THREAT ANALYSIS AND ATTACKS ON XTREEMOS: A GRID–ENABLED OPERATING SYSTEM*

Amit D. Lakhani, Erica Y. Yang, Brian Matthews, Ian Johnson, Syed Naqvi, Gheorghe C. Silaghi
Rutherford Appleton Laboratory,
Science and Technology Facilities Council, Didcot,
Oxon, UK
OX11 0QX
a.lakhani, y.yang, b.m.matthews, i.j.johnson, s.naqvi, g.c.silaghi@rl.ac.uk

Abstract We perform a preliminary threat analysis on a grid–enabled operating system, namely XtreemOS, in this paper. While currently under development, XtreemOS aims to provide native Virtual Organisation support in a secure and dependable manner. We investigate security within the XtreemOS architecture by identifying the security requirements and objectives. Further, we list assets within the system that need protection and detail attacks using the attacker tree methodology. At the end, we describe a specific attack on the overall XtreemOS–supported architecture using an attacker tree. Analysis of this nature will help in generating a number of test cases for testing an early prototype of XtreemOS and provide assurance to the security of the XtreemOS system.

Keywords: XtreemOS, Threats, Attacks, Grid, Threat Analysis, Attacker Tree

*This work is supported by the European Commission under the IST program #FP6–033576.

1. Introduction

Grid Middleware security has been researched extensively in literature [1, 7, 8, 9]. While various middleware security services have been developed, the unification and use of such services is left at the discretion of the implementers. We propose to develop a Grid–enabled Operating System, called XtreemOS [2], which has native support for Virtual Organisations (VOs). In the context of Grid and Web services, a VO is a static or dynamic group of entities (organisations, individuals, institutes etc.) that pool resources and use services to achieve common objectives. Security in XtreemOS is a major concern, and administrators and users require a high level of assurance in this area. To this end, we are in the process of developing a secure VO management strategy and also plan to use evaluation criteria, such as Common Criteria, to inspect the claimed security provided by XtreemOS.

In this paper, we describe our threat analysis and attacks identified in XtreemOS by understanding the basic threat model in Grid and Web Services architecture. We analyse various attacks possible in such a setting and build attacker trees to inspect various attacker tools. The benefits of our threat analysis are manifold. Such attacker trees will generate a number of test cases to test a working prototype of XtreemOS once developed. Our analysis will also identify threats, in addition to common threats in Grids and Web services which are created by XtreemOS. Included in the analysis is the study of risks in designing such underlying services and a consideration of mechanisms that can be used to mitigate such risks. While various other research proposals address Grid Operating Systems [3–4]; to our knowledge, there does not exist any threat analysis for a Grid-enabled Operating System.

2. Threat Analysis

To carry out a proper threat analysis we first need to define the security requirements, identify assets and consequently determine threats in the system. In the next subsection we start our analysis with security requirements of XtreemOS.

2.1 Security Requirements and Objectives for XtreemOS

While the exact XtreemOS architecture is still under development, a detailed description of the overall system and XtreemOS is given in [2].

The basic security objectives of XtreemOS are similar to those applicable to traditional operating systems, namely confidentiality, integrity and availability. In addition in the Grid, authentication and authorisation become a prime concern. However, the fulfillment of such objectives become more difficult due to the distributed nature of the Grid. Of greater importance are synchronisation

issues, inconsistencies within which can particularly lead to non–fulfillment of security objectives. We consider both stored data and data in–transit. The most important security requirements we consider for our system model are:

- Confidentiality of stored data
- Confidentiality of communicated data
- Integrity of stored data
- Integrity of communicated data
- Identification and authentication of users
- Authorized access to application services
- Guaranteed access to services by authorization parties
- Accountability of data access and service execution
- Isolation of data within a VO
- Isolation of services within a VO

In order for the secure running of the XtreemOS–supported system, these requirements should be fulfilled **at every point of time** and not just during VO formation or dissolution. Such emphasis becomes absolutely necessary due to distributed nature of the system.

2.2 Assets

Having defined the security objectives and requirements we list the identified assets in our system. We consider both stored and communication assets for our analysis. Our assets for an XtreemOS–supported system are as follows:

- user and administrator authentication credentials for the Grid;
- user and administrator authorization credentials for the Grid;
- VO–membership credentials;
- filesystems – both local and filesystems shared on the Grid;
- user and process data transmitted between nodes by XtreemOS;
- VO–specific data on a resource (there will be data of different VOs on a resource, so isolation of these data from each other is important);
- services within a VO and their identifiers;
- infrastructure–specific information (such as keys for Public–Key Infrastructure);
- user and service attributes;
- reputation data of services and resources (we envisage use of reputation for selecting services and resources at a later stage of XtreemOS development);
- OS–specific information (e.g. synchronization data);
- logging information.

