SDPS-2011
Printed in South Korea, June, 2011

INFERENCE OF CONFIDENTIAL PARAMETERS USING INTERNAL STRUCTURES: A CASE STUDY OF AIRCRAFT PYLON AND ENGINE ASSEMBLY

Quan Ye, Xuan Sun, Lingyu Wang, Yong Zeng*
Concordia Institute for Information Systems Engineering
Concordia University
1455 de Maisonneuve Blvd. West
Montreal, Quebec, Canada H3G 1M8
hardleaf99@hotmail.com xua_sun@encs.concordia.ca wang, Zeng@ciise.concordia.ca

Fortin, Clément
Department of Mechanical Engineering
Polytechnique Montréal, Quebec, Canada
clement.fortin@polymtl.ca

ABSTRACT

Aircraft structure is one of the most important aspects in the design and manufacture process of aircrafts. A typical aircraft includes several major sections, such as fuselage, landing gear, stabilizer, wing, pylon and engine. In order to save time and reduce cost, outsourcing parts is a common practice in the aircraft manufacturing industry. One of the main challenges faced by such outsourcing is the potential risk of leaking confidential information or parameters to competitors through shared suppliers. In this paper, we propose a model to capture potential inferences of confidential parameters through internal structures of aircrafts. We provide three methods to infer confidential parameters based on this model, and also apply those methods to a real industry case. The study indicates that such an inference based on internal structures is feasible, and usually cannot be effectively prevented with existing partitioning-based methods.

INTRODUCTION

A typical aircraft includes several major sections, such as fuselage, landing gear, stabilizer, wing, pylon, and engine. In order to save time, reduce cost and improve efficiency, outsourcing some of those sections or parts is a common practice in the aircraft manufacturing industry. However, the protection of confidential parameters or information is one of the main challenges faced by the aircraft outsourcing process. To protect confidential information, legal [1], bureaucratic and social measures [2, 3] are often taken; some technical methods [4, 5, 6, 7, 8, 9, 10, 11] are also developed recently. Confidential information is also referred to as "trade secret" in some cases [12]; it is protected only when it is not disclosed [1, 13]. This paper will focus on the disclosure of confidential information caused by inferences using internal structures of aircrafts.

Existing technical methods for protecting confidential information can be roughly divided into two categories: access control-based methods [4, 5, 7, 8, 10, 11] and secure multi-party computation (SMC)-based methods [6]. Access control-based methods ensure that only authorized companies or users are allowed to access specific shared information [14, 15, 16]; SMC-based methods ensure that a joint computation on multiple sets of data from multiple parties can be performed, while any private information that is implicitly or explicitly included in these data sets is not revealed [17, 18, 19]. However, these methods are usually ineffective against indirect inferences of private information [12].

In this paper, we model the indirect inferences of confidential parameters using the internal structures of an aircraft. We show that when aircraft parts are outsourced, the partners or suppliers may infer confidential information, which is not directly provided to them, based on internal structures of those parts. Such an inference can be achieved by studying the engineering relationships between different mechanical parameters inside the same part. Existing methods based on careful partitioning of a product during outsourcing are usually ineffective in preventing such inferences since internal structures are not addressed in such a partitioning.

In this paper, we also present a case study of aircraft pylon to demonstrate the feasibility of inferring confidential parameters in practice. We show that, based on internal structures of a pylon, some confidential parameters, such as the engine thrust and materials of the bolts, can be inferred. The case study clearly reveals limitations of existing partitioning-based methods for protecting confidential information.

* Corresponding author: zeng@encs.concordia.ca, Tel.: +1-514-848-2424#5801, Fax: +1-514-848-3171

The rest of this paper is organized as follows. Section 2 reviews related work. Section 3 introduces our model and methods for inferring confidential information from internal structures. Section 4 gives a case study about applying our inference methods to aircraft pylon. Section 5 concludes the paper by summarizing the proposed methods, its application and future work.

