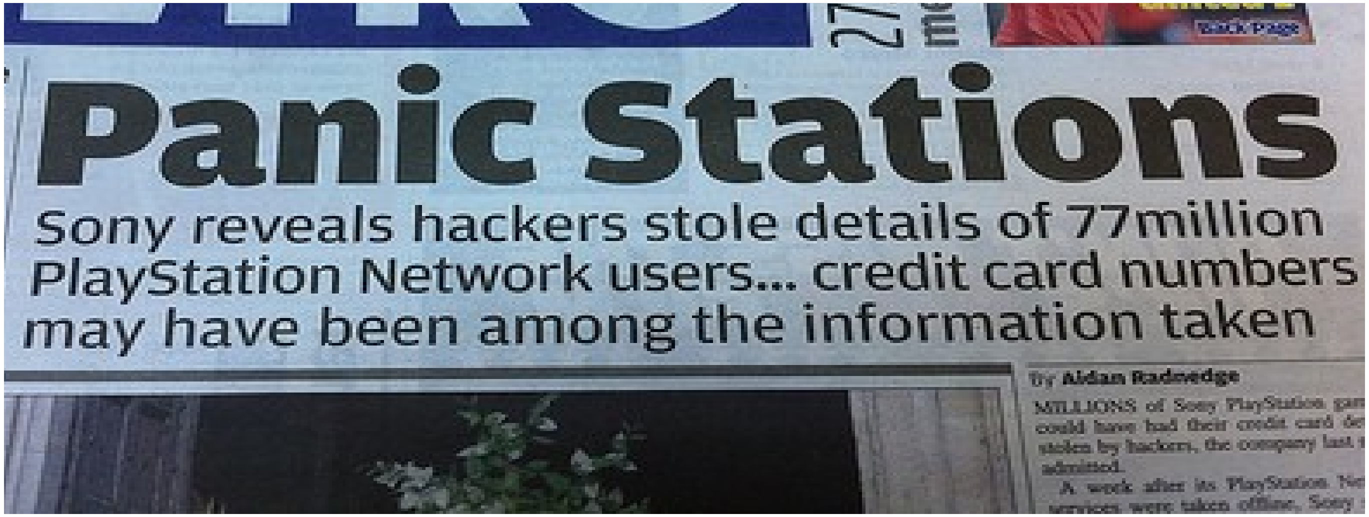
Securing Public Webservers: Why and How

Oxford University
Computer Emergency Response Team
and
Information Security Best Practice

David Ford, Mark Duller

14 July 2011

High-Profile Compromises



Panic Stations

Sony reveals hackers stole details of 77million PlayStation Network users... credit card numbers may have been among the information taken

By Aidan Radnedge

MILLIONS of Sony PlayStation gam
could have had their credit card de
stolen by hackers, the company last n
admitted.

A week after its PlayStation Ne
services were taken offline, Sony

name, birthdate, addresses, purchase history, usernames/passwords, security answers, possibly credit cards...

http://www.flickr.com/photos/ludens/5660651348/

High-Profile Compromises

- PSN down for 23 days
- Many other Sony sites hacked
- Simple attacks - mainly SQL injections (SQLi)
- Attack tools widely available (sourceforge etc.)
- Damaged reputation
- Simple security measures could have prevented it

Real Cases from Oxford University

- 25 webserver incidents in the past 3 months
  - 12 compromised via SQL injection
  - 13 vulnerable to SQLi – was just a matter of time
- 2179 SQL injection queries detected in the past 3 months from 108 external IPs targeting 52 webservers
  - only from one type of SQLi attack (Havij)
  - can't detect https or POST

What are the risks?