All these assets require a level of protection to be specified and mechanisms to be put in place to provide such protection.

2.3 Threats

Threat modelling for the Grid systems has been done in many other research studies [5–6]. While various common threats are identified for the overall Grid architecture, threats in Grid middleware and the underlying operating systems have not been studied in–depth. In the context of XtreemOS, we classify below some common threats and some XtreemOS–specific threats.

Threats to availability Denial–of–service attacks are the most common attacks in Grid systems. Although not specific only to Grids, these threats are easier to realise than any other threats in Grid systems. Denial of service to nodes, denial of service to services, denial of service to a VO, denial of service to filesystems are all examples of these threats. Recently, a new kind of threat has been derived from these threats; distributed denial of service (DDoS) on the Internet using Grid nodes (e.g. DDoS attack on Sun Grid in 2006). The realisation of such threats is drastic and defeats the purpose of collaboration in Grid systems, thereby making these threats significant to mitigate in any Grid system including XtreemOS.

Threats to authentication Threats in this category range from injecting false authentication credentials, to test misconfigurations in management of authentication mechanisms, to masquerading as genuine users of the Grid. Theft of authentication credentials, exploiting revocation policy within the system by replaying invalid credentials and brute–forcing user private keys are examples of threats in this category. These threats probably form the second largest category that Grid systems are exposed to.

Threats to authorization Authorization restricts access to resources and services only to users who provide respective credentials. Threats to authorization include false injection of authorization credentials, masquerading as authorization providing entity (e.g. masquerading as KTC in Kerberos) etc. Although realisation of these threats require skilful attack strategies, authorization threats if realised can be highly damaging to the normal functioning of Grid systems.

Threats to confidentiality of data The realisation of such threats will lead to unauthorised disclosure of data. Eavesdropping (both active and passive) and masquerading to reveal data are examples of such threats. Confidentiality is required while passing job results, inter–VO communications and during authentication in Grid systems.

Threats to integrity of data It is one of the fundamental requirements for XtreemOS to preserve the integrity of data. Threats to integrity will address unauthorised modification of data in–transit and stored data to achieve the goals of the attacker(s). It becomes difficult to detect such threats if the consequent state of the system remains unchanged. Active eavesdropping and man–in–the–middle attacks are realisation of such threats.

Threats to isolation of data Isolation of VO–specific data is of great concern in Grid systems due to possible conflict–of–interests between VOs. These threats are specific to Grid systems and to XtreemOS in particular. VO–session hijacks, compromising node security, worms, trojans etc are examples of threats in this category. To mitigate such threats, we are currently looking at virtualisation and Trusted Computing (TCPA) as possible solutions.

3. Attacks

Having identified various threats in XtreemOS, we move on to focus on attacks on XtreemOS system. At a later stage we visualise a few of these attacks by using attacker trees.

The overall XtreemOS architecture framework is given in Figure 1.

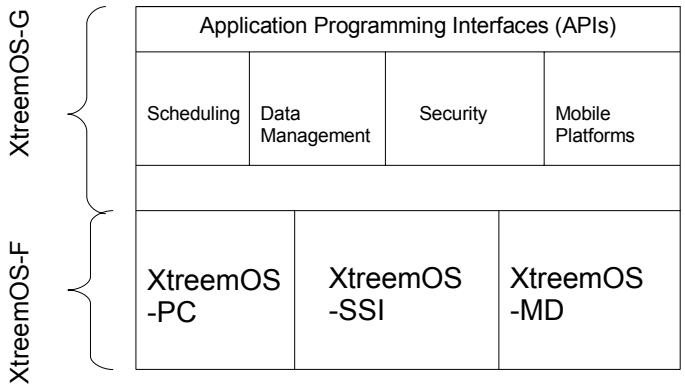

Figure 1. XtreemOS Architecture

For the attack analysis, in the XtreemOS architecture only the two layers, namely XtreemOS–F and XtreemOS–G layer are important to us. XtreemOS–F layer is concerned with kernel–level extensions to the native Linux operating system. As we envisage developing XtreemOS for a variety of platforms, various flavours of XtreemOS will exist to support mobile platforms (XtreemOS–MD), for PCs (XtreemOS–PC) and for clusters (XtreemOS–SSI). The XtreemOS–G layer implements the grid–oriented extensions and services for security, scheduling, data management (XtreemFS) and support for mobile platforms.

Considering this architecture and the overall system, the following are the types of attacks the attacker may execute.

