

# Layering Negotiations for Flexible Attestation

Yasuharu Katsuno, Yuji Watanabe, Sachiko Yoshihama,  
Takuya Mishina, Michiharu Kudoh  
IBM Research, Tokyo Research Laboratory  
1623-14, Shimotsuruma, Yamato-shi, 242-8502, Japan  
+81-46-215-{4541, 4634, 4828, 4614, 4642}  
{katsuno, muew, sachikoy, tmishina, kudo}@jp.ibm.com

## ABSTRACT

Recently, much attention has been paid to research on distributed coalitions that establish trust among the members of groups of computing components in distributed environments. The Trusted Virtual Domains (TVD) that our research division is proposing is a new model of a distributed coalition for establishing multiple trusted coalitions of components on nodes in distributed heterogeneous environments. In a large-scale distributed computing environment where many kinds of components exist and there might be difficult situations to agree common attestation methods among all components beforehand, it is necessary to provide each component with flexible attestation according to its usage scenario for increasing the number of components that can participate in TVD.

In this paper, we propose a layering negotiation approach. It divides an attestation process into a global attestation phase that verifies that a TVD is fundamentally secure and supporting essential trusted primitives and a local attestation phase that verifies the integrity of a specific component involved in a usage scenario. And, a combination of attestation methods is decided as a result of negotiation between the components for each kind of attestation at each phase. With our approach, the attestation corresponding to a usage scenario can be done flexibly based on the minimal required attestation needed in the TVD, so the component developers can concentrate on the implementation of the higher-level functions.

## Categories and Subject Descriptors

D.4.6 [Operating Systems]: Security and Protection

**General Terms:** Security

**Keywords:** Trusted Computing, Remote Attestation, Distributed Coalition, Trusted Virtual Domains

## 1. INTRODUCTION

There has been considerable interest in distributed coalitions that establish trust within a group of computing components in distributed environments, such as NetTop [3] and Terra [4], based on recent advances in distributed computing and security

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

STC'06, November 3, 2006, Alexandria, Virginia, USA.

Copyright 2006 ACM 1-59593-548-7/06/0011...\$5.00.

technologies. A distributed coalition can now manage the enforcement of different security policies for the components of each group.

The Trusted Virtual Domain (TVD) [8][9] that our research division is proposing is a new model of a distributed coalition. A TVD establishes multiple trusted coalitions called *domains* for components on nodes in distributed heterogeneous environments (Figure 1). A TVD can support distributed mandatory access controls whose security policies are different in each domain. A component that attempts to join a domain first verifies the domain's integrity, and will be forced to honor any security policy defined for that domain while in the domain. The Trusted Computing Group (TCG) technology [1] is the attractive technology for a TVD to allow a remote component to verify the precise configuration and state of a computing platform in a reliable way.

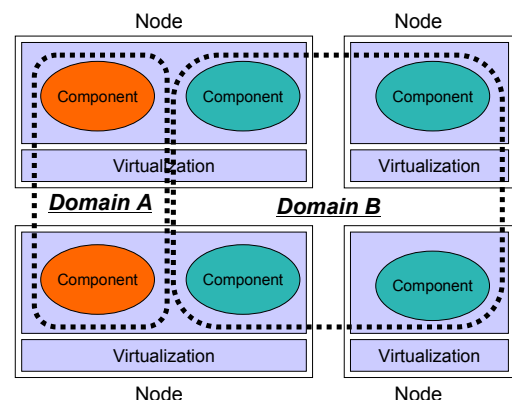


Figure 1: Trusted Virtual Domains

In a large-scale distributed computing environment, it is necessary to consider the differences between attestation strengths that components require. A TCG-based attestation for an entire component may be the strictest way to verify its integrity. However, if the TCG-based attestation is demanded by all of the components, only some of the components that can participate in the domains, because the attestation strength that each domain calls for is different according to its usage scenario, so the strictest method is not always needed for all of the scenarios. For example, an online shopping service would require strict attestation to guarantee secure transactions, perhaps TCG-based attestation for an entire component, while a social network service (SNS) might only call for lightweight attestation to encourage participation, such as check of component version.

