Cyberpatterns workshop

The Cosener's House, Abingdon
9/10 July 2012

Sponsored by Oxford Brookes University and SOPHOS

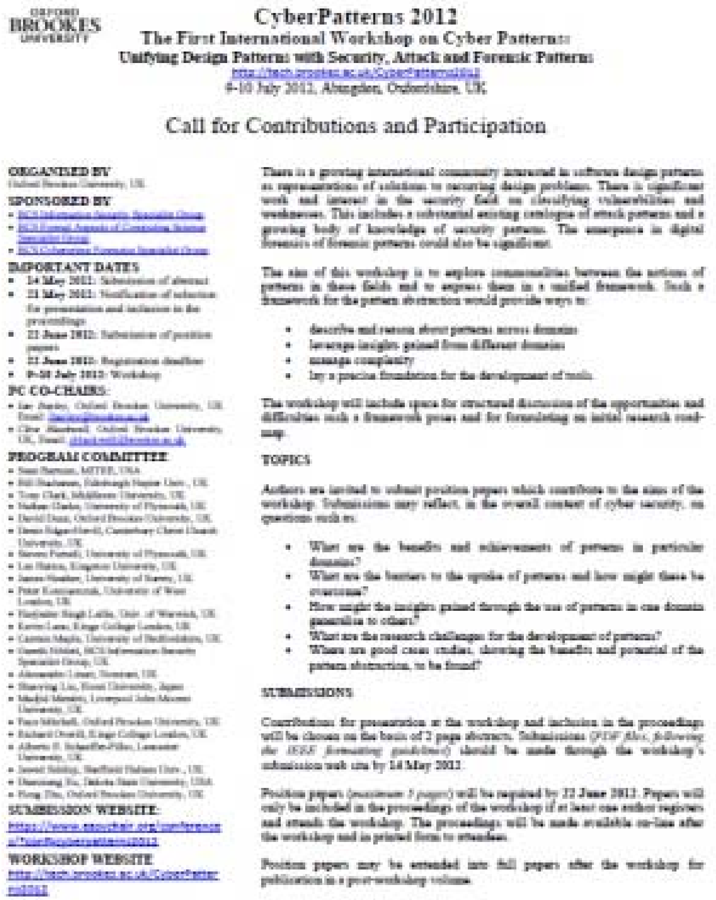
Ian Bayley, Clive Blackwell, David Duce, Hong Zhu

Oxford Brookes University

The First International Workshop on Cyber Patterns

- Unifying Design Patterns with Security, Attack and Forensic Patterns

- There is a growing international community interested in software design patterns as representations of solutions to recurring design problems.
- There is significant work and interest in the security field on classifying vulnerabilities and weaknesses.
- This includes a substantial existing catalogue of attack patterns and a growing body of knowledge of security patterns.
- The emergence in digital forensics of forensic patterns could also be significant.



OXFORD BROOKES UNIVERSITY

CyberPatterns 2012

The First International Workshop on Cyber Patterns:

Unifying Design Patterns with Security, Attack and Forensic Patterns

http://tech.brookes.ac.uk/CyberPatterns2012

9-10 July 2012, Abingdon, Oxfordshire, UK

Call for Contributions and Participation

ORGANISED BY

Oxford Brookes University, UK

SPONSORED BY

- BCS Information Security Specialist Group
- BCS Formal Aspects of Computing Science Specialist Group
- BCS Cybercrime Forensics Specialist Group

IMPORTANT DATES

- **14 May 2012:** Submission of abstract
- **21 May 2012:** Notification of selection for presentation and inclusion in the proceedings
- **22 June 2012:** Submission of position papers
- **22 June 2012:** Registration deadline
- **9-10 July 2012:** Workshop

PC CO-CHAIRS:

- Ian Bayley, Oxford Brookes University, UK, Email: ibayley@brookes.ac.uk
- Clive Blackwell, Oxford Brookes University, UK, Email: cblackwell@brookes.ac.uk