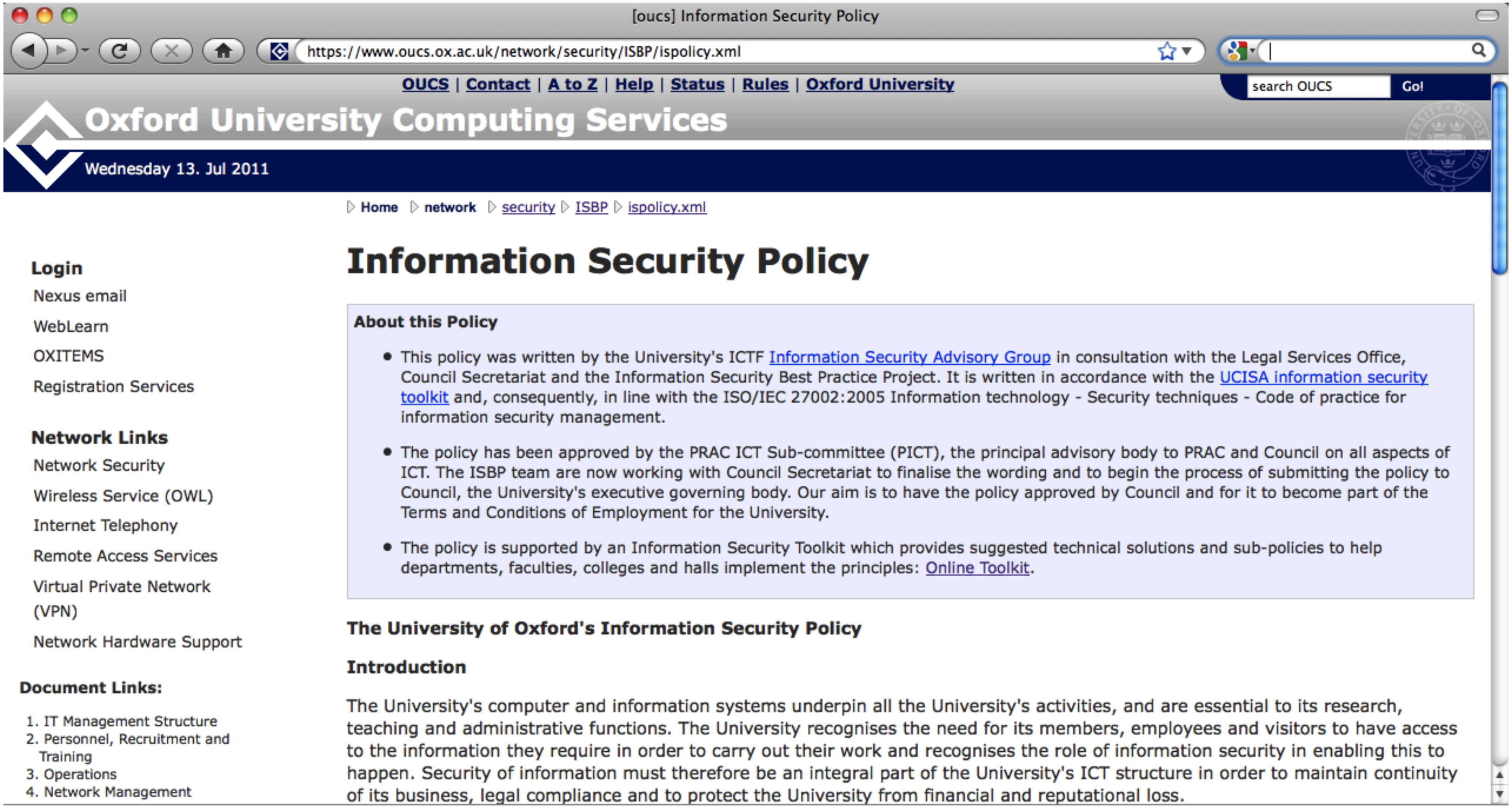
- Confidentiality, Integrity, Availability (CIA)
  - Data leaks
  - Defacements
  - Downtime
- Firefighting
- Reputation
- Monetary fines from Information Commissioner’s Office (ICO)
- Further compromises on network

Information Security Best Practice

how it can help

- An exercise in risk management
- Policies
  - Help identify and address the risks
  - Tell ***what*** to do
- Toolkit
  - Provides guidance on policies
  - Tells ***how*** to do it
  - Includes specific technical examples

Policies Relating to Webservers


[oucs] Information Security Policy
https://www.oucs.ox.ac.uk/network/security/ISBP/ispolicy.xml
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Wednesday 13. Jul 2011
Home network security ISBP ispolicy.xml

Login

Nexus email

WebLearn

OXITEMS

Registration Services

Network Links

Network Security

Wireless Service (OWL)

Internet Telephony

Remote Access Services

Virtual Private Network (VPN)

Network Hardware Support

Document Links:

