current risk is
Misuse cases
As a fraudster,
When I submit a fake claim for £1000,
A payment for £1000 gets authorised
Expected to fail
Really fun to write
Define a set of threat actors
External Attacker, Internal Attacker, Insider, Fraudster etc.
Executed like other user acceptance tests
Give confidence that a story hasn't had an impact elsewhere
Gives confidence in business process
Attack Trees
Think as an attacker
Evaluate Risk, Access, Effectiveness
Identify most efficient countermeasures
Use attack trees to pick misuse cases to automate
In summary
We have a duty of care to our users
Choose the right process for you
Apply some basic principles
Dedicate someone to it
Align security and delivery
We're still learning, so let us know if this works for you or not.
Michael Brunton-Spall
Technical Architect
Government Digital Service
@bruntonspall
mbs@digital.cabinet-office.gov.uk