EDSAC(21): Event-Driven, Secure Application Control for the twenty-first century

Jean Bacon and Ken Moody, April 2004,
University of Cambridge Computer Laboratory

Part 1: Previous research and track record

This proposal was not funded in August 2003. All five reviewers indicated that the project should proceed, three rated the proposal outstanding and two good; all with high confidence. Since submission we have developed our ideas in the area; our publications include "best paper" at Middleware. The proposal emphasised healthcare applications and our OASIS RBAC software has since been integrated with the Pennine Group's IBHIS. We were approached recently by Dr Michael Hu, Enterprise Architecture Manager in the Police Information Technology Organisation (PITO). PITO are in the process of modernising and integrating police IT systems and believe that our research is relevant to their requirements. We have also agreed to collaborate with CARET (Centre for Applied Research in Educational Technology) in Cambridge, who have encountered some of the issues we address. This proposal extends that of 2003, with PITO and CARET providing application scenarios. Professor Ehud Gudes of Ben Gurion University will visit us for 6 months in 2005-2006 to work with us in this area.

Research motivating this proposal

Jean Bacon and Ken Moody lead the Opera research group at the University of Cambridge Computer Laboratory. Opera focuses on the design and deployment of open, large-scale, widely distributed systems. Two major thrusts are in the areas of asynchronous middleware (**Hermes** a wide-area publish/subscribe system), and an open access control architecture for secure interworking services, **OASIS** role-based access control (RBAC). An overview is given in [3, 8].

This proposal is to extend and integrate these approaches using Hermes and OASIS without loss of generality. Access control is needed on event subscription and notification, both within applications and when applications share a common communications infrastructure. Asynchronous events are needed for timely revocation of access rights. The privileges associated with roles may change as applications progress. Also, event correlation (composition) is essential for controlling the volume of events generated in pervasive environments. Active database technology integrates naturally with event transmission and is needed by many services, for example when a police record update triggers the need for emergency action. Our early work opened up major new avenues and approaches, now recognised as urgently needed. Important problems remain and we are best placed to tackle them; indeed, without this background such wide-ranging research would be impossible.

Recent grants that have motivated this work are:

(1) Global Computing Using Events, EPSRC Oct 1998 - Dec 2001
(2) OASIS Access Control, PhD studentship, EPSRC July 1999 - June 2002
(3) Access Control Policy Management, PhD studentship, EPSRC Oct 2000 - Sept 2003
(4) Travel and subsistence support to advise Glasgow Caledonian and Strathclyde on using OASIS for distributed courseware, EPSRC Jan 2002 - March 2003
(5) EU Framework 5 Global Computing: SECURE Secure Collaboration among Ubiquitous Roaming Entities, Jan 2002 - Dec 2004

The Opera group were early to incorporate **asynchronous**, one-to-many, direct and indirect event notification into standard middleware. The application areas for this work included multimedia presentation management and tracking mobile entities in sensor-rich environments [1, 9, 2, 10]. [17] showed how an *advertise, register, notify* paradigm could be incorporated into standard CORBA, using CORBA-IDL to specify events. Under (1) we added event storage to the architecture, used ODL for event typing and OQL for querying event stores. The software and our publications are available from our web pages, http://www.cl.cam.ac.uk/Research/SRG/opera. In [5] we showed how to federate heterogeneous event systems (e.g. CORBA and Java-based) using gateways and contracts. Here, automatically generated XML was used as the inter-domain transfer syntax.

CEA is appropriate for simultaneously-running sources and sinks with static dependencies, such as in an active building. In **Hermes** [18, 19], we have explored loosely coupled, source-sink-anonymous, event-based communication, appropriate for large scale systems, both widely distributed and locally dense. Hermes is a publish/subscribe system built above a peer-to-peer routing network. Advertisements and subscriptions meet at distributed rendezvous nodes and filtering is distributed across a network of event brokers, exploiting subscription-covering to minimise the event propagation overhead. Hermes is an attribute-based pub/sub system with a rich programming model that exploits a type hierarchy. It is potentially heterogeneous, deploying XML for message transmission between clients with automatic translation between XML and programming language types.