RELATED WORK

Leong et al. [5] proposed a mixed access control model for a workspace-oriented distributed product data management (DPDM) system. In their model, the proposed DPDM system is stratified into multiply workspaces, and every workspace is assigned a security level. Users and product data are classified according to workspace stratification, and different workspace users are granted with different access rights on product data based on the workspace security level.

Cera et al. [7, 10] and Kim et al. [8] developed a new technique, role-based viewing, for collaborative 3D assembly design. It is achieved through the integration of multi-resolution geometry and Role Base Access Control (RBAC) model [14, 16]. In their model, geometric regions, features and constraints data of 3D assembly models are related with a set of roles. For a specific user, a 3D model is generated for viewing based on his or her assigned roles.

Wang et al. [4] proposed an access control model, S-RBDDAC, for collaborative design data. S-RBDDAC combines RBAC and cryptographic methods to support RBAC with consideration of time, scheduling and value adding activity, policy delegation relation in a distributed context and fine-grained access control at dataset level. S-RBDDAC allows a collaborator to send a subset of the dataset he or she received to a third party with supply chain relationships. Permissions are granted to roles through key distribution and policy delegation. [4]

Chen et. al. [11] presented a trust evaluation method for virtual project team (VPT). It can assist VPT members in deterring whether resource holders have made appropriate decisions to share resources with other VPT members. Combining with access control, Chen's trust evaluation method can enable secure resource sharing, facilitate collaboration and enhance in-formation transparency among members in a VPT [11].

Most existing access control-based methods can defend confidential information by preventing unauthorized users from accessing private information, but they cannot forbid users, authorized or unauthorized, from inferring the private information from the shared information.

Another approach, Secure Multi-party Computation (SMC) [17, 18, 19], was introduced into collaborative NPD by Atallah et al. [17]. They proposed several SMC protocols for supply-chain interactions. Their method is different from traditional information sharing. It enables supply-chain partners to cooperatively achieve desired system-wide goals without revealing any private information, even though the jointly-computed decisions require this information [17]. SMC based-methods protect confidential information by allowing users to perform joint computation on multiple datasets while not revealing information in these data sets. But they cannot effectively prevent the inferences from joint computation results to confidential information in original datasets, if this kind of inferences is possible.

PROBLEM STATEMENT

Model

For simplicity, the model is described by using a simple example abstracted from a real and common aircraft internal structure that will be used later, as illustrated in Figure 1.

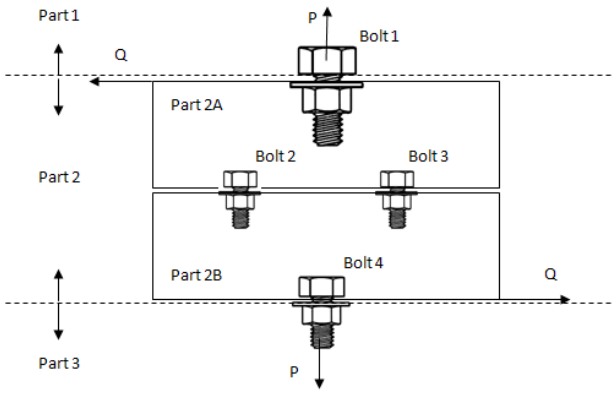

Figure 1 Three parts connected by bolts

In Figure 1, there are three parts (Part 1 and Part 3 are not shown). Part 2 is composed of two components: Part 2A and Part 2B. Part 2 is connected with Part 1 by bolt 1 and Part 3 by bolt 4, Part 2A is connected with Part 2B by bolt 2 and bolt 3. The stress of these bolts includes shear stress (τ) and normal stress (σ) and can be calculated using the below formulas [20]:

$$\textbf{shear stress } (\tau) = \frac{shear\ load}{area\ resisting\ shear} = \frac{Q}{A} \quad (1)$$

$$\textbf{stress } (\sigma) = \frac{load}{area} = \frac{P}{A} \quad (2)$$

Whether shear stress (τ) or stress (σ) is more important usually depends on nature of the load. In our model, in order to simplify the problem, bending and torsion can be ignored since they have smaller influence than others. Therefore, if we know the bolt's materials (shear stress (τ) and stress (σ) of the bolt are specified and identified) and size of the bolt (the area is known), according to formula (1) and formula (2) the following formulas can be developed:

$$\textbf{Q=A* shear stress } (\tau) \quad (3)$$

$$\textbf{P= A* stress } (\sigma) \quad (4)$$

Therefore, we can obtain the load P and shear load Q.

