Proactive Knowledge Sharing Security for Netchains with Breach-Directed Dynamic Policy Revision

Haluk Demirkan*, Daniel Soper, and Michael Goul
W. P. Carey School of Business, Arizona State University
PO Box 874606, Tempe, AZ 85287-4606
Emails: Haluk.Demirkan@asu.edu Daniel.Soper@asu.edu Michael.Goul@asu.edu
* Corresponding Author

Abstract - The increasing adoption of Service Oriented Architecture (SOA) is allowing more and more companies to integrate themselves in netchains with partner organizations through which they can share knowledge assets. The dynamic nature of these relationships implies a need for organizations to protect and monitor the flow of their valuable knowledge assets throughout the netchain if they hope to maintain their long-term competitive positions. In this paper, we propose a knowledge sharing security architecture that integrates the Value Chain Reference Model (VCOR), the Federated Enterprise Reference Architecture Model (FERA), and multidimensional data warehouse technologies to allow for the proactive monitoring of shared knowledge assets across an SOA-based netchain as part of an organization's overall business intelligence (BI) strategy. The proposed architecture can be easily incorporated into existing BI infrastructures, as data warehousing has already been adopted by most organizations.

Key Words: Knowledge security, netchain, value chain, supply chain, interdependence, collaboration, business intelligence

I. INTRODUCTION

Mergers and acquisitions, new regulations, rapidly changing technology, increasing competition and heightened customer expectations mean that companies must find innovative ways to become more collaborative, virtual, accurate, synchronous, adaptive and agile. Knowledge management plays a key role in today's very complex and continuous innovation-required business world. With dynamic knowledge management capabilities, companies have the ability to share their resources and expertise with their partners in response to changing demands, and they can build value chain-based intellectual capital. One of the most important challenges in value chain-based knowledge management is to maintain knowledge sharing security [6].

The phrase "netchain analysis" combines supply and value chain analysis research streams with network analysis research. A netchain is a set of networks comprised of horizontal ties between firms within a particular industry or group such that these networks (or layers) are sequentially arranged based on the vertical ties between firms in different layers [7]. A netchain analysis therefore differentiates between horizontal (transactions in the same layer) and vertical ties (transactions between layers), mapping how agents in each layer are related to each other and to agents in other layers. Netchains also share properties with other types of social network analyses, for example, the concepts of centrality, degrees of separation, density, etc. [10]. We posit that netchain analysis can facilitate value chain security governance for binary organizational knowledge exchanges in the short term. We also consider the question, "How can an organization govern the long term security of the knowledge assets it chooses to share within its netchain?"

Let's consider a large technology company (C) that produces a constantly changing mix of increasingly complex products operating in an environment of global competition that demands ever shorter product life cycles. Suppose this company's netchain analysis results in three distinct subsets. As a customer, this company purchases equipment from a variety of suppliers (N1). Also, it designs, develops and manufactures microchips in a second subset (N2). Lastly, it provides consulting services in the third subset (N3).

In all of these subsets, knowledge sharing is becoming as important as the physical movement of products as depicted in Figure 1. To effectively govern the secure transfer of knowledge initiated from C, there is a need for common and normalized business semantics to describe business processes both within C and with business partners – both vertical and horizontal within the netchain. In addition, as a part of the netchain agreements expressed using those semantics, each company should work closely with relevant vertical and horizontal partners to achieve common goals through a collectively governed approach to knowledge sharing. Also, each trusted netchain partner needs to extend its control over key shared and un-owned knowledge assets throughout their netchains, such that if a breach of security in any knowledge sharing relationship occurs, containment strategies can be triggered and modifications to the governance of future knowledge sharing relations with partners can be updated throughout relevant subsets of the netchain. All of this must take place in the context of changing market conditions, new business requirements and the constant gaining of new trusted partners and mitigation of losses associated with untrustworthy partners. This dynamic implies the need for constant adjustments to the policies that are in place to govern knowledge sharing security in an organization's netchain [e.g., 4, 13].