The starting point for **OASIS** RBAC was to support interworking between independently developed services in different administrative domains. Our Addenbrookes colleagues in the Clinical and Biomedical Computing Unit (CBCU), through their company CBCL, have used OASIS access control in their pilot software for electronic health record (EHR) management within the UK National Health Service. With them we have reimplemented OASIS using Enterprise JavaBeans technology and have built a demonstration infrastructure using a web portal and SSL for initial authentication and encryption. We propose to integrate event-driven notification of access control violations, essential for dynamic control situations such as limiting the effects of stolen credentials.

In (3) a graduate student worked on access control policy management for OASIS, building a policy store as an active database over Postgres. This approach will allow us to use existing distributed database best practice for policy storage as well as within applications. In (4) GCU and Strathclyde are using OASIS RBAC to control access in the management of courseware common to a number of universities. An unresolved issue is how to manage the changing privileges of roles as time passes. This proposal builds on the insights and experiences gained from (3) and (4) through the unifying concepts of (ad-hoc) workflow-driven, event-based, secure distributed applications.

In (5) we are exploring a computational basis for incorporating trust and risk into global computing. Here, previously unknown entities that encounter each other, and must decide whether to interact, may not be strongly authenticated but may operate under a pseudonym. Notions of trust and risk are applicable to event-broker networks.

Research supervision and dissemination

We have supervised graduate students in distributed systems, leading to 31 PhD awards and have examined 26 other internal and 22 external (including international) PhDs in related topics. Our recent graduate students have employment which includes: Citrix Research UK, AT&T Research UK, University Lecturers in Cambridge, Birkbeck, Israel, Singapore and Egypt, Bellcore US, Cisco US, Fore UK, FutureTV Cambridge, Microsoft Research Cambridge, Google, CBCU, Cornell and Harvard Universities.

Journals, programme committees, panels

From 2000 Jean Bacon has been EIC of IEEE's first online magazine, Distributed Systems Online *http://computer.org/dsonline/*. She is on the EBs of IEEE Pervasive and Internet Computing and was elected to the IEEE-CS Board of Governors for 2002-4. Our onference participation and panels include:
ACM SIGOPS European Workshop 1996, Programme Chair 1998 (Dr Bacon)
EDBT and BNCOD (many times, up to and including 2003) (Dr Moody)
IEEE Services in Distributed Networked Environments 1995,6 (Dr Bacon)
IEEE 24th IC Distributed Computing Systems (Dr Bacon) vicechair Middleware 2004
IFIP 8.1 Information Systems in the WWW Environment 1998 (Dr Moody)
ACM Symposium on Operating Systems Principles, 1999 (Dr Bacon)
IFIP/ACM Middleware 1998, 2000, 2001, 2003, 2004 (Dr Bacon)
POS9 2000, Data Engineering 2001, ACM SACMAT 2002, 2003, 2004 (Dr Bacon)
Policy1999, 2001, 2003, 2004: Policies for distributed systems and networks (Dr Moody)
Proposer/organiser of ICDCS workshop on event-based systems, July 2002, PC 2003, 2004 (Dr Bacon)
16th IFIP WG11.3 Conference on Data and Application Security. Cambridge, July, 2002 (Dr Moody)
VLDB-TES, Technologies for E-Services, PC 2002, 2003 (Dr Bacon)
Percom (Pervasive Computing) PC 2003, 2004 (Dr Bacon),
Distributed Objects and Applications (DOA 2003) (Dr Bacon)
EU project CORTEX (sentient computing) reviewer (Dr Bacon)
Distinguished dissertation panel (Dr Moody) and reviewers

Ehud Gudes is a distinguished international academic, a Professor of Mathematics and Computer Science at Ben Gurion University Israel. He will spend 6 months working with us on this project as a VRF. He has over 20 years experience of research in databases, database security, constraint systems and data mining. He also has a great deal of development experience. Please see attached CV.
Lauri Pesonen is a mature, self-funding PhD student. He came to us with several years post-MSc experience working for a messaging software supplier and is investigating security for messaging systems for his thesis work. This application is to support Lauri, and two new graduate students, to work with us for three years on event-driven systems, with integrated access control.