In these three parts, Part 2 includes two sections: Part 2A and Part 2B. Part 2A is connected with Part 2B by

bolt 2 and bolt 3. For bolt 2 and bolt 3, they bear the weight of Part 2B and load from bolt 4. So once we know the materials and size of bolt 2 and bolt 3 (assuming that bolt 2 and bolt 3 have the same size and the materials), as well as the weight of Part 2B, the load from bolt 4 can be inferred based on formula (3) and formula (4). The formulas are shown as the following:

Q4=2*A2*shear stress (τ2) (5)

P4=2*[A2*stress(σ2)- the weight of the Part 2B] (6)

Q4 and P4 represent the load from bolt 4; A2 represents the area of bolt 2 or bolt 3; shear stress (τ2) and stress (σ2) represent the character of materials of bolt 2 or bolt 3.

Part 2A is connected with Part 1 by bolt 1. Bolt 1 bears the weight of Part 2 (Part 2A and Part 2B), Part 3 and the load from bolt 4. So if we know the materials and size of bolt 1, the load from bolt 4 can be inferred based on formula (3) and formula (4). The formulas are shown as following:

Q4=A1*shear stress (τ1) (7)

P4=A1*stress (σ1) - the weight of the Part 2 (8)

Q4 and P4 represent the load from bolt 4; A1 represents the area of bolt 1; shear stress (τ1) and stress (σ1) represent the character of materials of bolt 1.

On the other hand, assuming that we already know load Q, load P and the size of bolts, if the materials of these bolts comprise new materials, or apply new heat treatment comparing with the normal bolts, we still can infer what kind of materials are used to produce these bolts or the new method of heat treatment. Because new materials and heat treatment methods can improve bolts' strength, which means new bolts have higher shear stress (τ) and stress (σ) with the smaller area A, smaller diameter (that can reduce weight of bolts; weight is one of the major concerns and also an important factor in some industry such as aviation industry). Comparing these parameters with the normal bolts based on formula (1) and formula (2), we can infer information about the new bolts.

Application

The assumption is that three manufactures are assigned to fabricate Part 1, Part 2 and Part 3, which is called outsourcing production. If the manufacture of Part 2 wants to know the load from Part 3, which may represent the characters of Part 3 such as the thrust that are provided by Part 3 or the weight of Part 3, even though he does not have information about Part 3, some characters of the Part 3 still can be inferred. There are several methods as follows to infer the load from Part 3.

- Method 1: according to the materials and size of bolt 4 and formula (3) and formula (4), we obtain following results:

Q4=A4* shear stress (τ4) (9)

P4= A4* stress (σ4) (10)

Q4 and P4 represent the load from bolt 4, they are provided by Part 3; A4 represents area of bolt 4; shear stress (τ4) and stress (σ4) represent the character of materials of bolt 4. Therefore, the load from Part 3 can be inferred.

- Method 2: according to formula (7) and formula (8), Q4 and P4 are known, thus some characters of Part 3 can be inferred.
- Method 3: assuming that bolt 2 and bolt 3 have same size and materials, basing on formula (5) and formula (6), Q4 and P4 can be acquired, and then some characters of Part 3 can be inferred.

Similarly, assuming the manufacturer of Part 2 can correctly estimate the load value from Part 3, if he can find the diameter of bolt, such as bolt 4, is smaller than what he estimated, according to formula (1) and formula (2), it is easy to calculate the value of shear stress (τ4) and stress (σ4) and also find these values are higher than the other bolts with the same diameter, so the manufacturer of Part 2 can find out that the material of bolt 4 is different from other bolts or the material of bolt 4 has different heat treatment comparing with others.