User and Admin Credential Attacks: Attacks on user identity credentials and VO–membership credentials fall into this category. A Grid user credentials are normally proxy certificates given to the user on successful registration. These proxy certificates have a validity period (e.g. for VOMS it is normally 12 hours), which makes the attack harder to execute. These attacks can be carried out either by brute–forcing user passwords, compromising user system to reveal private keys, replaying revoked credentials to inspect cycling or even masquerading as Certificate Authority.

Communication Attacks: These types of attacks focus on gaining credentials and assertions in communications between nodes, VO administrators and VO members. Eavesdropping, packet–filtering of unencrypted communications, brute–forcing encrypted communications etc are examples of these types of attacks.

Site Management attacks: Detecting vulnerabilities in site management and exploiting those vulnerabilities are part of these types of attacks. XML Poisoning, insufficient authentication credential verification (AuthN/Z), insecure logging etc are examples of these attacks. Attacks of this nature should be detected by intrusion detection systems (IDS) and by having strong policies and mechanisms to implement them.

Perimeter and Injection attacks: Attackers may try to compromise a site's perimeter security by tunnelling through firewalls (SSH tunnelling), malicious inputs, dictionary attacks, brute–forcing, SOAP message poisoning etc. Once attackers gain access to site resources, they can try to disrupt communications by denying services or eavesdropping.

Denial of service (DoS) attacks: The attacks of this kind try to disrupt communications and deny services to resources to users. These are probably the best identified and prevalent attacks in current Grid systems. Examples include denying service for registration, job submission, results delivery etc.

In case of XtreemOS, if we consider the architecture in Figure. 1, in the XtreemOS–F layer we need to consider User Credential attacks, Site Management Attacks and DoS attacks.

User Credentials are stored in native Linux as passwords in `/etc/passwd` and `/etc/shadow` files. Security of these files is of prior importance to prevent User Credential Attacks. Proxy Certificates and proxy agents used should be secured and unauthorised tampering should be prevented. Site Management

attacks could be realised by improper management, for e.g. by insecure auditing or logging. For example, we plan to extend the Pluggable Authentication Modules (PAM) to authenticate users. Testing of modules should be done prior to using them in XtreemOS–F and any conflicts with other modules which arise need to be inspected. In addition, in every administrative domain a strong password policy should be implemented in order to mitigate brute–forcing password threats.

Site Management Attacks include a wide range of attacks. If logging is enabled for accountability, logs should be secured and if possible backups stored in a location separate from production nodes. For detecting abnormalities in usage, Intrusion Detection Systems (IDS) and firewalls should be used.

Defence against DoS attacks is difficult. However, proper policy management and implementation can lead to lessening of such attacks. Detection of unauthorised use and proper authentication procedures will make it difficult for attackers to compromise security controls. In XtreemOS–F layer, authorised access control, proper authentication and secure logging and log inspection will lead to a considerable decrease in such attacks.

In the XtreemOS–G layer, the opportunity of attacks becomes wider. From the above classification it is obvious that all the types of attacks can be realised at this layer. A short description is given below.

In the XtreemOS–G layer, we include security services provided to achieve security objectives. In respect to User Credential attacks, security services for authentication become prominent. Communications between users, VO administrators, Certification Authorities (CAs) and other authorities (for e.g. if Kerberos is used than between KTC and user) need to be encrypted. This is not only a requirement in XtreemOS–G, but also a building block for leveraging other services like authorization. Revocation of user credentials is another important aspect at this layer. The revocation mechanism, window of acceptance and updates to Certificate Revocation Lists (CRLs) must be correctly implemented at this layer.

Site Management is a major security issue in this layer. As we are using VOs, VO Management (VOM) needs to be robust against various attacks. VOM should not have conflicting policies and policies should be implemented as designed. In case of node failures, job controllers and users should be notified and before restarting jobs policies should be consulted. Authorization to use resources depends heavily on site management. User roles, capabilities and other attributes need to be verified before granting access to resource. Misconfigurations in any of these critical decisions will lead to vulnerabilities and attack realisation.

DoS attacks at this layer can be realised by denying access to resources and services. For resources, replicas of files can be a considerable defence against these attacks. In addition, regular backups and replicated systems can help in

providing near–constant availability. For services, proper timeout features and suitable error handling can prove to be a defence.

For perimeter attacks, detection of unauthorised use is probably the best method. Site perimeters are often deployed with application and packet–filtering firewalls. Strong firewall rules based on access policies, accompanied by IDS and constant log inspections can help to disregard such attacks. Port scans, unsuccessful login attempts and XML poisoning detection through XML firewalls will help in securing sites against perimeter attacks.

4. Visualising Attacks

In this section, we use a common approach to visualise attacks in networks, namely attacker trees. Having identified a set of attacks in XtreemOS and overall system we here create attacker trees to identify what tools attacker(s) may use to realize these attacks. Due to space restrictions, we only present a single attacker tree here, but currently we are developing a number of attacker trees covering the range of threats to Xtreemos as part of our threat analysis.