Part 2: The proposed research

2.1 Introduction, background and motivation

Event-based communication has long been used within application components such as window managers but the potential of this asynchronous communication style for a wide range of distributed applications, including global, pervasive and mobile computing, has only recently come to be realised. Until the mid 1990s the research culture in middleware was focused on LAN-based distributed systems with synchronous communication between closely coupled components. Early attempts at building event-based systems used asynchronous extensions to the then-dominant object oriented middleware, such as CORBA, Java and DCOM. Although message passing was offered commercially, for example by IBM's MQSeries, only one-to-one communication was supported, via statically named queues.

Large-scale distributed systems, both widely distributed and locally dense, require asynchronous communication between loosely coupled components, and communication patterns other than one-to-one are essential. The publish/subscribe communication paradigm was designed to meet these needs, and forms the basis of event-based middleware. Here, a network of event brokers serves clients that may be publishers, subscribers or both. A pub/sub service allows event types to be advertised, subscribers to indicate their interests and publishers to notify a given event to the group of interested subscribers. Sources and sinks are mutually anonymous at notification time. Pub/sub systems may be topic based (in which only coarse-grained subscriptions are supported) or (topic and) attribute based, for fine-grained subscription. They may have a programming model, in which case events are automatically translated between programming language types and a transfer syntax, such as XML. A type hierarchy may then be exploited so that subscriptions may automatically be generalised. A comprehensive database of event-based systems can be found at http://dsonline.computer.org/middleware/em/EMLinks.htm. Our locally developed system Hermes [18, 19] is an attribute-based pub/sub system with a rich programming model. We will use Hermes in this research, without loss of generality.

Adding **access-control** to large-scale event notification, while maintaining efficient propagation, has not yet been tackled and is one aspect of this proposal. We envisage a future where global pub/sub services are offered commercially, and are used by applications that need both protection and support for sharing. Such a service must provide access control beyond restricting the service to those who have paid. Each application will define the event types it is concerned with, and needs to control the principals that can advertise, subscribe to and notify them. For example, public services such as police, fire, ambulance and utilities may separately use a metropolitan pub/sub system. As well as intra-service communication, some inter-service communication is needed, for example, during an emergency such as a serious traffic accident. The services need controlled sharing of event information: victims' identities are needed by the ambulance service, so that medical data can be looked up, but must remain confidential in general, although the number of victims can be made public. We use this example in [11]. The police IT organisation PITO have a national multi-service scenario, with tens of local police forces interacting and using court-case, vehicle and identity information services.

In a pub/sub service with many brokers it is unlikely that services will trust all brokers uniformly, particularly when confidential information is to be transmitted at times of media interest. In [11] we discuss the use of attribute encryption and the management of encryption keys so that only trusted parties can decrypt sensitive information. Lauri Pesonen's thesis will address these issues. We have studied computational trust in global computing in the EU SECURE project and are in a position to integrate the trust architecture and software throughout a broker network.

For scalability, access control policy is most appropriately expressed in terms of roles (RBAC) rather than individuals. The motivation is that role-privilege associations change less frequently than individuals join, leave or change role within an organisation. Separating role-privilege policy specification from the administration of individuals assists scalable management. In the example above, police, fire and ambulance services will each define their roles and specify which roles can read which attributes in which messages. Also, through service-level agreements, they will specify which roles of one service may subscribe to which attributes of which events of another; OASIS also allows constraints to be imposed.

As computer-dense environments become commonplace it will be important to control the volume and propagation of events. An event correlation (composition) service, above the basic event transmission service, has potential for controlling volume; the design, and dynamic placement of instances, of such a service is part of this proposal. Event composition has been tackled for centralised active database [13]. In distributed systems, for example in network management scenarios, the standard approach is to search an event-condition-action (ECA) rule base sequentially. Parallel evaluation is preferable for efficiency and scalability, and our approach is to define event composition operators within finite state machine recognisers, and thus to search in parallel for patterns defined to be significant for applications.