Result

According to above discussion, there are two ways for information inference: (1) Using the shear stress (τ) and stress (σ) of materials, the diameters of bolt, load P and load Q can be inferred. The characters of the connected parts such as Part 3 can also be estimated. (2) If load P and load Q can be correctly estimated and the diameter of the bolt is known, we can deduce that the materials of the bolt or the method of material heat treatment are different from other bolts with the same diameters since this bolt has higher value of the shear stress (τ) & stress (σ).

Figure 2 shows the ways of inference confidential parameters.

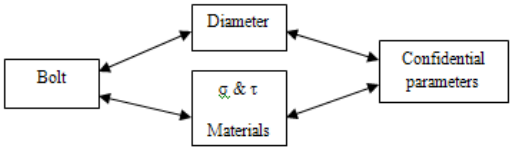

Figure 2 Ways of information inference

Implication

Zhang et al. [12] proposed a "partitioning" method to protect confidential information. The manufacturer can find one or more allocations from components and tasks to suppliers, which satisfy the constraints of product structure and supplier capabilities with low risks of information leakage caused by inferences and minimum operational cost. These allocations will make it possible for the manufacturer to mitigate its risks of information leakage caused by inferences before sharing information with its suppliers [12].

However, this "partition" method can only address the inferences at the border of allocation, for example, the inferences caused by bolts 1 and 4 in Figure 1. It cannot prevent a supplier inferring confidential parameters from

internal structures of its allocated component. It is not realistic to partition all components whenever there is an internal structure that can potentially lead to inference, since such a partition may lead to too many suppliers for manufacturing a single product. Therefore, with the current partition method applied, there is still such a possibility that partners or suppliers may be able to infer confidential information from internal structures. Further research is needed to address this issue.

CASE STUDY

In this section, we present a case study based on the manufacturing of an aircraft pylon. We assume the pylon is manufactured by company A, engine by company B and wing by company C. These three parts will later be assembled by the main manufacturer. We will show that company A who is responsible or manufacturing the pylon can actually infer confidential parameters of the engine based on internal structures of the pylon used to connect that engine. First, Table 1 shows the pylon components.

Table 1 Pylon components

Major component	Functionality
Pylon Bulkhead	Including front and rear section
Engine to Pylon Mount	Connecting pylon with engine
Firewall	Inner structures like web
Pylon mid spar	Connecting pylon with wing
Upper link	Connecting pylon with wing
Diagonal brace	Connecting pylon with wing

Figure 3 shows the connection of engine, pylon, and wing. Between pylon and wing there are three joints which are upper link, diagonal brace and mid-spar wing fitting using bolts and fuse pins. Their positions are similar to bolt 4 mentioned in the previous model. These joints not only undertake the weight including overload which is several times as the weight of pylon and engine, but also bear bending, torsion load and aerodynamic load. Therefore, using these joins to infer the parameters of engine may not be feasible. However, company A can still infer materials of these joints, assuming that company A could correctly estimate the range of load value by comparing with other similar products. If company A finds that diameters of the bolt are smaller than the known bolts, according to formula (1) and formula (2), the values of shear stress (τ) and normal stress (σ) undertaken by the bolts will become larger than the known bolts. So the new materials or method of heat treatment will be inferred.

Figure 3 also shows the position of engine to pylon mount using bolt connection. These are similar to bolt 1 that we mentioned in the model. Figure 4a and Figure 4b show the detail of the front engine mount and the rear engine mount which are connectors between pylon and engine. According to design pattern of the engine mount, we can find that the rear engine mount does not take the thrust which is provided by engine and the front engine mount does not take the engine weight at the lower joints. So the thrust is taken by the bolts that connect with the front engine mount at the lower joints. Although these bolts also take other loads such as bending, the major load is the thrust. According to formula (3) and formula (4), the maximum thrust of the engine can be inferred. On the other hand, assuming that company A knows the thrust from other channels, the materials of bolt will be inferred based on formula (1) and formula (2). The value of shear stress (τ) and normal stress (σ) undertaken by the bolts will become larger than the known bolts. So the new materials or method of heat treatment will be inferred.

