Security Architecture of the Distributed System
– Layered Approach

Miloš M. Cvetanović, Zaharije R. Radivojević

Abstract—Architecture of a security subsystem is a very
important aspect of any computing infrastructure, so, it is not
usual practice to dedicate special attention to problem
addressed in this paper. Modern attack techniques require new
theoretical model for their elimination. Layered approach
incorporated with metadata promises easy extensibility, flexibility
and above all reliable security.

Index Terms—Architecture, Database systems, Distributed
systems, Hierarchical structure, Layer, Layered approach,

I. INTRODUCTION

SECURITY is a very important aspect of any computing
system, and has become a serious problem since
companies and their infrastructure have become distributed in
very heterogeneous fashion. As software on which
infrastructure relies has become ever more complex,
interdependent and interconnected, company’s reputation has
in turn become more vulnerable [6]. Companies that are faced
with a choice between adding features and resolving security
issues need to choose security. In any other case they will be
faced with possibility of compromising sensitive data, loss of
reputation and customer/collaborator confidence in other word
faced with possibility of tremendous financial loss. So, it is
necessary to build new systems incorporating security as
integral part of their design. Instead, many companies and
organizations try to avoid the definition of a security
architecture and jump directly to ad-hoc testing against the
security of their computing and networking infrastructures.

What we need is a security model that should be easy for
developers to understand and build into their applications.
Then again, it must be build upon the appropriate trust model
[1], [7]. Layered approach is a design philosophy for
protecting assets using layers of defensive protections. Each
layer is extensible and therefore capable to respond on
increasing of asymmetric threat and attack tool sophistication.
In order to meet rapidly changing business and technical
requirements flexibility of this model must not be forgotten.
But we have to be aware that ultimate goal of this approach is
security. It will be accomplished through mutually reinforcing,
complementary security controls and processes. So, what we
have here is an architectural strategy implementing “defense in
depth” motto.

Although much of what will be discussed here will be
considered by some as intuitively obvious, it is these principles
that are often forgotten and lead to misunderstandings. Even
experienced researchers and practitioners should review this
document.

II. PRECONDITION

Before we get deeper into the consideration of mentioned
problems, the precondition must be fulfilled. What we need is
a switch in a way of thinking and distinction from traditional
deep-rooted stereotypes. The most evident switch has to be
made in comprehension of central to global networked
environment. Central control has to be delegated to the widely
dispersed nodes with limited visibility of the entire system.
While projecting entire system one should not assume it as
fixed bounded entity, on the contrary one should have in mind
continuously evolving structure and therefore end points and
perimeters should have relaxed boundary. This kind of
structure requires that currently used fortified and insular
approaches to security system design have to be abandoned,
and replaced with one which will include more
interdependency between nodes. There should be no
absolutely trustable node only limited confidence is allowed.
In such environment distinction between insiders and outsiders
disappears. This will enable uniform defense mechanism
whether the attack origins from inside or outside of the specific
node.

Another important switch in the way of thinking includes
importance of the fact that most events occur stochastically
and asynchronously. This is opposite to the current
architectures which base their security systems on the
assumptions of predictability and patterns of the malicious
attacks.

The next suggested change in thinking could cause polemics
about it. It is about collective guilt and responsibility that
should be shared. This is in a contrast with inherent practice of
single point of known responsibility which is held by theory of classical management. Principle of shared responsibility has its argument in the fact that it causes multiple responsibility of each participant and in the same time it will increase fault tolerance of the entire system. Then again, it will make management more difficult and complex. Security of the system should be considered as an essential part of the business infrastructure rather than just an overhead [2]. So, in any way it should not be a question which will be dealt only by technical experts, it should be accepted as a risk management perspective which will require involvement of the whole organization. It is not important to insure complete secure of each node, but to provide survival of mission. In other words survivability over security.

III. OVERVIEW OF THE EXISTING ARCHITECTURES

Purpose of this section is to emphasize the lacks of the current available security systems. Majority of existing systems are burdened with the uniform protection of all the parts whether they are mission critical or not. This may cause overhead of the resource utilization in the cases when only important assets need protection. Another important disadvantage of legacy security systems is their basic paradigm that says “all or nothing”. But instead of that, the “show must go on” paradigm must be used. Also, static structure of the security systems implies the impossibility to accommodate to a new and sophisticated attack tools. Dynamic prediction of the malicious attacks should be incorporated as basic functionality, but with the existing architecture only post-attack analysis is possible.

Most of the present systems have some kind of hierarchical structure but not the structure in which multiple independent supervisors can act in order to protect the important resource.

Issues that can not be neglected are inabilities of the existing systems to adopt themselves to everyday needs in the company’s workflow. That means that these systems are inappropriate for the modern concepts of total management of entire system. From all the issues mentioned above it could be concluded that new methodology in system architecture is an essential need.