PROGRAM COMMITTEE

- Sean Barnum, MITRE, USA
- Bill Buchanan, Edinburgh Napier Univ., UK
- Tony Clark, Middlesex University, UK
- Nathan Clarke, University of Plymouth, UK
- David Duce, Oxford Brookes University, UK
- Denis Edgar-Nevill, Canterbury Christ Church University, UK
- Steven Furnell, University of Plymouth, UK
- Les Hatton, Kingston University, UK
- James Heather, University of Surrey, UK
- Peter Komisarczuk, University of West London, UK
- Harjinder Singh Lallie, Univ. of Warwick, UK
- Kevin Lano, Kings College London, UK
- Carsten Maple, University of Bedfordshire, UK
- Gareth Niblett, BCS Information Security Specialist Group, UK
- Alexander [illegible], Siemens, UK
- Shaoying Liu, Hosei University, Japan
- Madjid Merabti, Liverpool John Moores University, UK
- Faye Mitchell, Oxford Brookes University, UK
- Richard Overill, Kings College London, UK
- Alberto E. Schaeffer-Filho, Lancaster University, UK
- Jawed Siddiqi, Sheffield Hallam Univ., UK
- Dianxiang Xu, Dakota State University, USA
- Hong Zhu, Oxford Brookes University, UK

SUBMISSION WEBSITE:

https://www.easychair.org/conferences/?conf=cyberpatterns2012

WORKSHOP WEBSITE

http://tech.brookes.ac.uk/CyberPatterns2012

There is a growing international community interested in software design patterns as representations of solutions to recurring design problems. There is significant work and interest in the security field on classifying vulnerabilities and weaknesses. This includes a substantial existing catalogue of attack patterns and a growing body of knowledge of security patterns. The emergence in digital forensics of forensic patterns could also be significant.

The aim of this workshop is to explore commonalities between the notions of patterns in these fields and to express them in a unified framework. Such a framework for the pattern abstraction would provide ways to:

- describe and reason about patterns across domains
- leverage insights gained from different domains
- manage complexity
- lay a precise foundation for the development of tools.

The workshop will include space for structured discussion of the opportunities and difficulties such a framework poses and for formulating an initial research road-map.

TOPICS

Authors are invited to submit position papers which contribute to the aims of the workshop. Submissions may reflect, in the overall context of cyber security, on questions such as:

- What are the benefits and achievements of patterns in particular domains?
- What are the barriers to the uptake of patterns and how might these be overcome?
- How might the insights gained through the use of patterns in one domain generalise to others?
- What are the research challenges for the development of patterns?
- Where are good case studies, showing the benefits and potential of the pattern abstraction, to be found?

SUBMISSIONS

Contributions for presentation at the workshop and inclusion in the proceedings will be chosen on the basis of 2 page abstracts. Submissions (*PDF files, following the IEEE formatting guidelines*) should be made through the workshop's submission web site by 14 May 2012.

Position papers (*maximum 5 pages*) will be required by 22 June 2012. Papers will only be included in the proceedings of the workshop if at least one author registers and attends the workshop. The proceedings will be made available on-line after the workshop and in printed form to attendees.

Position papers may be extended into full papers after the workshop for publication in a post-workshop volume.

Aims [as Call for Papers]

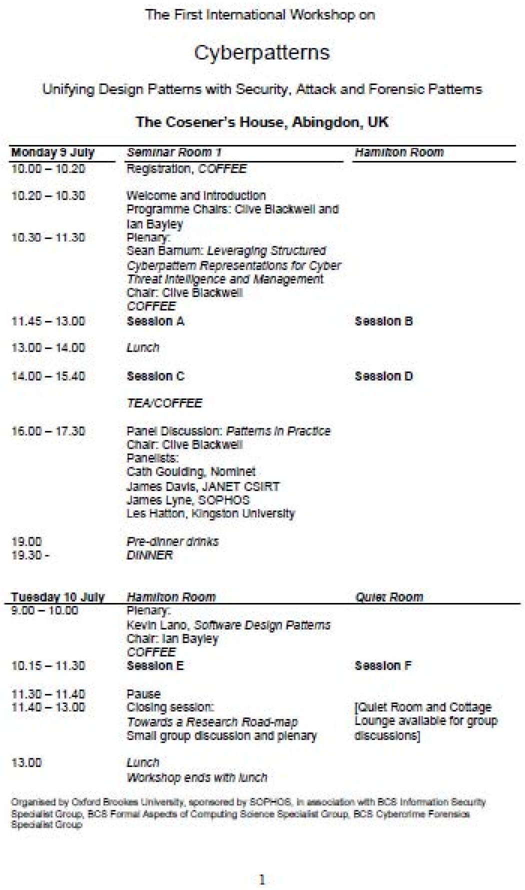
- The aim of this workshop is to explore commonalities between the notions of patterns in these fields and to express them in a unified framework. Such a framework for the pattern abstraction would provide ways to:
  - describe and reason about patterns across domains
  - leverage insights gained from different domains
  - manage complexity
  - lay a precise foundation for the development of tools.
- The workshop will include space for structured discussion of the opportunities and difficulties such a framework poses and for formulating an initial research road-map.