Using fuse pins as marked with circle in the Figure 3 which is similar to bolt 2 and bolt 3 as we discussed before to infer parameters of engine would be difficult. The reason is that we will face more unknown parameters like aerodynamic load and more engine parameters. Under some assumed conditions we may derive partial results, while such results may clearly contain significant errors. However, if company A knows the loads and compares bolts with the similar products, according to the diameters of the bolts, which are smaller than the others, and formula (1) and formula (2), the materials of the bolts can still be inferred.

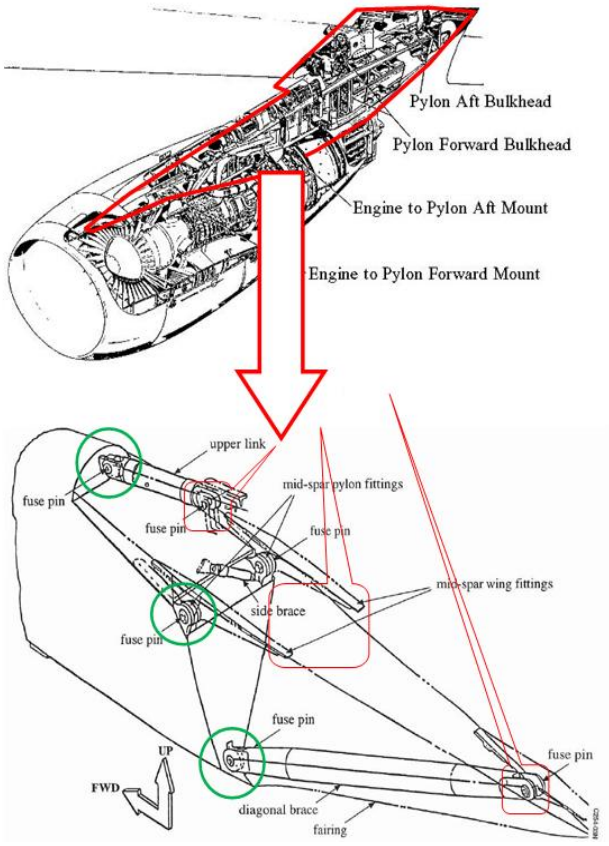

Figure 3 Wing-to-Pylon-to-Engine connections: for the #3 pylon the left-hand side is inboard

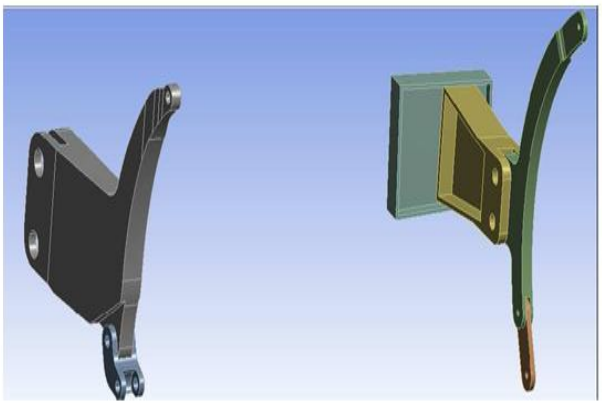

Figure 4a Front engine mount [21] **Figure 4b Rear engine mount [21]**

CONCLUSION AND FUTURE WORK

In this paper, we describe a novel threat of information leakage during product outsourcing. We describe a model of inferring confidential parameters from internal structures. We apply the model to aircraft components as a case study. Our study shows that the existing partitioning-based technical methods cannot effectively prevent inferring confidential parameters with our model. This means there is still a practical risk that partners or suppliers may infer confidential information not directly provided to them from internal structures.

In order to clarify our thoughts, we describe this risk based on a simple model. In our future work, we will consider other types of loads, such as three-dimensional bending and torsion, and strive to develop a generic and unified model that can capture most potential inferences of confidential parameters. Also, we will study novel methods for protecting confidential information from the type of inferences we discovered in this paper.

