What a shame.....”cry-baby”
Govt bunglers lose 25m names

By ONLINE REPORTERS
Published: 21 Nov 2007

THE Metropolitan Police are now leading the hunt for two computer discs lost by the Government containing highly sensitive personal details of HALF the population.

The news comes as it is revealed that the junior official at the centre of the scandal has been put into a safe house.

The move is thought to help stop him being targeted by organised criminals who might try to get the password to the files from him.

Chancellor Alistair Darling yesterday stunned MPs as he confessed the data included names, addresses, dates of birth, National Insurance numbers — and even bank or building society details.

The discs — containing info on EVERY family receiving Child Benefit — went AWOL after taxmen amazingly sent them to another department 250 miles away by post.
About The Open Web Application Security Project

Guide Table of Contents

Contents [hide]

1 Overview
2 Structure
3 Licensing
4 Participation and Membership
5 Projects
6 OWASP Privacy Policy

Overview

The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security include

[edit]
.com
FINDSTONE

KNOW VULNERABILITIES

Managed Security Services
Professional Services
Education

www.foundstone.com
McAfee to buy Foundstone for US$86 million

PAUL ROBERTS, IDG NEWS SERVICE
17/08/2004 08:20:52

Antivirus software company, McAfee, is buying Foundstone, which makes software for detecting and managing software vulnerabilities, for $US86 million in cash.

The acquisition will add Foundstone’s line of vulnerability management software to McAfee’s growing list of security products. McAfee plans to
VISION OR DELUSION? YOU DECIDE!
(either way hopefully it will be fun)
People solve complex problems

- Smallpox
- Deadliest disease in history
- 1900-1979
  - 500 million victims died
  - 15 million per year in 60s
  - ½ of all blindness in Asia
People solve complex problems

- Smallpox
- Deadliest disease in history
- 1900-2000
  - 500 million victims died
  - 15 million per year in 60s
  - ½ of all blindness in Asia
- WHO campaign to eradicate the disease

Photo: Wikimedia
“Security is not my problem......”
“Security really (really, really, really........) is my problem”
“Security is my problem......but I really don’t care”
1. **Process Matters**
   - Integrated Development Practices
   - Clear Security Requirements
   - Measurement of Success

2. **Technology Matters**
   - Security Features / API’s (right tool for the job)
   - Tools are critical. People Don’t Scale!
   - Architecture is Not a Dirty Word
   - Purple Dinosaurs are Everywhere

3. **People Matter**
#1 – Adopt Chinese Medicine Business Model
#2 – Stop Human Pattern Matching
How many pencils are there in this picture?
How many pencils are there in this picture?
How many pencils are there in this picture?
If you are still not convinced?
To Be Clear Computers Pattern Match (Some Things) Very Well!
# 3 Community Driven Statistical Modeling
Wine Quality = 12.145 + .00117 * winter rainfall + .0614 average growing season - .00386 harvest rainfall

Where is the security equivalent?
\[ \Pr[T_A < 1, T_B < 1] = \phi_2(\phi^{-1}(F_A(1)), \phi^{-1}(F_B(1)), \gamma) \]
Security is a function of

$$S = f(\text{\textdegree WFF})$$
Degrees of Warm Fuzzy Feeling

$$S = f(p,d) + R_n$$
Prayer, Denial) + Number of Days till Retirement

$$S = f(n)$$
Where $n$ is the number of security guys you know

$$S = f(1/n)$$
Where $n$ is the number of security standards documents you have read
# 4 – Teach Kids Computer Security

![Image of a child using a computer]

Lesson 1B
Saying

Click on the name of your program **Asking** to go back to editing it. We’re going to do something else with that name.

Here’s the new program (the first 2 lines are the same):

```plaintext
# Asking and saying
name = ask("Your name please?")
say("Your name is \{name.length\} letters long")
sleep(name.length())
```

Type this one in carefully. You’ll notice in the quotes that there is a little number sign and some curly braces. The curly braces are right above your square bracket keys (on a US keyboard.)