To construct domains flexibly, we have proposed the concept of Secure Messaging Router (SMR) [7]. A SMR provides trusted components with the TVD fundamental functions for messaging in distributed heterogeneous environments. In a SMR, attestation methods for components are assumed to be agreed among all components beforehand. However, there might be difficult situations to pass this assumption, considering in a large-scale environment.

In this paper, we propose a layered negotiation approach. First of all, we divide an attestation into two phases, a global attestation and a local attestation. The global attestation verifies the fundamental TVD parts prepared as common trusted primitives. The local attestation verifies a component-specific part that applies integrity verification corresponding to usage scenarios, and the component-specific part is implemented by component developers. Next, global and local attestations can prepare for some attestation methods, such as TCG-based attestation, hash value comparison of component images, and checks of component version. The components negotiate which attestation method to be used or combined. There is a restriction that a global attestation must be equal to or stronger than a local attestation. For example, the only check of component version should not be selected for a global attestation when a local attestation needs a TCG-based attestation. In this case, TCG-based attestation should be put in addition to the check of component version at the global attestation. With our attestation approach, the attestation corresponding to a usage scenario can be done flexibly while guaranteeing the minimal required attestation in the TVD. In addition, component developers can easily achieve TVD fundamental features by using trusted primitives, and concentrate on the implementation of the higher-level parts.

## 2. DESIGN

Figure 2 shows our system architecture. A node is composed of three components, a trusted component base (TCB), a trusted component (TC), and a Trusted Virtual Domain Agent (TVD Agent) as a key component for our layered negotiation approach.

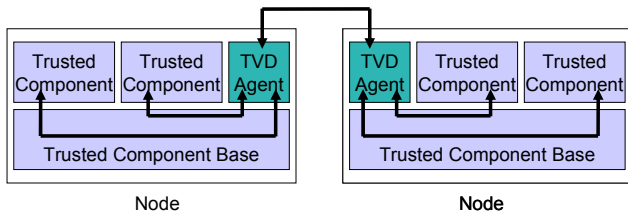


Figure 2: System Architecture

A CCB is highly assured by the lowest layer, such as the hardware-layer. Assurances of TCs and a TVD Agent are achieved by chains of assurance from a CCB on the same node. In addition, a CCB isolates TCs and a TVD Agent at the system resource level.

TCs achieve application services cooperatively with other TCs.

A TVD Agent manages assurances of all TCs on the same node, and plays the role of a single common contact point that guarantees the integrity of each node communicating with any other nodes. That is, integrity of a TVD Agent is attested when a node tries to attest integrity of the other node. All communications inside and outside the node are intensively managed by a TVD Agent, and TCs communicate with other TCs via TVD Agents on the same nodes.

There are established two kinds of domains, a primitive domain among TVD Agents with global attestation, and a TC domain among TCs with local attestation. A primitive domain is established first and a TC domain is next.

A primitive domain provides common trusted primitives with a TC domain. The primitives include messaging to exchange messages between applications over nodes in the same domain on secure communication channels, file access to provide secure file systems where access is limited only to applications in the same domain, and domain lifecycle management to make new domains, join and leave existing domains, and delete domains. A TC domain utilizes the common trusted primitives and provides TC specific features with TCs.

Figure 3 shows an example of primitive domains and TC domains across nodes. The TC Domain 1 and the Primitive Domain 1 are built by a check of a software version and hash value comparison of an image respectively. The TC Domain 2 combines them. The TC Domain 3 applies TCG-based attestation, and the Primitive Domain 2 check which kinds of OS-level reference monitor is used in addition to TCG-based attestation. The Primitive Domain 2 is included in the Primitive Domain 1, because the TCG-based attestation is stricter than the hash value comparison attestation. In other words, TVD Agents 3 and 4 have already established shared primitive domains with TVD Agents 1 and 2.