There is a fundamental problem in ordering events in distributed systems (which is often ignored) and the best that can be done is to assign to events source-specific interval timestamps which bound UCT, as proposed in [16]. Our first attempt at an event composition service, which takes this approach, achieved "best paper" award at Middleware03 [20]. This research, with PhD students who have now moved on, will be carried forward and will be evaluated for large-scale, wide-area contexts. We shall also investigate the limitations, if any, of this bottom-up composition, and will study proposed top-down approaches such as ECA rules and TFOL [15]. The ideal is that intuitive top-down registrations of interest by humans can be automatically translated into efficient composite event recognisers.

The RBAC community first developed models for single organisations; [22] is seminal and there are many related references. Implementations were slow to emerge, particularly for distributed contexts. Our OASIS RBAC started from an architecture and implementation for widely distributed deployment over multiple administrative domains [6] and we developed a formal model for precise specification [7].

OASIS uses parametrised roles activated within sessions. Figure 1 shows its credential-based role activation, where credentials may be prerequisite roles and persistent (appointment) certificates. In addition, access control policy may indicate environmental constraints that must be satisfied for a role to be activated. Any part of the role activation conditions may be tagged as having to remain true for the role to remain active. Should such a condition become false the role is revoked; this requires an **event infrastructure** to be integrated with the architecture, part of this proposal. In order to use an OASIS-secured service or to access data managed by it, the services' access control policy must be satisfied by the invoker: proof of active role membership must be presented and any environmental constraints satisfied. When a pub/sub service is to be secured, this could allow restrictions to be imposed on, for example, the time of publication, the size of messages etc.