ACKNOWLEDGEMENT

The research reported in this paper is partially supported by NSERC through a CRD project (PJ 350114-06). We are grateful to the financial support from NSERC, CRIAQ, Pratt & Whitney Canada Corp., Bombardier Inc., CMC Electronics Inc., and Rolls-Royce Canada Limited.

REFERENCES

[1] K. T. Ulrich, S. D. Eppinger, Product design and development, 4th Edition, Mcgraw-Hill/Irwin, 2008.

[2] A. Hoecht, P. Trott, Trust risk and control in the management of collaborative technology development, International Journal of InnovationManagement 3 (3) (1999) 257-270.

[3] A. Hoecht, Control in collaborative research and technology development: a case study in the chemical industry, Journal of Managerial Psychology 19 (3) (2004) 218-234.

[4] Y. Wang, P. N. Ajoku, J. C. Brustoloni, B. O. Nnaji, Intellectual property protection in collaborative design through lean information modeling and sharing, Transactions of the ASME, Journal of Computing and Information Science in Engineering 6 (2) (2006) 149-159.

[5] K. K. Leong, K. M. Yu, W. B. Lee, A security model for distributed product data management system, Computers in Industry 50 (2) (2003) 179-193.

[6] M. J. Atallah, H. G. Elmongui, V. Deshpande, L. B. Schwarz, Securesupply-chain protocols, in: 2003 IEEE International Conference on E-Commerce, 2003, pp. 293-302.

[7] C. D. Cera, T. Kim, J. Han, W. C. Regli, Role-based viewing envelopes for information protection in collaborative modeling, Computer-Aided Design 36 (9) (2004) 873-886.

[8] T. Kim, C. D. Cera, W. C. Regli, H. Choo, J. Han, Multi-level modeling and access control for data sharing in collaborative design, Advanced Engineering Informatics 20 (1) (2006) 47-57.

[9] K. Rouibah, S. Ould-Ali, Dynamic data sharing and security in a collaborative product definition management system, Robotics and Computer-Integrated Manufacturing 23 (2) (2007) 217-233.

[10] C. D. Cera, I. Braude, T. Kim, J. Han, W. C. Regli, Hierarchical role based viewing for multi-level information security in collaborative cad, Transactions of the ASME, Journal of Computing and Information Science in Engineering 6 (1) (2006) 2-10.

[11] T.-Y. Chen, Y.-M. Chen, H.-C. Chu, Developing a trust evaluation method between co-workers in virtual project team for enabling resource sharing and collaboration, Computer in Industry 59 (6) (2008) 565-579.

[12] Da Yong Zhang, thesis: Modeling and Evaluating Information Leakage Caused by Inferences in Supply Chains. The Department of Concordia Institute for Information Systems Engineering. 2009

[13] D. E. Bouchoux, Intellectual property: the law of trademarks, copy rights, patents, and trade secrets for the paralegal, 3rd Edition, DelmarCengage Learning, 2008.

[14] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, Role-based access control models, IEEE Computer 29 (2) (1996) 38-47.

[15] W. Tolone, G. J. Ahn, T. Pai, S. P. Hong, Access control in collaborative systems, ACM Computing Surveys. 37 (1) (2005) 29-41.

[16] D. F. Ferraiolo, R. Kuhn, R. S. Sandhu, Rbac standard rationale: comments on a critique of the ansi standard on role based access control, IEEE Security & Privacy 5 (6) (2007) 51-53.

[17] A. Yao, How to generate and exchange secrete, Harvard Business Review (January-February) (1989) 190-196.

[18] O. Goldreich, S. Micali, A. Wigderson, How to play any mental game, in: Proceedings of the 19th annual

ACM conference on theory of computing,1987, pp. 218-229.
[19] Y. Lindell, B. Pinkas, Privacy preserving data mining, Journal of Cryptology 155 (3) (2002) 177-206.
[20] E J Hearn, Mechanics of Materials, third edition, page 2 and page 11.
[21] CAMAQ virtual environment project 2008-2009 official document: pylon design