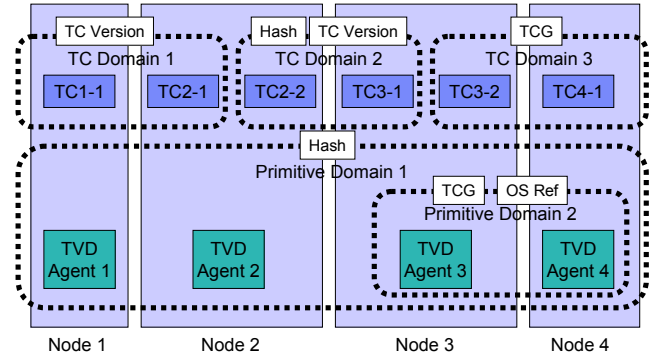


Figure 3: Primitive Domains and TC Domains

Figure 4 illustrates an example of a communication sequence between nodes when a TC on another node participates in an existing TC domain (TC Domain 2).

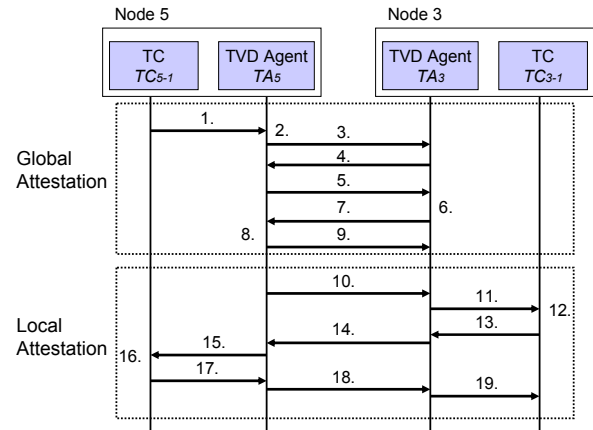


Figure 4: Example of Communication Sequence

First, a primary domain is established to include  $TA_3$  and  $TA_5$  with global attestation.  $TC_{3-1}$  sends to  $TA_5$  a TC domain establishment request message for  $TC_{3-1}$  along with  $TC_{3-1}$ 's proof of integrity for the hash value comparison attestation of the image in order to participate in the TC Domain 2 (Step 1).  $TA_5$  examines if the primitive domain can be established with  $TA_3$  using the hash attestation or a TCG-based attestation, and sends to  $TA_3$  a primitive domain establishment request message with  $TA_5$ 's proof of integrity for the hash attestation (Steps 2-3).  $TA_3$  recommends a combination of TCG-based attestation and check of OS level reference monitor to  $TA_5$  for the Primitive Domain 2 (Step 4), but  $TA_5$  rejects the request because it is not ready for TCG-based attestation, and again requests the only hash attestation from  $TA_3$  (Step 5). Now  $TA_3$  agrees to use the only hash attestation for the Primitive Domain 1, verifies  $TA_5$ 's integrity, and sends a primitive domain establishment response message with  $TA_3$ 's proof of integrity as long as the verification succeeded (Steps 6-7).  $TA_5$  verifies  $TA_3$ 's integrity, and sends to  $TA_3$  a primary domain establishment complete message for the Primitive Domain 1 as long as the verification succeeded (Steps 8-9).

Next, the TC Domain 2 is established between  $TC_{5-1}$  and  $TC_{3-1}$  with local attestation.  $TA_5$  sends to  $TC_{3-1}$  a TC domain establishment request message via  $TA_3$  (Steps 10-11).  $TC_{3-1}$  agrees to use the only hash attestation, verifies  $TC_{5-1}$ 's integrity, and sends to  $TC_{5-1}$  a TC domain establishment response message with  $TC_{3-1}$ 's proof of integrity via  $TA_3$  and  $TA_5$ , as long as the verification succeeded (Steps 12-15).  $TC_{5-1}$  verifies  $TC_{3-1}$ 's integrity, and sends to  $TC_{3-1}$  a TC domain establishment complete message for the TC Domain 2 via  $TA_5$  and  $TA_3$  as long as the verification succeeded (Steps 16-19).