Topics (from Call for Papers)

- What are the benefits and achievements of patterns in particular domains?
- What are the barriers to the uptake of patterns and how might these be overcome?
- How might the insights gained through the use of patterns in one domain generalise to others?
- What are the research challenges for the development of patterns?
- Where are good cases studies, showing the benefits and potential of the pattern abstraction, to be found?

Programme

- ca. 35 participants, 19 accepted papers
- Universities
  - Abertay
  - Dartmouth College
  - Glasgow
  - KCL
  - Kingston
  - Lancaster
  - Liverpool John Moores
  - Newcastle
  - Oxford
  - Oxford Brookes
  - UCL
  - Warwick
  - West London
- Industry, government
  - Auroa Consulting
  - BT
  - CESG
  - Janet CSIRT
  - Mitre Corporation
  - Nominet
  - Sophos



The First International Workshop on

Cyberpatterns

Unifying Design Patterns with Security, Attack and Forensic Patterns

The Cosener's House, Abingdon, UK

Monday 9 July	*Seminar Room 1*	*Hamilton Room*
10.00 – 10.20	Registration, *COFFEE*	
10.20 – 10.30	Welcome and Introduction Programme Chairs: Clive Blackwell and Ian Bayley	
10.30 – 11.30	Plenary: Sean Barnum: *Leveraging Structured Cyberpattern Representations for Cyber Threat Intelligence and Management* Chair: Clive Blackwell *COFFEE*	
11.45 – 13.00	**Session A**	**Session B**
13.00 – 14.00	*Lunch*	
14.00 – 15.40	**Session C**	**Session D**
	TEA/COFFEE	
16.00 – 17.30	Panel Discussion: *Patterns in Practice* Chair: Clive Blackwell Panelists: Cath Goulding, Nominet James Davis, JANET CSIRT James Lyne, SOPHOS Les Hatton, Kingston University	
19.00	*Pre-dinner drinks*	
19.30 -	*DINNER*	

Tuesday 10 July	*Hamilton Room*	*Quiet Room*
9.00 – 10.00	Plenary: Kevin Lano, *Software Design Patterns* Chair: Ian Bayley *COFFEE*	
10.15 – 11.30	**Session E**	**Session F**
11.30 – 11.40	Pause	
11.40 – 13.00	Closing session: *Towards a Research Road-map* Small group discussion and plenary	[Quiet Room and Cottage Lounge available for group discussions]
13.00	*Lunch* *Workshop ends with lunch*	

Organised by Oxford Brookes University, sponsored by SOPHOS, in association with BCS Information Security Specialist Group, BCS Formal Aspects of Computing Science Specialist Group, BCS Cybercrime Forensics Specialist Group

1

Sean Barnum - invited paper

- *Sean Barnum*: Leveraging Structured Cyberpattern Representations for Cyber Threat Intelligence and Management
  - Cyber Security Principal at Mitre Corporation
- Patterns “repetitive commonality of characteristics”
- Prescriptive vs descriptive patterns
  - Prescriptive provide context and guidance; apply to solve a problem
  - Descriptive capture characteristics, enable search and recognition
- Patterns, anti-patterns, remediation patterns to rectify anti-patterns
- Need for standardisation of representations
- Talked in detail about attack patterns, patterns in attackers’ behaviours; many classification schemes in development
- Need for formalisation, more solid foundations, verbal descriptions unclear

Panel session – Patterns in Practice

- Chair: Clive Blackwell, Oxford Brookes
- Sean Barnum, Mitre Corporation
- James Davis, JANET CSIRT
- Cath Goulding, Nominet
- Graeme Hickman (Sophos)
- Les Hatton, Kingston University

- Started with opening remarks from each on state of the art of pattern usage in their practices

- Discussion
  - What are patterns?
  - Discussion of prescriptive/descriptive categories (and alternative
  - Importance of patterns in many industry sectors, even if practitioners do not use the language of patterns
  - There is more to recognising attacks than recognising byte strings, emergence and application of patterns of behaviour
  - More general notion of pattern in socio-technical systems