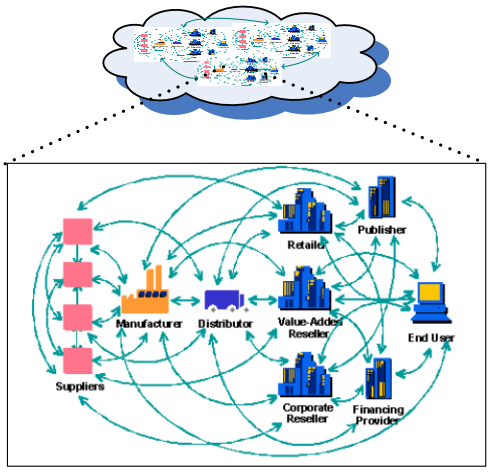

Figure 1: Information and knowledge sharing in netchains

II. Our Approach

Although space limitations prohibit a complete description of the details of our approach to addressing knowledge sharing security dynamics based on netchain analyses, we do address general considerations here. In our approach, we use the integrated process and technology framework that is a combination of the Value Chain Group's "Value Chain Reference Model" (VCOR) [12] and Intel's Federated Enterprise Reference Architecture Model (FERA) [5] to represent and map business semantics to architectural semantics (e.g. Figure 2) [3]. VCOR defines a unified business process framework and reference model utilizing a common language and taxonomy to facilitate effective value chain communication for information and knowledge sharing that can be used for process modeling, gap analysis, simulation, benchmarking, and consensus building. In addition FERA is an architectural representation that allows collaborative process models to be mapped to components of the conceptual architecture and to required resources for dynamic allocations. FERA is currently the basis for the ebSOA proposed standard (OASIS) [9]. The two independent but reconciled process representations facilitate the mapping of business processes to core collaboration capabilities for efficiency.

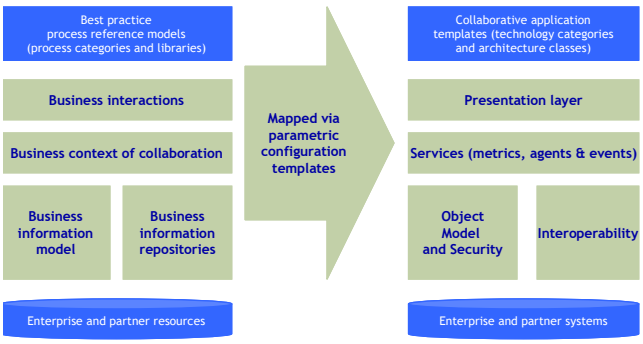

Figure 2: Business semantics to technology semantics

In today's world, knowledge sharing can be considered in the context of three patterns: person to person, system to system, and person to system (and vice versa). In person to person, knowledge is exchanged using a vocabulary and semantics. In system to system, information exchange is enabled by systems interpreting and processing semantics [1]. In person to system, we rely on people's understanding and systems' processing. Relying on FERA and VCOR, there are several opportunities for knowledge sharing and exchange within a netchain, expressed as patterns in Table 1 along the dimensions of 'business context' and 'exchange agent type.' These patterns are described as follows [e.g., 1, 2, 3]:

1) Bulletin boards and web meetings are used for remote access to share public information and for virtual collaboration, e.g., the reporting of schedule status, changes in forecasts, inventory and delivery updates, and exchanges for conducting virtual meetings. In terms of the process, a remote participant signs in through a portal to start a session, follows the available commands, and concludes the session by leaving all of the results in the remotely-administered system. Participants exchange information via the system's upload and download functionality. Remote participants are exposed to selected information by a resource from within the control domain, whereby they consume only the sets of information presented directly by that resource [2]. In this pattern, drilling down may expand the context that some of the parties cannot follow, which is why it is limited to those contexts that are intuitive and fully comprehensible to all parties.