IV. LAYERED APPROACH

Glance on existing distributed systems reveals their variety of node dispersion across wide geographic regions. Nodes typically belong to the large-scale private networks and are not necessarily connected through Internet. What we are dealing with is a complex information system with the characteristics that are general and common for other infrastructure systems. In this kind of system, security must be considered at all stages of design, which not only satisfy their functional specifications but also satisfy security requirements.

The main idea is the decomposition of a system into hierarchical layers of abstraction, where the higher levels monitor lower levels by using some of their services and data produced in a regular operation mode. The lowest level (node level or functional level) consists of the interconnected nodes whose security architecture is based upon hierarchical multilevel design. The internal security design of each node is depicted on the Figure 1. This figure differs from the standard one because each level provides unique interface based on metadata [4]. This additional complexity has practical consequence that will allow upper levels (see Figure 2) to make probes at any level inside of the particular node. Upper layers (control layers) are designated for real-time monitoring and management of the lower layers. All layers operate independently and in parallel, but not necessarily on different machines. Although, executing on the same machines can be a significant resource drain, running them exclusively on the separate nodes is beneficial for efficiency reasons. Because of the scale and the complexity of the presented system, each node in the upper layer is responsible for managing a set of the

Figure 1. The internal security design of each node. This figure differs from the standard one because each level provides unique interface based on metadata. Dark levels represent metadata levels, which will be used as access points for probes.

Figure 2. Security Architecture of the Distributed System – Layered Approach. Upper layers (control layers) are designated for real-time monitoring and management of the lower layers. The lowest layer is functional layer. Arrows are directed from observers toward subjects of monitoring. Note that nodes on different layers are not necessarily on separated machines.
nodes in the layer beneath it. These sets in lower layers are not
disjunctive, in other words any node could be subordinated to
the more then one node from the upper layer. This kind of
structure implies that two basic principles of security are
accomplished (diffusion and confusion). Mechanism by which
upper layer could gather data from the node in the lower layer
is by set of monitoring and actuating programs (probes) [3].
With the collected raw data, upper layer node can execute
analysis programs. If analysis report any disparity from the
normal results, such event could be handled generally in two
ways. Locally, with some additional data requested from the
node on the same or lower layer (not necessarily involved in
the situation). Globally, by sending error signal to the upper
layer nodes, and sending warning to the nodes on the same
layer. As we have already mentioned metadata is used in intra-
layer communication of each node. That provides probes with
ability to accommodate and to work with heterogeneous nodes.
In some cases probes are assigned to the control function, and
it could lead to the collision with some other control probes.
This could be solved with some kind of priority mechanism,
which would preserve unique command chain of the
architecture, but this is not topic of this paper.

The architecture, as described above, gives rise to a series of
security concerns. These security concerns can be grouped into
two loosely-defined categories. The first category is node
protection, which includes both protecting of the node integrity
and protecting the appended probes. Each node, as stated
before, has its own multilevel internal structure (Figure 1), and
is also defended by the one (or more) nodes from the upper
layer. The second category is inter-node communication
protection. This communication usually occurs over network
channels, whose defending mechanisms are part of traditional
security theory.

Described architecture poses one very important
characteristic that is desirable not only for administrators but
also for users and developers. It is transparency of whole
security system which is achieved by multiple abstraction
levels interconnected with metadata exchange [5]. Presented
security model fits into a hierarchy of standard transparencies
as shown in Figure 3. It is not always easy to delineate clearly
the levels of transparency, but such a figure serves an
important instructional purpose even if it is not fully correct

Beside all that was already mentioned in the previous
sections proposed architecture have three more implicit
advantages. The first one arises from metadata usage, and it
enables dynamic reconfiguration of the defense architecture
(increased flexibility)[8], [9]. The second one is presented
through system capability to survive node failure (increased
fault tolerance). And, the third one presents the opportunity to
use data mining techniques in order to advance prevention
measures (increased attack prediction) [10].

\[ \text{Figure 3. Layers of Transparency. Presented security model fits into a hierarchy of standard transparencies between Data Independence and Network Transparency. All layers which encompass security layer are not burden with security details.} \]
VI. CONCLUSION

In this paper we have presented a new methodology for architecture of the entire security system. It could be also used like an upgrade on the existing systems. Sustainability and robustness of this approach is appropriate for the requirements of the modern dynamic structured systems. Layered approach incorporated with metadata open numerous possibilities for self-modifying structure that would be adequate answer to the modern trends of asymmetric attacks. Most of these are yet to be explored, but some of the techniques like data mining could be already used for increasing real-time prevention measures.

REFERENCES