### 3. IMPLEMENTATION

Figure 5 illustrates a prototype system.

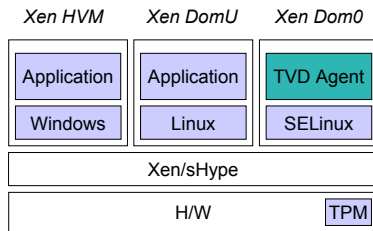


Figure 5: Prototype System

Xen [6] is a well known and widely used open source hypervisor. Xen is running each node. Xen isolates each TVD Agent and each application in the unit of a Xen domain, and establishes peer-to-peer communication channels between each TVD Agent and each application. A TVD Agent runs on the Xen administration domain called  $Dom0$ , and the application on the Xen user domain called  $DomU$  for para-virtualization domain or  $HVM$  for full-virtualization domain.

The sHype [5] is a mandatory access control framework for a virtual machine monitor in Xen. Mandatory access controls for the network interfaces in sHype would guarantee enforcement of peer-to-peer communications between  $Dom0$  and  $DomU/HVM$  domains.

For TCG-based attestation, Integrity Management Architecture (IMA) [2] and vTPM [13] are used. IMA utilizes TCG integrity measurements and attestations, and vTPM virtualizes the Trusted Platform Module (TPM) [1] for operating systems on a hypervisor

layer. The attestation of a TVD Agent is done with TCG-based attestation over the whole  $Dom0$  domain. The  $Dom0$  domain is booted with a trusted boot loader, Trusted GRUB [14], and its configurations are stored in a Platform Configuration Register (PCR) [1] in the vTPM.

It is preferable that the operating system on the Xen domain be as lightweight as possible to simplify the attestation. We are currently planning to use SELinux configured to load minimum set of services.

### 4. RELATED WORK

Property-based attestation [11] proposes an attestation model with a trusted third party that translates low-level integrity information into a set of properties. In attestation, the properties such as security requirements are used instead of the configuration of its software and hardware components.

Semantic remote attestation [12] uses a trusted virtual machine as the basis of remote attestation. The trusted virtual machine verifies various properties of applications on it by explicitly deriving or enforcing them.

WS-Attestation [10] proposes efficient and fine-grained remote attestation on Web Services. It exchanges attestation in the form of a credential which asserts properties and binds those properties with the hash value based attestation generated by a TPM chip.

NetTop [3] uses VMWare to isolate execution environments, and allows connecting isolated environments to each other to form a network of trusted environments, leveraging secure OS such as SELinux to increase the level of security on the host and the guest OS.

Terra [4] realizes isolated trusted platforms on top of a virtual machine monitor, and allows attestation by a binary image of each virtual machine. Terra employs non-TCG based attestation to verify software stacks running in the guest OS, setting up a trusted relationship between multiple virtual machines.

### 5. SUMMARY

A layered negotiation approach that we proposed in this paper provides flexible attestation according to usage scenarios of components, by dividing attestation into a fundamental and common TVD phase called global attestation and a component-specific part called local attestation, and combining suitable attestation methods as a result of negotiations between components. Components can participate in suitable TVD domains with appropriate combinations of attestation methods. A TVD Agent on each node provides components on the same node a single common contact point and common trusted primitives, such as messaging, file access, and domain management.

Some challenges have been left yet toward flexible attestation. First, a common attestation method is required on heterogeneous environments. An ontology-based negotiation by using ontology language such as OWL [15] would be useful. Next, a combination of a global attestation and a local attestation may be still coarse-grained according to some applications. A combination of hierarchal global attestations and hierarchal local attestations would be able to provide fine-grained attestation, though both are single in this paper.