1. IT Management Structure
2. Personnel, Recruitment and Training
3. Operations
4. Network Management

Information Security Policy

About this Policy

- This policy was written by the University's ICTF Information Security Advisory Group in consultation with the Legal Services Office, Council Secretariat and the Information Security Best Practice Project. It is written in accordance with the UCISA information security toolkit and, consequently, in line with the ISO/IEC 27002:2005 Information technology - Security techniques - Code of practice for information security management.
- The policy has been approved by the PRAC ICT Sub-committee (PICT), the principal advisory body to PRAC and Council on all aspects of ICT. The ISBP team are now working with Council Secretariat to finalise the wording and to begin the process of submitting the policy to Council, the University's executive governing body. Our aim is to have the policy approved by Council and for it to become part of the Terms and Conditions of Employment for the University.
- The policy is supported by an Information Security Toolkit which provides suggested technical solutions and sub-policies to help departments, faculties, colleges and halls implement the principles: Online Toolkit.

The University of Oxford's Information Security Policy

Introduction

The University's computer and information systems underpin all the University's activities, and are essential to its research, teaching and administrative functions. The University recognises the need for its members, employees and visitors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this to happen. Security of information must therefore be an integral part of the University's ICT structure in order to maintain continuity of its business, legal compliance and to protect the University from financial and reputational loss.

Policies Relating to Webservers

Subsidiary policies:

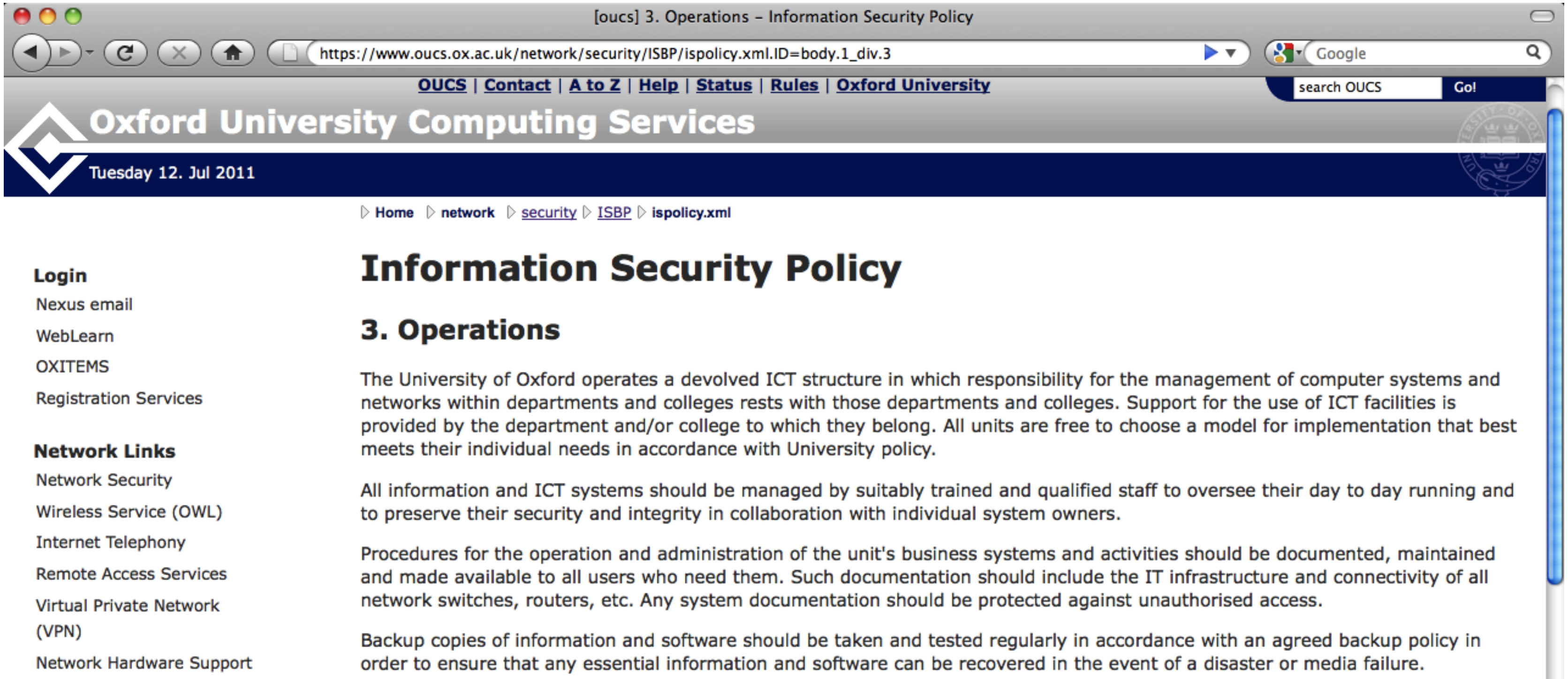
1. IT Management Structure
2. Personnel, Recruitment and Training
3. Operations
4. Network Management
5. Access Control
6. User Management
7. Information Handling
8. Physical and Environmental Security
9. Incident Handling
10. Business Continuity Planning
11. Compliance