2) Personal interactions supported by collaborative software are used for the ad-hoc exchange of secure knowledge between parties with familiar contexts, e.g., dynamic replenishment, engineering changes, multi-party conceptual design, portfolio planning, etc. In this pattern, participants interact by exchanging information through direct inquiries into each other's systems through a common portal, in addition to using their own systems supported by collaborative software [3]. For example, two planners may inquire into the sales forecast over a common portal directly with each other after each one conducts their own analysis. This pattern relies on manual reconciliation and shares information in an abstraction layer. It does not support detailed data moves.

3) Fixed workflow automation for an industry standard content is provided by a system-to-system publish and subscribe pattern, e.g., warranty administration, inventory updates. In this pattern, participants generally do not need to communicate with each other; rather, the systems exchange the information [1]. This configuration requires that all participants agree on common semantics of the information to be exchanged. It may be used to support multiple instances of the same application, e.g., ERP, CRM. It does not support multi-threaded exchanges of information.

4) Collaborative business process management is used for non-deterministic complex processes that need iterative and dynamic reconciliation of multi-threaded information and knowledge sharing, e.g., dynamic replenishment, direct and reverse allocation management, concurrent distributed security systems engineering, etc. Many processes do not have standards for the business logic that can govern distributed systems and participants. In this pattern, technically, participants map to the shared business logic representing the equivalent semantics from their internal business logic. An agent-based framework reconciles the internal logic dynamically and coordinates events between the collaborative event handlers on the federation server and the interval workflow systems [e.g., 1, 3]. This pattern combines the functional capabilities of other patterns in addition full VCOR-FERA collaboration.

Table 1: FERA process patterns (Adapted from [3])

collaborative process patterns	people exchange business content with other people	systems exchange business content with other systems	people exchange business content with systems
business context is managed by a single authority			1. Bulletin boards and web meetings
business context is distributed over several authorities	2.Personal interactions supported by collaborative software	3. System to system publish and subscribe	4. Collaborative business process management

Given these patterns, we propose a data warehouse-coupled knowledge security policy hub located at each netchain entity (Figure 3). Policies are to be maintained and managed within each associated FERA implementation, i.e., messages passing through FERA gateways at both the sending and receiving ends of a particular knowledge collaboration are governed by the hub. The hub must have the ability to manage and control the governance of knowledge sharing security for each of the patterns discussed above in order to support binary knowledge exchanges. For example when company C from Figure 5 purchases equipment from a supplier, design specifications and the knowledge associated therewith must be governed by policies at both ends of the exchange.

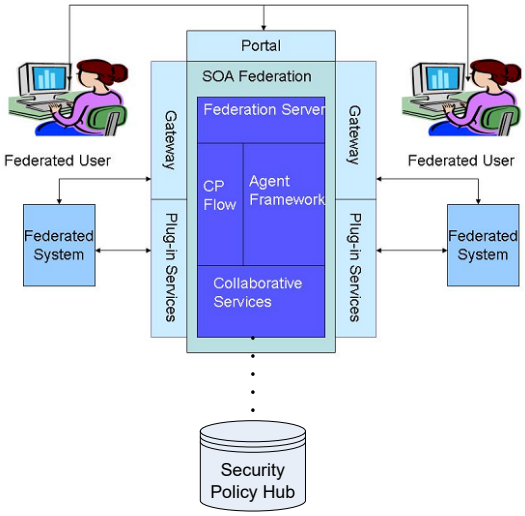

Figure 3: A knowledge security policy hub located at each netchain entity (Adapted from [11]]

Common FERA semantics at the two entities enable interpretation of security provisions for this type of knowledge exchange, and the exchange pattern that is being used can be deployed according to those security provisions. Situated at the policy hub, then, are meta-security policy provisions for sharing a particular type of VCOR business process semantic (e.g., DESIGN) between two entities, say A and B, using a pattern, say pattern 2, from Table 1 above: personal interactions. In this way, not only can C manage security for knowledge exchanges between A and B, but the process also supports recording the exchange in repositories at both ends, and C can apply, for example, non-disclosure agreements for involved people before facilitating collaboration through the FERA gateway. Note that even in this binary exchange, C may stipulate that it is acceptable for B to share A's DESIGN exchange with some of its partners involved in marketing, i.e., indirect sharing through the MARKET semantics in VCOR (e.g., Figure 4).