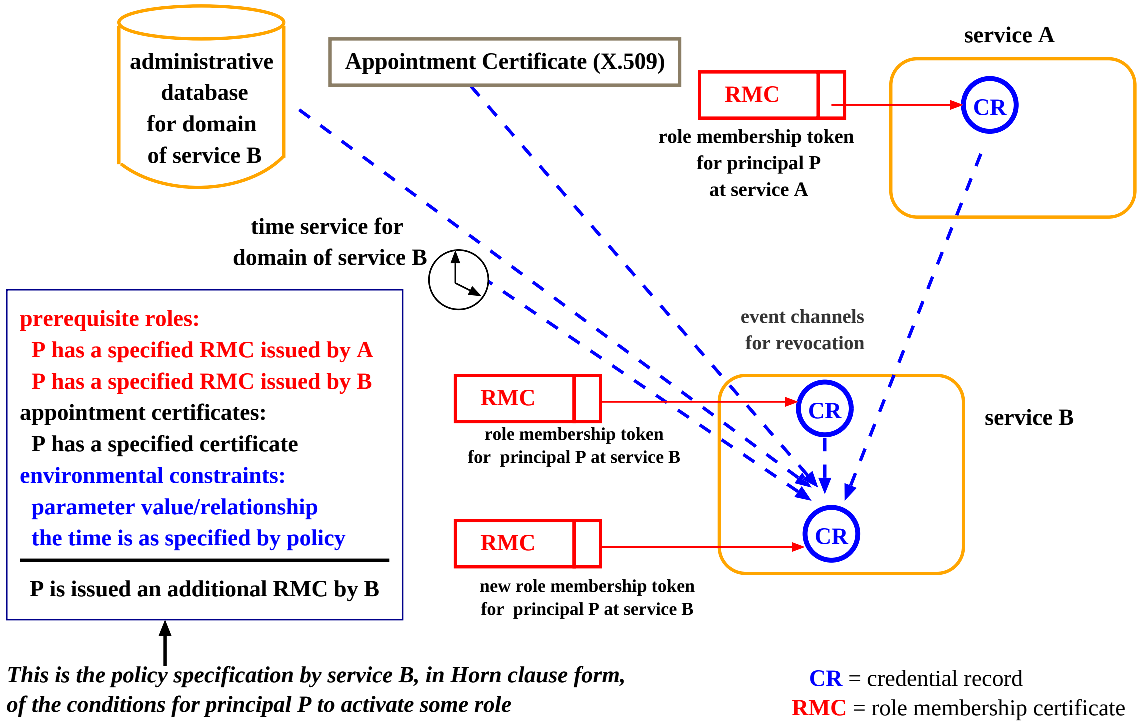

Figure 1: OASIS role activation within a session

OASIS has been implemented for NHS Electronic Health Record access control using Enterprise JavaBeans. We have taken the relevant components of this implementation to form a generic OASIS implementation. Our colleagues on the RAED project have used it to control access to courseware. Their research interests are in groupware and HCI for education and they import systems technology. One requirement is to facilitate student interaction over submitted project work, but only at the appropriate time - for example when a deadline has passed or when all coursework has been submitted. There is therefore a change of the access rights of roles to specific data as the application progresses that cannot be solved by RBAC alone. This can be programmed ad hoc; all that is possible in the 2-year RAED project. This proposal is to work on the fundamental issues that have been raised. We will evaluate the use of environmental constraints, internal roles or integration with a workflow. Our colleagues at CARET have also encountered these problems and will provide more application scenarios.

We have met with Dr Wade's group from the eLearning Centre, Trinity College Dublin, who work both on courseware and workflow. They confirm that we may think of this style of application as driven by an "ad-hoc workflow" [26] rather than a heavyweight, industrial style of workflow [24, 25]. Professor Shrivastava's group at Newcastle are also working on a flexible approach to workflow [14] and are interested in using OASIS RBAC. We request support for further collaboration with these groups.

Our talks with PITO have reinforced the need to support related but independently managed services sharing a secure messaging infrastructure. In addition, their services involve database management. There are tens of local police forces, each maintaining records of cases; cases are tracked through the courts in a separate court service; there are services supplying vehicle and identity-related data. At present, a reply to a given request may require explicit access authorisation by a senior person, bringing delay into the process. Integration of workflow and OASIS RBAC model this scenario well, and we hope to be able to create automated, securely audited procedures. The use of active database triggers should assist in raising alarm signals. There are many problems associated with federation, for example, over the subtly different semantics of similarly named roles in different police forces.

In general, the integration of database management and active database functionality leads to many research issues. For example, an event triggered by an active database might have been published by an uncommitted transaction. Strong consistency is not achievable in many application domains, such as worldwide stock-market dealings, and these applications typically use pub/sub messaging. We have used locally-developed Postgres/T5 technology to implement an active predicate store. This will be used to set up triggers from administrative databases to enforce OASIS environmental constraints as well as to support alarms.

We propose to bring these threads together within the general context of secured event-based systems, to achieve the goals below. The research will be carried out as detailed in the next section and workplan.

- To secure a large-scale, attribute-based publish/subscribe communications service by integrating RBAC. Separate services may share the pub/sub service; each is supported in defining its roles and events, and in specifying role activation and access control policy. Inter-application messaging, through service-level agreements, will also be supported.
- To allow for different levels of trust by applications of each other and of the brokers in the pub-sub network, through the management of encryption keys and the use of attribute encryption.
- To support active security, where privileges are individually and immediately revocable, by extending OASIS RBAC with an event infrastructure.
- To support dynamically changing privileges of roles, using a lightweight workflow to drive applications, and thus to facilitate, for example, both static and dynamic separation of duty constraints.
- To create secure audit trails of application workflow procedures.
- To integrate active database triggers with the event infrastructure.
- To allow for events published during the course of transactions that may subsequently abort.
- To expose all system features and administration through a secure web interface.
- To provide facilities for users to specify the required application behaviour at a high level: a policy editor will make it unnecessary to edit the XML specifications by providing interfaces for defining roles and associated privileges. A graphical visualisation of policy structure will be provided.
- To test our approach in a range of scenarios: pervasive computing (an active house, an active city); wide-area, large-scale data management (electronic records held by public bureacracies and utilities); electronic delivery of courseware.
- To make our software available in component form under open-source licensing.

2.2 Methodology and work programme (please refer to the workplan)

We will work as a team throughout, with responsibilities divided as follows: **Lauri Pesonen** (RA), will work on securing pub/sub systems. One PhD student (PhD1) will focus on workflow and database issues, the other (PhD2) on sensor networks in pervasive environments. All will develop applications and make software available. **Ehud Gudes**, VRF, will work exclusively on this project with us for 6 months.