Case Study: Unauthorised Access to Resources attack

A specific attack was identified while considering the below attacker tree. The attack is a Site Management Attack whereby the attacker observes the conflict between VO and local site policy and exploits such a vulnerability to mount an attack.

Setting: A realistic setting is assumed in the attack. A set of users are members of the VO and are administered by their local site policy. The VO itself has its VO policies in respect to access, membership etc. A VO manager grants users access to resources. On the resource side, local site administrators govern access to resources. Local site policy for access to resources exists for VO/Grid users. For the current attack, we consider one particular case. Access to resources is granted based on *union* of site and VO policy (for other case studies we also consider other approaches to combine local and VO policies).

Assets: Assets in this case are user credentials, VO attributes, roles (Grid User, VO Admin, Local Admin), filesystems and authentication, authorization, discovery, VO registration services.

Threats: Since we only consider stored data in this case study, we identify the following threats:

- Unauthorised disclosure of information and stored data.
- Unauthorised modification of stored data.
- Unauthorised disclosure of job results.

Attacker Tree: The Attacker tree is shown below with the attack marked.

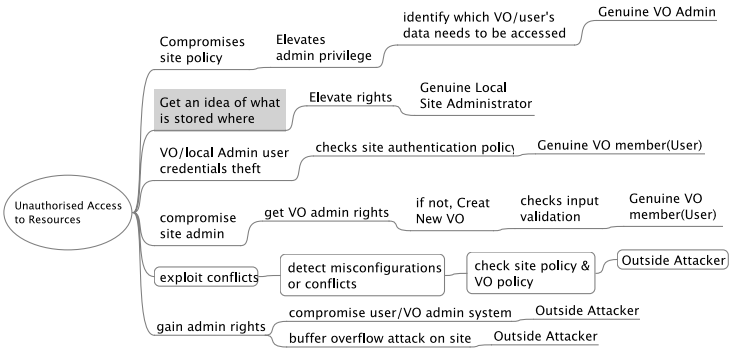

Figure 2. Attacker Tree

Attack: The attack was identified on recursively expanding the attacker tree. In this particular case, as the access is granted based on union of VO and site policies, either a user or VO admin will get more than required access. For example, if VO policy grants only `read` access to a user and the local policy grants only `write` access, the user will have `read/write` access on the resource rather than just a `read` access. Merging VO and site policies is a difficult problem, but we are required to provide a service within XtreemOS that can detect such conflicts if they occur.

5. Conclusions

We have presented here a preliminary threat analysis on XtreemOS, a Grid–enabled operating system. We have identified various threats and attacks in accordance with our set security requirements and visualised attacks in attacker trees. This work is ongoing and we will continue to expand on our threat analysis as our system develops and document a variety of threats throughout the process. A rigorous threat analysis will help in making XtreemOS robust against a wide range of attacks. We will then use this analysis to provide a set of test cases and, thus, provide a level of assurance to the user community. This analysis will also be used for formal security modelling of the XtreemOS system and consequently help in derivation of the system's security policy.

Acknowledgments

We would like to thank all the members of XtreemOS consortium for their constant support and hard–work.

References

[1] Grid Security Infrastructure http://www.globus.org/security/overview.html.

[2] C. Morin. *XtreemOS: a Grid Operating System Making your Computer Ready for Participating in Virtual Organizations*. 10th IEEE Intl. Symposium on Object–oriented Real–time distributed Computing (ISORC 2007) – to appear.

[3] P. Padala, GridOS, http://www.eecs.umich.edu/ ppadala/research/gridos/

[4] Legion Project, http://legion.virginia.edu/index.html

[5] S. Naqvi and M. Riguidel. *Threat model for grid security services*. LNCS. Volume 3470 pp. 1048–1055, 2005.

[6] Demchenko Y., *Web Services and Grid Security Vulnerabilities and Threats Analysis*, EGEE JRA3 Technical document.

[7] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke. *Security for Grid Services*. Proceedings of HPDC–12, pp. 48–57, IEEE Press, 2003.

[8] I. Foster, C. Kesselman, G. Tsudik, S. Tuecke. *A Security Architecture for Computational Grids*. Proceedings of the 5th ACM Conference on Computer and Communications Security Conference, pp. 83–92, 1998.

[9] R. Alfieri, R. Cecchini, V. Ciaschini, L. dell'Agnello, A. Frohner, K. Lrentey, and F. Spataro. *From gridmap–file to VOMS: managing authorization in a Grid environment*. Future Generation Computing Systems. Volume 21(4), pp. 549–558, ACM Press, 2005.