Policies Relating to Webservers

- Trained and Qualified Staff
- Documentation
- Logging
- Access Restrictions
- Permissions and Process Privileges
- Controls to Protect against Malicious Code

Policy on Documentation

- Documentation should be:
  - created
  - maintained
  - made available to users who need them



[oucs] 3. Operations – Information Security Policy
https://www.oucs.ox.ac.uk/network/security/ISBP/ispolicy.xml.ID=body.1_div.3
Google
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Tuesday 12. Jul 2011
Home network security ISBP ispolicy.xml
Login
Nexus email
WebLearn
OXITEMS
Registration Services
Network Links
Network Security
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)
Network Hardware Support

Information Security Policy

3. Operations

The University of Oxford operates a devolved ICT structure in which responsibility for the management of computer systems and networks within departments and colleges rests with those departments and colleges. Support for the use of ICT facilities is provided by the department and/or college to which they belong. All units are free to choose a model for implementation that best meets their individual needs in accordance with University policy.

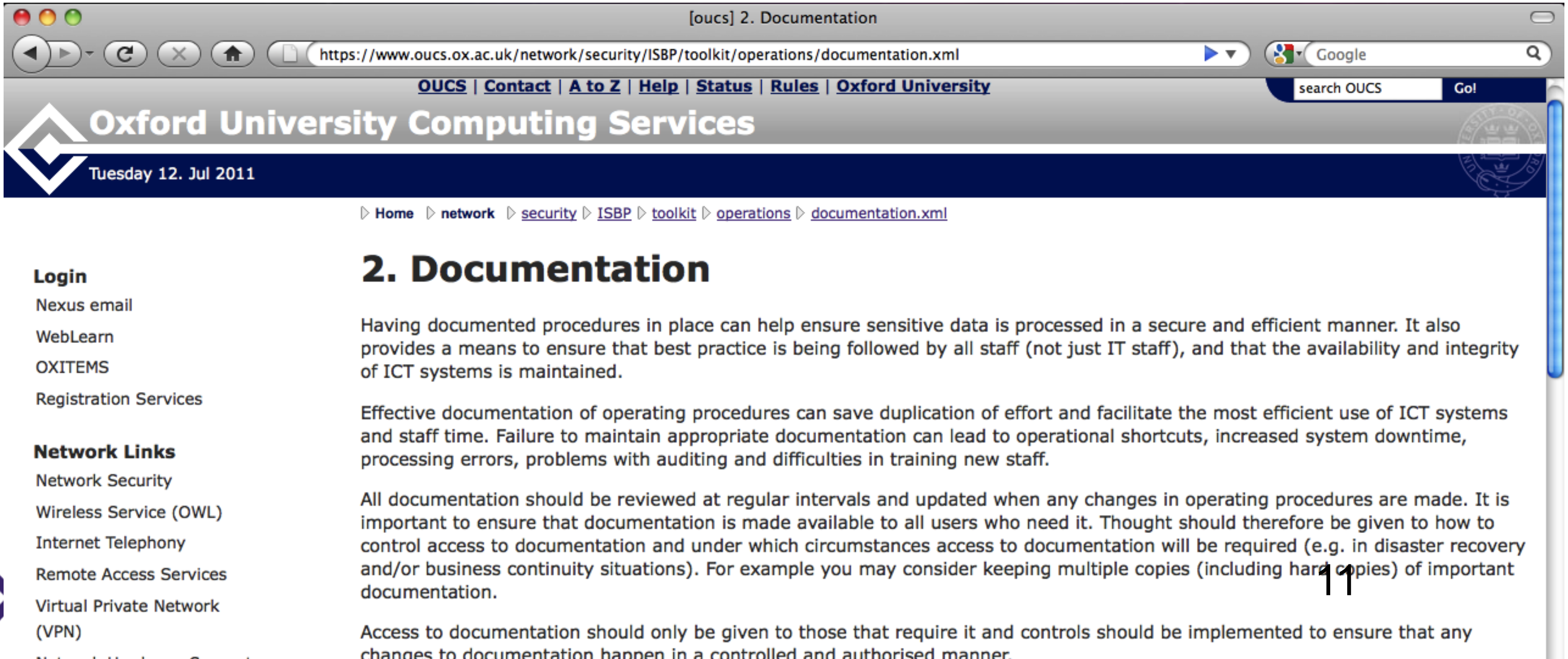
All information and ICT systems should be managed by suitably trained and qualified staff to oversee their day to day running and to preserve their security and integrity in collaboration with individual system owners.