First year

The RA will work on RBAC-secured pub/sub. This will involve naming issues - of services sharing the pub/sub infrastructure and of events and roles within services. This is essential for the service-level agreements that allow inter-service operation. He will also work on topic and attribute-level key management, evaluating overhead; a secure client package or a private, trusted end-broker will be provided.

The PhD students will take some time to get up-to-speed on OASIS RBAC and Hermes. PhD1 will work with us on RBAC-workflow integration, evaluating the requirements of electronic courseware delivery from the RAED project and CARET in Cambridge, establishing PITO services' requirements, including a secure audit trail, and using active house and city scenarios as examples. PhD1 will work with the RA on integrating event communication into OASIS RBAC, including active database triggers. Ehud Gudes will contribute from July 2005.

PhD2 will work on (bottom-up) event composition, evaluating its potential as a distributed, internet-based detection service as well as within sensor-rich environments. In both scenarios, bandwidth can be saved by strategic placement of detection subtrees, for example, to aggregate data from dense sensor clusters. This placement will be automated, as we began in [21]. The student will also investigate intuitive, user-level queries such as, for a mobile user, "nearest ATM machine", "nearest empty meeting room" and whether an automatic mapping can be carried out between these high-level queries and bottom-up-composed events. Current approaches will be evaluated, e.g. [15].

Second year

The RA will implement a secured, shared pub/sub system with intra-and inter application RBAC using key management and attribute encryption. Overhead will be evaluated, as in our prototype [11]. Support for non-uniform trust in brokers (from our EU SECURE project) and secure audit will be included.

PhD1 will work with Ehud Gudes on the design and implementation of workflow technology using Postgres/T5 for active database functionality. The aim is to control applications, representing the changing context, and effect the changes of privileges associated with roles as the context changes. We will work closely with CARET in this area. We envisage that we will define primary actor roles (in courseware delivery, examples would be student, tutor, administrator) and implicit system-defined roles (controlled by the OASIS appointment mechanism) which are acquired and lost depending on the application/workflow state. The integration of events with OASIS in year 1 is an important prerequisite for this work. The alternative approach is to use the OASIS environmental constraint mechanism, which involves a check of context (application/workflow state) on every user action. This is at the heart of the research; only after this period will we be able to decide on the best approach.

PhD2 will implement an event correlation service, building on [18, 20, 21]. This is needed to control the volume of events in pervasive computing environments and to express complex conditions that trigger actions in workflow-controlled and other applications. Use of the service as distributed instances, placed to optimise the use of communication services, will be evaluated for widely distributed large scale systems and sensor clusters.

Third year

The RA will develop an application to evaluate secured pub/sub, for example, an active city or PITO scenario with various public services sharing pub/sub communication.

PhD1 will also be concerned with application development and evaluation, focusing on the data-management functionality of services (as in PITO) integrated with workflow and transactions.

PhD2 will demonstrate and evaluate distributed CED services in a pervasive computing scenario. Mobile users will issue queries from handheld devices.

Policy is represented internally in XML. A higher-level interface will be provided for clients to specify and edit application behaviour and access control policy. We have experience of representing OASIS RBAC policy graphically and have carried out preliminary research using controlled natural language, translated into first-order logic [4] and on representing queries about pervasive environments in FOL [15].

Throughout the project we will make the software available as milestones are reached and will demonstrate how it is used by means of selected applications (see workplan). We have extensive experience in guiding PhD research and in fostering teamwork. The VRF will work exclusively with the project.

2.3 Beneficiaries

This research will create components of a comprehensive software platform to support event-driven applications with integrated access control. Commercial pub/sub providers are emerging (Gryphon, Apama, Dualstar) but no-one has yet addressed security issues. As well as pub/sub service providers, many applications are potential beneficiaries. One style is small-footprint, pervasive applications providing personalised, instantaneous access to information (stock quotes, news, email, calendar-alerts). In another, the application state and behaviour evolve as users progress through it (the delivery of training and courseware material). Yet another is pervasive, sensor-rich environments with support for client query. Our most complex scenario is represented by PITO, where the separate services communicate about persistent data, constrained by workflow and transactions. All need pub/sub services with RBAC, and other application-specific middleware services. There will be a huge market for such components.