### 6. ACKNOWLEDGEMENTS

The authors wish to thank our colleagues at IBM who helped us with their insights in earlier discussion in our collaborative work

on TVD. Especially we thank Reiner Sailer, Stefan Berger, Ronald Perez, John L. Griffin, Matthias Schunter, Megumi Nakamura, Seiji Munetoh, and Hiroshi Maruyama. We also benefited from insightful comments by Chris I. Dalton, Michael Franz, and Christian Stuble. This work was supported by Research for Next Generation Information Security, Ministry of Economy, Trade and Industry (METI), Japan, under the contract number H17-11-25-1.

## 7. REFERENCES

- [1] Trusted Computing Group (TCG), <http://www.trustedcomputinggroup.org/>.
- [2] Sailer, R., Jaeger, T., Zhang, X., and Doorn, L. V. Attestation-based Policy Enforcement for Remote Access, *11th ACM Conference on Computer and Communications Security (CCS 2004)*, 2004.
- [3] Meushaw, R. and Simard, D. NetTop: Commercial Technology in High Assurance Applications, *Tech Trend Notes Volume 9 Edition 4, National Security Agency*, 2000.
- [4] Garfinkel, T., Pfaff, B., Chow, J., Rosenblum, M., and Boneh, D. Terra: A virtual machine-based platform for trusted computing, *In Proceedings of the 19th Symposium on Operating System Principles (SOSP 2003)*, 2003.
- [5] Sailer, R., Jaeger, T., Valdez, E., Cáceres, R., Perez, R., Berger, S., Griffin, J., and Doorn L. V., Building a MAC-based Security Architecture for the Xen OpenSource Hypervisor, *Annual Computer Security Applications Conference (ACSAC 2005)*, 2005.
- [6] Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., and Warfield, A. Xen and the Art of Virtualization, *In Proceedings of the nineteenth ACM symposium on Operating systems principles (SOAP'03)*, 2003.
- [7] Watanabe, Y., Yoshihama, S., Mishina, T., Kudo, M., and Maruyama, H. Bridging the Gap between Inter-Communication Boundary and Inside Trusted Components, *to be appeared in the 11th European Symposium On Research In Computer Security (ESORICS 2006)*, 2006.
- [8] Griffin, J. L., Jaeger, T., Perez, R., Sailer, R., Doorn, L. V., and Cáceres, R. Trusted virtual domains: Toward secure distributed services, *In IEEE First Workshop on Hot Topics in System Dependability (Hot-Dep2005)*, 2005.
- [9] Bussani, A., Griffin, J. L., Jansen, B., Julisch, K., Karjoth, G., Maruyama, H., Nakamura, M., Perez, R., Schunter, M., Tanner, A., Doorn, L. V., Herreweghen, E. A., Waidner, M., and Yoshihama, S. Trusted Virtual Domains: Secure Foundations For Business and IT Services, *IBM Research Report RC23792*, 2004.
- [10] Yoshihama, S. Ebringer, T., Nakamura, M., Munetoh, S., and Maruyama, H. WS-attestation: Efficient and fine-grained remote attestation on web services, *International Conference on Web Services (ICWS 2005)*, 2005.
- [11] Sadeghi, A. R. and Stuble, C. Property-based attestation for computing platforms: Caring about properties, not mechanisms, *New Security Paradigms Workshop*, 2004.
- [12] Haldar, V., Chandra, D., and Franz, M. Semantic Remote Attestation - A Virtual Machine directed approach to Trusted Computing, *Virtual Machine Research and Technology Symposium*, 2004.
- [13] Berger, S., Cáceres, R., Goldman, K., Perez, R., Sailer, R., Doorn, L. V. vTPM: Virtualizing the Trusted Platform Module, *In 15th USENIX Security Symposium*, 2006.
- [14] Applied Data Security Group. Trusted GRUB, [http://www.prosecco.rub.de/trusted\\_grub.html](http://www.prosecco.rub.de/trusted_grub.html).
- [15] McGuinness, D. L. and Harmelen, F. V. Web Ontology Language (OWL): Overview, <http://www.w3.org/TR/owl-features/>.