Procedures for the operation and administration of the unit's business systems and activities should be documented, maintained and made available to all users who need them. Such documentation should include the IT infrastructure and connectivity of all network switches, routers, etc. Any system documentation should be protected against unauthorised access.

Backup copies of information and software should be taken and tested regularly in accordance with an agreed backup policy in order to ensure that any essential information and software can be recovered in the event of a disaster or media failure.

Toolkit on Documentation

- Network connectivity
- Computer operations
- Error/Incident handling
- Audit trails and system logs
- System capacity
- Software and services
- Change control


[oucs] 2. Documentation
https://www.oucs.ox.ac.uk/network/security/ISBP/toolkit/operations/documentation.xml
Google
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Tuesday 12. Jul 2011
Home ▷ network ▷ security ▷ ISBP ▷ toolkit ▷ operations ▷ documentation.xml
Login
Nexus email
WebLearn
OXITEMS
Registration Services
Network Links
Network Security
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network (VPN)

2. Documentation

Having documented procedures in place can help ensure sensitive data is processed in a secure and efficient manner. It also provides a means to ensure that best practice is being followed by all staff (not just IT staff), and that the availability and integrity of ICT systems is maintained.

Effective documentation of operating procedures can save duplication of effort and facilitate the most efficient use of ICT systems and staff time. Failure to maintain appropriate documentation can lead to operational shortcuts, increased system downtime, processing errors, problems with auditing and difficulties in training new staff.

All documentation should be reviewed at regular intervals and updated when any changes in operating procedures are made. It is important to ensure that documentation is made available to all users who need it. Thought should therefore be given to how to control access to documentation and under which circumstances access to documentation will be required (e.g. in disaster recovery and/or business continuity situations). For example you may consider keeping multiple copies (including hard copies) of important documentation.

Access to documentation should only be given to those that require it and controls should be implemented to ensure that any changes to documentation happen in a controlled and authorised manner.

Toolkit on Documentation

Example Solutions

- Wikis
  - Moinmoin, Mediawiki, TWiki...
- SharePoint
  - Nexus, WSS
- File based
  - SVN, CVS, RCS...