2.4 Dissemination and exploitation

The Opera group were innovators in using event-based systems as the paradigm for pervasive and mobile computing. We have also worked on architecting and implementing (as well as modelling) RBAC for widely distributed systems. We will continue to publish our work and participate as organisers and programme committee members of workshops and conferences in these areas. We aim for prestigious publication arenas in which the research has to be evaluated practically. We will also investigate wider applications of the approach, for example in relation to the emerging behaviour of complex systems.

The basic OASIS software is already available for free download. It is being used by CBCL for NHS EHRs, by the RAED project at Glasgow Caledonian and Strathclyde, in the Pennine Group's IBHIS software and is being evaluated by Professor Shrivastava's group at Newcastle. As milestones are reached we will add to the software available. We will augment the software with web-accessible demonstrations, selected from those listed in the workplan, to show how it can be used.

2.5 Resources

We request three years of support for **Lauri Pesonen** as an RA, two PhD studentships and 10% of a computer officer's time for systems, communications and dissemination support. This is necessary because the research is broad ranging and specifically addresses integration.

We request £8000 travel and subsistence support for the VRF, Prof. Ehud Gudes. His salary will be paid by Ben Gurion University, but this is low after tax (£13500pa net) at the current exchange rate. We are fortunate that he is taking a UK, rather than US-based, sabbatical.

We will present our work at international conferences and workshops, for example, Percom, UbiComp, Middleware, SACMAT, Policy, and others in the emerging area of complex systems and sensor networks. Several groups' work overlaps with aspects of our proposal and we request support to maintain contact with them: Professor Buchmann, TU Darmstadt (event-based systems, active database): Dr Pietzuch, creator of Hermes, now at Harvard working on medical sensor networks; Dr Sturman, the Gryphon project at IBM TJW(event transmission), (Peter Pietzuch was a summer intern with Gryphon in 2002); Trinity College Dublin (Prof. Cahill, Head of Distributed Systems (pervasive computing) and Dr Wade, Director, Centre for eLearning (workflow)); Professor Shrivastava, University of Newcastle, (workflow, dependable systems); Professor Sloman, Imperial College (policy expression and management).

We request PCs for the PhDs and RA, a shared portable for visits and presentations, and a small number of handheld devices for experiments in pervasive computing.

References

[1] Bacon J, Bates J, Hayton R and Moody K, "Using Events to Build Distributed Applications", Proc IEEE SDNE Services in Distributed and Networked Environments, pp148 - 155, Whistler, British Columbia, June 1995.

[2] Bacon J, Bates J and Halls D, "Location oriented multimedia" IEEE Personal Communications 4(5), pp.48-57, Oct 97.

[3] Bacon J et al, Generic support for distributed applications IEEE Computer 33(3), 68–77, March 2000.

[4] Bacon J, Lloyd M and Moody K, Translating role-based access control policy within context Policy 2001, Workshop on Policies for Distributed Systems and Networks, Bristol, UK, January 2001. Lecture Notes in Computer Science Vol. 1995, 107–119, Springer 2001.

[5] Bacon J, Hombrecher A, Ma C, Moody K and Yao W, "Event Storage and Federation using ODMG" 9th International workshop on persistent object systems, design, implementation and use (POS9), Lillehammer, Norway, Sept 2000, Lecture Notes in Computer Science vol. 2135, 265 – 281, Springer 2001

[6] J.Bacon, K.Moody and W.Yao, Access Control and Trust in the Use of Widely Distributed Services. In Middleware 2001, Lecture Notes in Computer Science 2218, pages 295-310, Springer 2001. Selected for extended publication in Software Practice and Experience 2003.

[7] J Bacon, K Moody and W Yao, A model of OASIS role-based access control and its support for active security. ACM Transactions on Information and System Security (TISSEC), 5(4), pp.492-540, November 2002

[8] Jean Bacon and Ken Moody, Toward open, secure, widely distributed services. Communications of the ACM, 43(6) pp 59-63, June 2002

[9] Bates J, Halls D, and Bacon J, "A Framework to Support Mobile Users of Multimedia Applications" ACM Mobile Networks and Nomadic Applications (NOMAD),1(4), pp. 409-419 , 1996.