Kevin Lano – invited paper

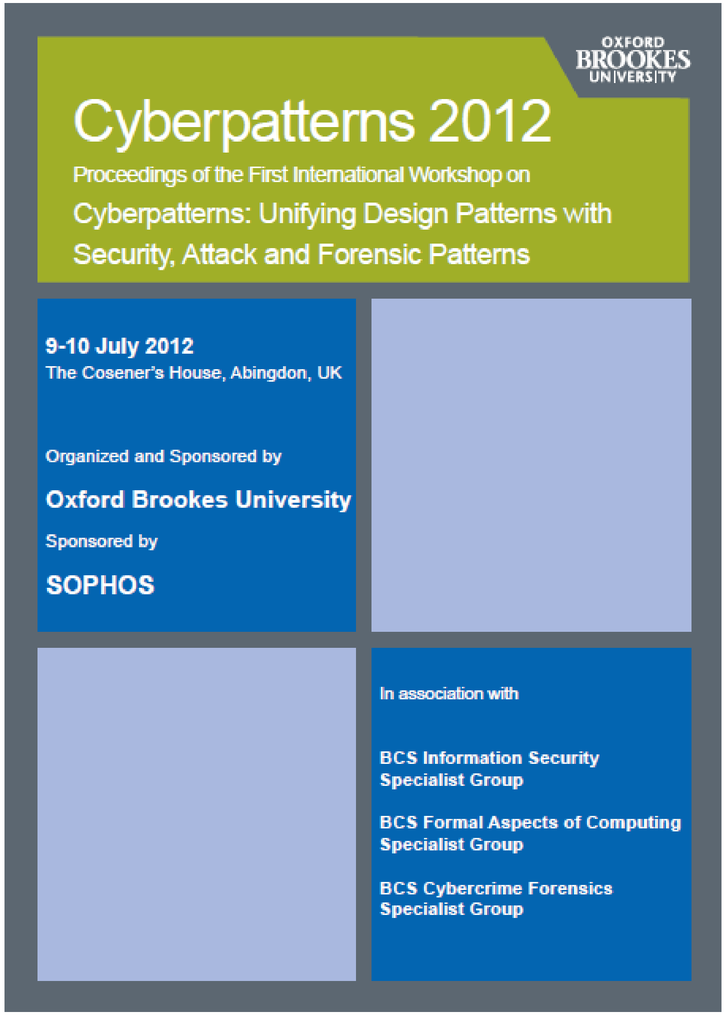
- *Kevin Lano*: Software Design Patterns
  - Reader in Software Engineering, KCL
- Patterns: transformations from imperfect to (more) perfect system
- Eliminating “bad smells” in a design/system
- Role of patterns in software engineering: specification, design, model transformation
- Transformations to eliminate bad properties
- This problem = use this pattern
- Patterns for special areas, e.g. Enterprise information systems, service oriented architectuers, cloud, ...
- Verification of patterns considered as transformations: system after transformation has same semantics/ properties as before (semantic preservation)

Next steps

- Towards a research road map: emerging themes, goals, challenges
- Lacking story: need for collections of case studies, surveys of field, …
- Establishing common language across the fields:
  - Dimensions: domain, level of abstraction, source, audience, points in lifecycle
  - New fields: digital forensics, data driven, cyber warfare, socio-technical systems, use in teaching
  - Taxonomy, “ontology”
- Repository, wiki
- Establish network
- More workshops: better understanding of commonality, differences, better understanding of field, engagement of different audiences, rationales for patterns, formalisation,.. , preserve multi-disciplinary nature
- “Patterns in practice” theme
- Funding: EPSRC, industry, …

Proceedings

- Can be downloaded from the workshop website:
- http://tech.brookes.ac.uk/CyberPatterns2012/index.html



OXFORD BROOKES UNIVERSITY

Cyberpatterns 2012

Proceedings of the First International Workshop on

Cyberpatterns: Unifying Design Patterns with Security, Attack and Forensic Patterns

9-10 July 2012

The Cosener's House, Abingdon, UK

Organized and Sponsored by

Oxford Brookes University

Sponsored by

SOPHOS

In association with

BCS Information Security Specialist Group

BCS Formal Aspects of Computing Specialist Group

BCS Cybercrime Forensics Specialist Group