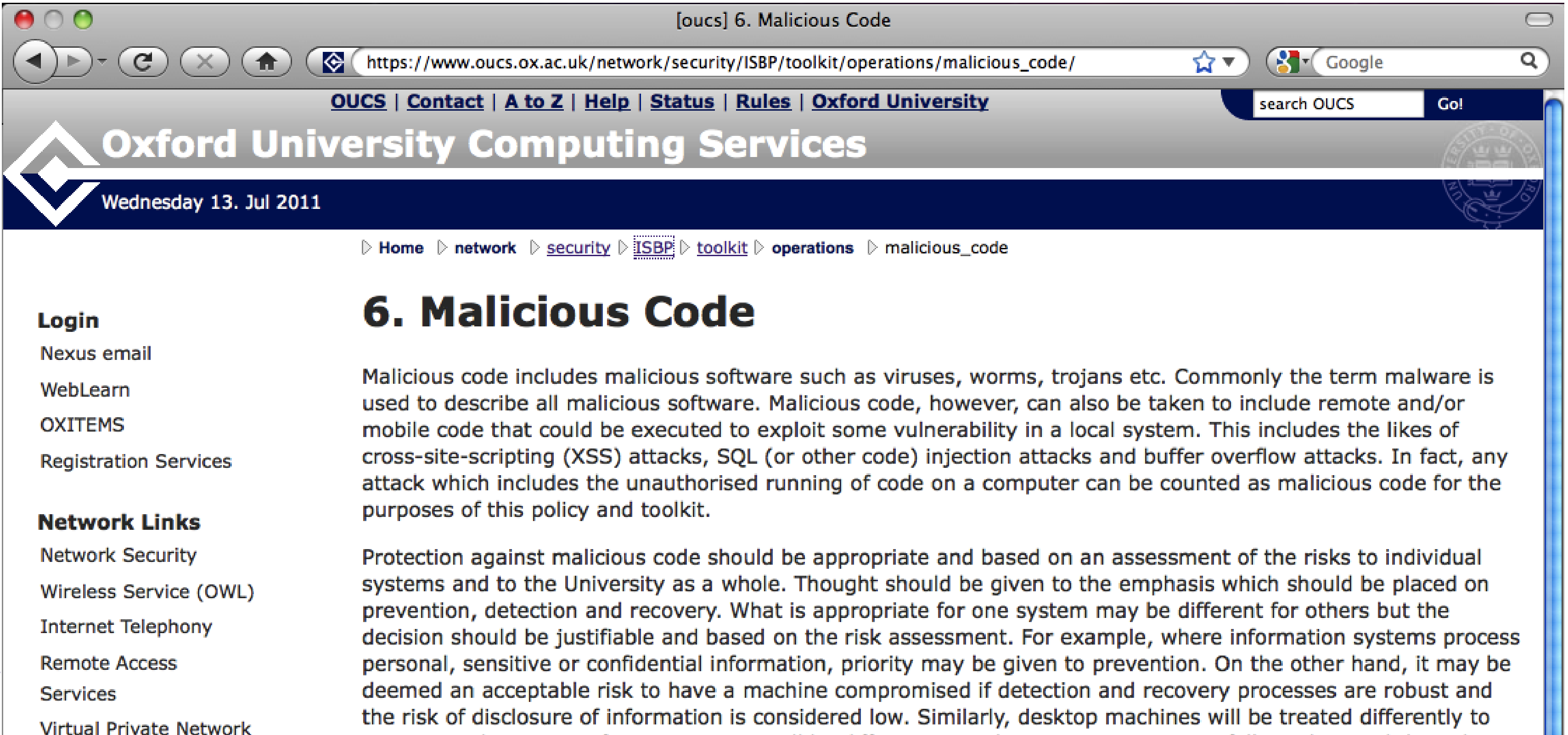
Policy on Malicious Code

- Protect against malicious code
  - Detection
  - Prevention
  - recovery

Toolkit on Malicious Code

Malicious Code Includes

- Cross-site-scripting (XSS)
- SQL (or other code) injection attacks
- buffer overflow attacks


[oucs] 6. Malicious Code
https://www.oucs.ox.ac.uk/network/security/ISBP/toolkit/operations/malicious_code/
Google
OUCS | Contact | A to Z | Help | Status | Rules | Oxford University
search OUCS
Go!
Oxford University Computing Services
Wednesday 13. Jul 2011
Home ▷ network ▷ security ▷ ISBP ▷ toolkit ▷ operations ▷ malicious_code
Login
Nexus email
WebLearn
OXITEMS
Registration Services
Network Links
Network Security
Wireless Service (OWL)
Internet Telephony
Remote Access Services
Virtual Private Network

6. Malicious Code

Malicious code includes malicious software such as viruses, worms, trojans etc. Commonly the term malware is used to describe all malicious software. Malicious code, however, can also be taken to include remote and/or mobile code that could be executed to exploit some vulnerability in a local system. This includes the likes of cross-site-scripting (XSS) attacks, SQL (or other code) injection attacks and buffer overflow attacks. In fact, any attack which includes the unauthorised running of code on a computer can be counted as malicious code for the purposes of this policy and toolkit.

Protection against malicious code should be appropriate and based on an assessment of the risks to individual systems and to the University as a whole. Thought should be given to the emphasis which should be placed on prevention, detection and recovery. What is appropriate for one system may be different for others but the decision should be justifiable and based on the risk assessment. For example, where information systems process personal, sensitive or confidential information, priority may be given to prevention. On the other hand, it may be deemed an acceptable risk to have a machine compromised if detection and recovery processes are robust and the risk of disclosure of information is considered low. Similarly, desktop machines will be treated differently to

Oxford University Computing Services

Toolkit on Malicious Code

Example Solutions

How to prevent SQL injection attacks?
Next speaker: David Ford