Securing the DSS

A Government perspective on the need for a secure IT infrastructure

David Blair
Department of Social Security
d_blair@msn.com
Scale of DSS Operation

1996/1997

DSS
- Money collected: £47 billion
- Money Out: £89 billion
- 24 hours/day
- 364 days/year

ITSA
- Annual Budget: £348 million
- Over 70% external

Over 2,000 locations throughout Great Britain & Northern Ireland
### Our Key Customers

<table>
<thead>
<tr>
<th>Agency</th>
<th>Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benefits Agency</td>
<td>65,000</td>
</tr>
<tr>
<td>Contributions Agency</td>
<td>10,000</td>
</tr>
<tr>
<td>Child Support Agency</td>
<td>6,200</td>
</tr>
<tr>
<td>ITSA</td>
<td>2,200</td>
</tr>
<tr>
<td>DHSS Northern Ireland</td>
<td>7,500</td>
</tr>
</tbody>
</table>

**TOTAL approx 91,000**

### Number of recipients: 1995/6

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Recipients</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retirement Pension</td>
<td>10,167,000</td>
</tr>
<tr>
<td>Child Benefit</td>
<td>6,995,000</td>
</tr>
<tr>
<td>Income Support</td>
<td>5,675,000</td>
</tr>
<tr>
<td>Sickness &amp; Invalidity Benefit</td>
<td>1,812,000</td>
</tr>
<tr>
<td>Attendance Allowance</td>
<td>996,000</td>
</tr>
<tr>
<td>One Parent Benefit</td>
<td>941,000</td>
</tr>
<tr>
<td>Unemployment Benefit</td>
<td>458,000</td>
</tr>
<tr>
<td>War Pension</td>
<td>309,000</td>
</tr>
<tr>
<td>Others</td>
<td>2,735,300</td>
</tr>
</tbody>
</table>

**Plus over 55 million National Insurance contributors**
DSS computing

ICL & IBM Mainframes

Proprietary minis

Gateways and firewalls

Communications Network

ICL & IBM Mainframes

Proprietary minis

Government Secure Intranet
Service Providers, etc

Novell

Office Network Server

PC

PC

PC

XPG3 based

STAP Server

Dumb Terminal

PC

PC

XPG4 based

Multi-Function Server

PC

PC

PC

to be secured

Department of Social Security - ITSA
Source of security requirements

- Highest level set by HMG
  - mostly based on CESG Memos 5, 10 and 13
  - plus advice from the security services
- DSS business requirements plus HMG advice informs
  - Community security policy
  - System Security Policies
  - where necessary standard(s) and product selection
In addition

Today’s problems and issues:

• Issues
  • IT systems offer limited security functionality
  • Functionality is intricate and sensitive to change
  • Products not available to satisfy all requirements

• Problem has grown as:
  • PCs become pervasive
  • Networking more widespread
  • Multi-tier architectures became the norm
  • We offer services direct to the citizen
Each system has its own security mechanisms

For administrators and users that can mean many different views of the Information System
Sector as a whole

• A number of Government IT users have attempted to produce an agreed prioritised statement of security requirements

• List of requirements that follows is actually based on an ESF list and Departmental IT Security Officer views.

• I'll give an update on where DSS have got to

Note:- excludes defense and security forces
**Enterprise requirements**

- Single Sign-On from anywhere in the enterprise
- Simplified administration and operation of security features
- Secure networking
- Perimeter Security
- Unique user ID
Enterprise requirements (2)

- Control of access privilege by user ID, token and/or role
- Minimal impact on performance
- Greater standardisation (as a minimum - standard products available from multiple sources)
- Secure audit trails and logs
Enterprise requirements (3)

- Secure System Interoperability
- Virus detection
- Error avoidance and recovery as a feature
- Improved file, program and record locking
- Ideally - available out of the box
Need for a component based model

Administration of users

Audit

Administration of services

Security server

Security & welcome at the terminal or PC

Security customisation tools
What it means for DSS

- one secure log-on:
  - across administrative domains
  - across heterogeneous system environments
  - regardless of location
  - with ability to synchronise password changes

Savings for users and administrators
Single Sign-On

SSO-APIs

GSS-APIs

ID1/PW1

ID2/PW2

DSS1 Blackpool

Legacy Systems Mainframe Systems

New - yet to be deployed Distributed Applications

Department of Social Security - ITSA
Secure Networking

• The security of many systems are unacceptably compromised when linked to a network. We are attempting to implement:-
  • common approach to local and wide area networking
  • secure file sharing
  • firewall capabilities (at appropriate level ie ITSEC 3)
  • availability and integrity as well as confidentiality
Threats over an insecure network

Line taps
Masquerades
Unauthorized access to resources
Message replay
Message alteration
Management of users

- Offer coherent and global security management
- Hide the differences between systems
- Ease the work of the security administrators
- Provide a complete management system with:
  - tools for managing the customers organisation
  - user registration to services by authorised administrators
  - coherent management of users and systems
  - automatic updating of target systems

In effect we want single hit user management but we are still a long way off
Access Controls and User ID

- Control of access privileges by user ID and token
- Recognition of security breaches
- Greater precision and flexibility's than has been the case in UNIX, Mainframes etc.
- Enforcement of individual accountability
- Access based on role e.g. reflecting organisational structures
- Expandable to cater for external links
A security product must not seriously degrade performance when key features are turned on, e.g.:-

- audit logs
- access controls
- role allocation / modification
- cryptography services

One audit trail analysis system we piloted would have needed 6 additional mainframes
Greater Standardisation

- The variation between systems weakens and/or drives up the cost of security
- Government wants a standardised set of security features which function in a standard way
- We don’t want application developers doing their own thing. They should rely on the underlying security systems
- We don't want to invest in Government bespoke solutions
Challenges and issues

• How do we extend connectivity beyond our Virtual Private Networks such as GDN and GSI
• Very limited pilot across Government of digital signature (Iforms) - how do we ensure scalability
• For DSS identity is major issue - how do we verify identity without resorting to a Government or DSS identity card
• Political issues - smartcards, PKI, civil liberties etc
Mandates for Infrastructure / Product

- Meets HMG requirements
- Modular architecture
- Meets DSS (and industry) wish list
  - single sign-on in line with standards
  - role / group access
  - one hit user management
  - enhances network security
  - modular, flexible, easy to use, etc.....
DSS conclusions

- Ideally wouldn’t need to buy separate security product(s), reality is we do
- Therefore;
  - need standards
  - product which meets requirements
  - interoperability between products / providers
  - infrastructure provided by industry