Figure 4: VCOR Semantics and Sub-Processes for the Execute process (adapted from [12])

Meta-security policy provisions expressed in VCOR semantics for each FERA process pattern and deployed through FERA gateways can manage binary knowledge sharing in a proactive way. But should those policies remain static, or can they be dynamically informed by events that take place to either reduce or increase levels of trust among netchain participants? Further, can the significance of those events be coordinated within a subset of a netchain where the impact of trust dynamics is most important? To address these questions, our approach augments the policy hub discussed above with gateway communications in the event of security breaches associated with specific binary knowledge sharing arrangements. When knowledge security is breached, it is the duty of collaborating netchain partners to broadcast the details of the breach. Each entity in the netchain must then assess how best to adjust meta-security policy provisions for the netchain linkages that ultimately led to the breach. To clarify, consider the slightly different view of a netchain shown in Figure 5.

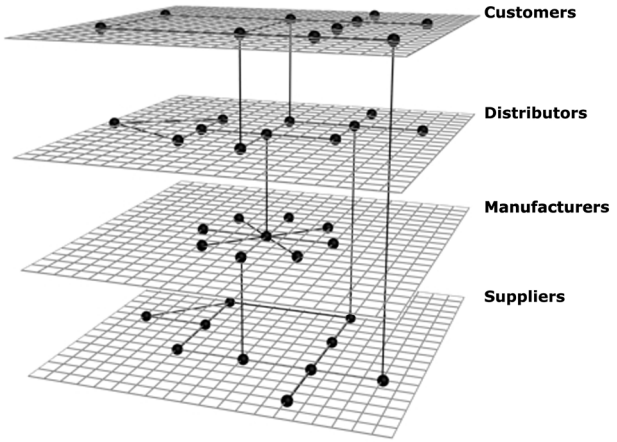

Figure 5: A different view of a netchain

If the manufacturer has a new product design compromised through the release of information by a distributor that was never trusted in a binary arrangement, then that leak can be tracked through the relationships between organizations involved in trusted exchanges. The reduction in trust with the distributor responsible for the breach can then be relegated to more secure knowledge exchanges or it can be governed by more restrictive non-disclosure agreements. Another example can be derived from the so-called "Small World" model (i.e., the social network theory which posits that all humans are connected to one another by a distance of no more than six intermediate acquaintances) [8]. When this model is applied in the context of a fully-interconnected SOA business world, it becomes apparent that a manufacturer could be linked to its closest rival by a very short distance – perhaps only a few hops on the netchain. If the manufacturer is planning to roll out a new product pricing scheme involving its distributors and customers, for example, a breach in the interorganizational knowledge sharing netchain might lead the manufacturer's closet rival to have knowledge of the new strategy prior to its public release. Following the detection of such a breach, the manufacturer would clearly want to protect any further erosion of its competitive position by updating its security policies regarding the trustworthiness of the culprit. The capability to dynamically manage this type of netchain-based security provisioning is obviously dependent upon the integrity and completeness of the netchain model. However, the value of the model in providing for dynamic knowledge exchange is significant to sustaining a long-term competitive position.

III. Schema To Support Datawarehouse Coupled Knowledge Security Policy Hub

All of the linkages between netchain entities need to be stored and managed in a tightly coupled data warehouse system in order to contain security breaches in a timely fashion. In this section, we extend the discussion of the exemplar infrastructure with a multidimensional database schema design. At the outset, we wish to stipulate that it is beyond the scope of this paper to automate all of the tasks associated with the nature of the infrastructure; we have not, for example, developed recovery or backup procedures capable of handling every possible scenario of system or subsystem failure. The required database schema must be able to support fully automated business intelligence and data mining functionalities with active data warehousing. Figure 6 shows a high-level entity/relationship model that captures the essence of a knowledge security hub that relies on the patterns discussed earlier.

