CERIAS Tech Report 2001-100
Applying Fault-tolerance principles to security research
by A Bhargava, B Bhargava
Center for Education and Research
Information Assurance and Security
Purdue University, West Lafayette, IN 47907-2086

Applying Fault-tolerance principles to Security research

by

Anjali Bhargava
TRW, Redonodo Beach CA 90278
bhargava_anjali@hotmail.com

Bharat Bhargava
CERIAS and CS Dept
Purdue University
bb@cs.purdue.edu

We have been conducting research in reliable distributed systems in the last twenty years. We have worked on the development of concepts such as consistency, atomicity, durability, availability, rollback, check points, adaptability etc. [1,2]. IEEE symposium on Reliable Distributed systems held every year contains many of the papers dealing with high availability, dependability, and non-stop operations of applications. The IEEE symposium on Fault-tolerance is another source.

Recently there has been much focus on building secure distributed systems. CERIAS center has been established at Purdue along with 14 other such centers in USA. We note that many of the ideas, concepts, algorithms being proposed in security have many common threads with reliability. We need to apply the science and engineering of reliability research to the research in security and vice versa.

We briefly give some examples to illustrate the ideas. To increase reliability in distributed systems, the use of quorums allows the transactions to read and write replica even if some replicas have failed or are unavailable. So the systems manage the replicas so that a forum can be formed in the presence of failures. To make systems secure against unauthorized access, one can use the reverse strategy of making it difficult to form quorums. All accesses require permission from a group of authorities who could coordinate to deny a yes majority vote.

Checkpointing research has similarities to the work in intrusion-detection. In both cases, monitoring of either failures or security violations are recorded. The checkpoints ensure that the systems can be brought to a safe consistent state through the use of recovery lines. Such checkpoints can be used to determine secure and safe states of a system. The action taken to rollback to a consistent state will be similar to bring the system to a secure status.

To deal with failures, we build systems that are adaptable. This way, we can deal with the type, duration, severity, timing, extent of a failure. The system will dynamically reconfigure and utilize the best scheme to deal with a specific situation. We must build systems adaptable to security attacks in the same way. The models, experiments, and infrastructure of adaptability to failures with failures are very similar to the ones needed for adaptable secure systems.

A failure can be classified as functional or operational. Functional failure implies that a component of the system has failed while the operational failure implies that system is unavailable due to heavy traffic or load. Denial of service attacks are like the operational failures and the solutions to these problems in security or reliability research are similar.

There is no way that we can make a system one hundred percent reliable or secure. In the past, we have designed schemes that deal with one failure and integrated such schemes to build reliable systems. We actually believe that failures will come and go just like a person can get sick and healthy. We actually can not worry about each individual failures and spend all our resources in dealing with it. We need to identify transient and non catastrophic errors and failures and ignore them if it can benefit the system in dealing with severe causes of non availability. In the same tune, we need to conduct research in dealing with benign security violations that are part of daily system activity. In addition, we must find optimal solutions that allow the applications to succeed inspire of a large mix of failures, security attacks when large number of processes are communicating and accessing large databases.

Such effort is expected to lead us towards a dependable computing system that is adaptable to meet the performance, reliability and security requirements.

[1] B. Bhargava (Editor), “Concurrency Control and Reliability in Distributed Systems", Van Nostrand and Reinhold, 1987.

[2] B. Bhargava, S. Babu, and S. Madria, “Fault-Tolerant Authentication and Group Key Management in Mobile Computing", *Proceedings of International Conference on Internet Computing* (Special session on advances in security), Las Vegas, June 2000, pp 67-76