[10] Bates J, Spiteri MD, Halls D and Bacon J, Integrating Real-World and Computer-Supported Collaboration in the Presence of Mobility. Proceedings of IEEE Workshops on Emerging Technologies in Collaborative Environments (WET'ICE) 1998, Workshop on Collaboration in the Presence of Mobility, Stanford, CA USA. June 1998. Best paper award of conference and workshop.

[11] Andrs Belokosztolszki, David M. Eyers, Peter R. Pietzuch, Jean Bacon, and Ken Moody. Role-based access control for publish/subscribe middleware architectures. In International Workshop on Distributed Event-Based Systems (DEBS03), ACM SIGMOD, San Diego, CA, USA, 2003. ACM.

[12] Carzaniga A, Rosenblum D, Wolf A, Design and evaluation of a wide-area event notification service. ACM Transactions on Computer Systems 19(2001) pp.332-383

[13] Chakravarthy S, Mishra D, Snoop: An Expressive Event Specification Language For Active Databases Data Knowledge Engineering 14(1), pp.1–26, 1994

[14] J. J. Halliday, Santosh K. Shrivastava, Stuart M. Wheater Flexible Workflow Management in the OPENflow System. EDOC 2001: pp.82-92

[15] E. Katsiri, J. Bacon and A. Mycroft, An Extended Publish/Subscribe Protocol for Transparent Subscriptions to Distributed Abstract State in Sensor-Driven Systems using Abstract Events accepted for DEBS04, Third International Workshop on Distributed Event-Based Systems,with ICSE May 24th/25th Edinburgh UK, 2004

[16] Liebig C, Cilia M and Buchmann A, Event composition in time-dependent distributed systems, Proc 4th Int Conf on Cooperative Information Systems (COOPIS) pp.70-78, 1999

[17] Ma C and Bacon J, COBEA: A CORBA-Based Event Architecture Proceedings USENIX COOTS'98, Santa Fe, New Mexico, USA, pp117-131 April 1998

[18] P. Pietzuch and J. Bacon, Hermes: A Distributed Event-Based Middleware Architecture, Proceedings of the 1st International Workshop on Distributed Event-Based Systems (DEBS'02) with IEEE ICDCS, July 2002.

[19] P. Pietzuch and J. Bacon, Peer-to-Peer Overlay Broker Networks in an Event-Based Middleware. In H. Arno Jacobsen, editor, Proceedings of the 2nd International Workshop on Distributed Event-Based Systems (DEBS'03), ACM SIGMOD, San Diego, USA, June 2003. ACM.

[20] P. Pietzuch, B Shand and J. Bacon, A Framework for Event Composition in Distributed Systems.In M. Endler and D. Schmidt, editors, Proc. of the 4th ACM/IFIP/USENIX Int. Conf. on Middleware (Middleware '03), pages 62-82, Rio de Janeiro, Brazil, June 2003. Springer. **Best paper award**

[21] P. Pietzuch, B Shand and J. Bacon, Composite event detection as a generic middleware extension. IEEE Network, 18(1):44-55, February 2004.

[22] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman. Role-Based Access Control Models. *Computer*, 29(2):38–47, Feb. 1996.

[23] Brian Shand, Nathan Dimmock and Jean Bacon, Trust for Ubiquitous, Transparent Collaboration. Proc of the 1st IEEE International Conference on Pervasive Computing and Communications (PerCom), Dallas-Ft. Worth, Texas, USA, 23-26 March 2003.

[24] Schmidt M, The Evolution of Workflow Standards, IEEE Concurrency, July-September 1999.

[25] Sheth AP, van der Aalst W and Arpinar IB, Processes Driving the Networked Economy, IEEE Concurrency, July-September 1999.

[26] Vincent Wade Workflow - A Unifying Technology for Operational Support Systems Proceedings of Seventh IEEE/IFIP Network Operations and Management Symposium (NOMS 2000) Hawaii, IEEE Computer Society Press