The schema contains tables for capturing the relationships between nodes from the perspective of the policy hub owner. For example, if an enterprise has agreed with a partner to share knowledge through one or more of the patterns discussed previously, then for each of those patterns, an entry for the link will be included in the NETCHAIN_LINK_STATE table. The PATTERN table stores information about the pattern relevant to a link. The NODE and PLANE tables record the details of the nodes that exist on the various layers (planes) in the distributed netchain, e.g., suppliers, manufacturers, distributors, and customers. POLICY stores information regarding the internal and external security policies that exist between nodes in the netchain table. VCOR_SEMANTIC table stores semantics for each sub-processes and processes. SNAPSHOT includes a blueprint of the structure of a netchain model at a given time. The BREACH table captures the details of historical information relevant to a breach that may be useful in containing future breaches. In short, when an organization enters into a knowledge sharing relationship with another organization, a Start-Node and End-Node are added to the NETCHAIN_LINK_STATE

table, the Policy-ID related to that link is recorded, the Plane of the organization being linked to is recorded, the relevant Pattern is entered, the VCOR Semantics related to that link is recorded, and the current snapshot counter is recorded. For complex knowledge sharing arrangements such as when a company (say A) grants permission for another organization (say B) to share knowledge with B's trusted partners (say C, D, and E), then A must record in its policy hub each of these indirect linkages with B as the Start Node and C, D and E, respectively, as three distinct links in the NETCHAIN_LINK_TABLE. It is important to note that the schema of Figure 6 shows a recursive relationship relevant to entries in the NETCHAIN_LINK_TABLE to reflect this type of complex knowledge sharing arrangement. It is also important to note that each policy hub associated with an organization in a trusted federation of partners will be unique, but that subsets of recorded relationships would be common, even while planes, patterns, policies, snapshot and breach entries would be distinct.

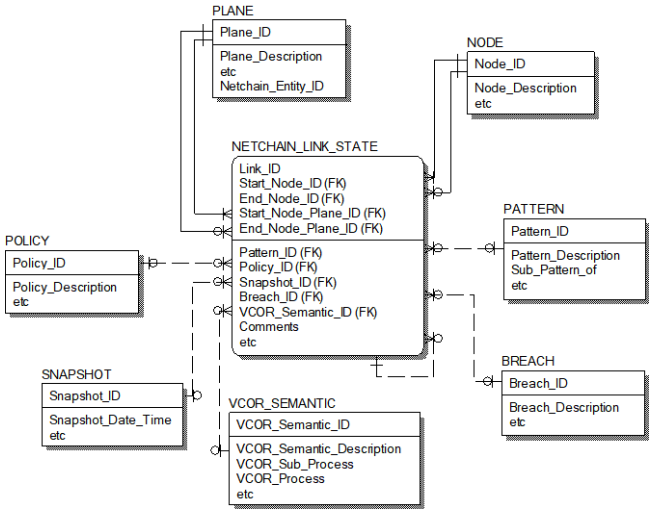

Figure 6: A high-level entity/relationship model of a security hub

Now, we consider the situation of a breach (e,g., Table 2). When a breach is discovered by any partner in the federation, information about that breach must be broadcast to all relevant partners. Upon receipt of breach information, an organization's NETCHAIN_LINK_TABLE can be queried to ascertain the potential causes of the breach, to assess the policies relevant to mitigating breaches of this type in the future, and to examine the potential for the source of the breach to cause loss of security over other knowledge sharing arrangements. It can also guide in the development of a breach impact mitigation strategy. If an organization is able to discover or find a limited subset of those organizations that could have caused the breach through its search of its policy hub data, then that information would also be broadcast to the federation partners. Of course, the federation may have to develop specific policies such as when a root cause is traced to a federation member. Upon receipt of broadcast information regarding the limited set of potential culprits, another node may possess, through analysis of its policy hub data, sufficient information to further limit that subset. As the root cause of the breach is possibly ferreted out in this process, there is major advantage to being a part of the federation – even while each individual organization is clearly in charge of maintaining and implementing its own, independent knowledge sharing policies.