---

Asking and Saying

A blank program, started on May 31th, 2007 at 11:26 PM.

```plaintext
1 # Asking and saying
2 name = ask("Your name please?")
3 say("Your name is \{name.length\} letters long")
4 sleep(name.length())
5 6 7
```
#5 Make Developing Countries Centers for Security Excellence
Make Me Stop and Take a Photo of The Audience
# 6 – Make Hacking a Competitive Sport

<table>
<thead>
<tr>
<th>Country</th>
<th>Players Entered</th>
<th>Players Remaining</th>
<th>Wins/Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russia</td>
<td>23</td>
<td>0</td>
<td>30 / 23</td>
</tr>
<tr>
<td>Spain</td>
<td>20</td>
<td>1</td>
<td>27 / 19</td>
</tr>
<tr>
<td>Denmark</td>
<td>1</td>
<td>0</td>
<td>4 / 1</td>
</tr>
<tr>
<td>Serbia</td>
<td>5</td>
<td>0</td>
<td>12 / 5</td>
</tr>
<tr>
<td>Australia</td>
<td>9</td>
<td>0</td>
<td>15 / 9</td>
</tr>
<tr>
<td>Sweden</td>
<td>3</td>
<td>0</td>
<td>7 / 3</td>
</tr>
<tr>
<td>Italy</td>
<td>13</td>
<td>1</td>
<td>16 / 12</td>
</tr>
<tr>
<td>Switzerland</td>
<td>6</td>
<td>0</td>
<td>9 / 6</td>
</tr>
<tr>
<td>Cyprus</td>
<td>1</td>
<td>0</td>
<td>2 / 1</td>
</tr>
<tr>
<td>United States of America</td>
<td>20</td>
<td>0</td>
<td>19 / 20</td>
</tr>
</tbody>
</table>
# 7 – Connected Information Security Framework
#8- Embrace Design Driven Security

“We must reward the builders and the breakers”
#9 Crowd Source Access Control
Adopt Agile Mindset

#10 Adopt Agile Mindset
The Agile Manifesto - http://agilemanifesto.org/

<table>
<thead>
<tr>
<th>New thinking</th>
<th>versus</th>
<th>old thinking</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals and interactions</td>
<td>over</td>
<td>processes and tools</td>
</tr>
<tr>
<td>Working software</td>
<td>over</td>
<td>comprehensive documentation</td>
</tr>
<tr>
<td>Customer collaboration</td>
<td>over</td>
<td>contract negotiation</td>
</tr>
<tr>
<td>Responding to change</td>
<td>over</td>
<td>following a plan</td>
</tr>
</tbody>
</table>

“That is, while there is value in the items on the right, we value the items on the left more.”
“By embracing constraints you can do the most important half of a job, rather than a half-assed job”
The Ralph Stacey Diagram

- Complexity
- Certainty
- Predictable
- Simple
- Complex
- Chaotic

“Information Security”

“The Ralph Stacey Diagram”
The Truth About Estimation

Accurate Estimate

Understanding & Accuracy

Issue A

Issue B

Issue C

Big Range

Accurate Estimate
Common Statement: “But Agile is not for the Enterprise.”

Factual Answer: “Enterprise? – A colossal spaceship from the 80’s flown by people with bad taste: Highly advanced, but purely fictional”
10 Crazy Ideas That Might Just Change the State of the Security Industry

# 1 – Adopt the Chinese Medicine Business Model
# 2 – Stop Human Pattern Matching
# 3 – Community Driven Statistical Modeling
# 4 – Teach Kids Security
# 5 – Make Developing Countries Security COE’s
# 6 – Make Hacking a Competitive Sport
# 7 – Build a Connected Information Security Framework
# 8 – Design Driven Security
# 9 – Crowd Source Access Control
# 10 – Adopt Agile Methodologies
It doesn’t have to be this hard!