Table 2: Sample queries from the datawarehouse

A partner has indicated a knowledge breach relevant to a graphic design that contains two of our new chips:
1. What people and systems do we have with DESIGN sharing policies that are involved in manufacturing? 2. What are the relationships between partners' systems and our systems regarding DESIGN semantics? 3. How might a recent breach be related to any similar one from two months ago?

Overall, the approach we have taken implies reliance on a business intelligence capability coupled with a data warehouse to capture knowledge sharing relationships that take into account various patterns of inter-organizational collaboration. Policy hubs located at each node of a federation that maintain information about the netchains within which a node engaged to conduct business provide a level of proactive, breach directed, knowledge sharing policy revision. Furthermore, the ability to capture states of the netchains in various snapshots could enable more complex analysis such as data mining to discover patterns of breach combinations that represent complex attempts to steal corporate knowledge. One reason for adopting the business intelligence and data warehouse approach for the policy hub is that many organizations already possess this technology and the expertise to manage it.

IV. Summary And Future Work

The need for new collaboration and infrastructure models relevant to today's very complex and continuous innovation-required business world are apparent. Novel aspects of suitable models must reflect value-chained based collaboration needs and requirements, and facilitate any security issues. Our approach to knowledge security in netchains is targeted at proactive governance of binary knowledge sharing exchanges through process patterns supported by the emerging FERA ebSOA standard. In addition, the meta-policy provisions maintained in our policy hub approach extend value chain collaboration advantages to the realm of enhanced security. By relying on VCOR semantics, specific provisions can be applied to knowledge sharing both vertically and horizontally within netchains. By using dynamic adaptation mechanisms to handle breaches as facilitated through netchain analysis, the security model can be adapted as appropriate by netchain

partners. In short, the idea is to facilitate the handling of breaches by automating as much of their root-cause detection as possible and facilitating the exchange of revised trust profiles through closely collaborating netchain subsets.

Next steps include assessing the stability of our approach under a variety of conditions. By stability, we are investigating netchain characteristics (like number of partners by layer, number of relationships on a given layer and between layers, etc.) and their propensity for potential collapse under situations of severe knowledge exchange breaches. Similarly, we seek to assess the impacts of alternative 'indirect breach relationships,' and we are examining the best methods for supporting meta-policy revision/update in a dynamic setting given different types of indirect breach relationships.

REFERENCES

1. Brown, G. and R. Carpenter, "Successful application of service-oriented architecture across the enterprise and beyond" Intel Technology Journal, November 2004, 8:4, pp. 343-360.
2. Collaborative Product Development Associates, "Integrated Process and Technology Framework," Collaborative Research Services, 2004.
3. Drecun, Vasco and D. H. Brown, "Closing the Process/Technology Gap FERA," Collaborative Product Development Associates, LLC, July 2004.
4. Eisenhardt, K. and J. Martin, "Dynamic capabilities: what are they?," Strategic Management Journal (21), 2000, pp. 1105-1121.
5. FERA-based SOA - Semantion Inc. http://www.ebxmlsoft.com/papers/fera-based-soa.html
6. Grant, R.M., "Toward a Knowledge-Based Theory of the Firm," Strategic Management Journal (17), Winter Special Issue, 1996, pp. 109-122.
7. Lazzarine, S.G., F.R. Chaddad and M.L. Cook, "Integrating supply chain and net-work analyses: the study of netchains," Journal of Chain and Network Science (1), 2001, p.p. 7-22.
8. Newman, M.E.J., "Models of the Small World," Journal of Statistical Physics, 101(3/4), 2000, pp. 819-841.
9. OASIS, http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebsoa , 2006.
10. Scott, J. P., "Social Network Analysis: A Handbook, Sage Publications", Limited, 2000.
11. Semantion Inc., "Run-time Service Oriented Architecture (SOA V 0.2," Whitepaper, October 2005.
12. VCOR – MODEL - http://www.value-chain.org/index.asp
13. Weill, P, Subramani, M., and M. Broadbent, "Building IT Infrastructure for Strategic Agility" Sloan Management Review, 44 (1), Fall 2002, pp. 57-65.