Data Destruction – How can you destroy data and prove it is destroyed?

Dan Pollack
AOL LLC
dpollack@aol.net

The disposal of storage hardware used to store sensitive information is a subject of constant interest. The seemingly simple task of destroying data takes on a surprising amount of complexity. Maintaining consumer trust and, in some cases, laws require that data stored on customers behalf be disposed of in a manner that keeps the customers data private. The cost of maintaining storage systems and support systems can be a burden if the data destruction process is lengthy. The increased load placed on storage devices during data destruction can cause accelerated wear-out and failure. The added complexities due the requirements of proof of data destruction, the desire to do the job quickly, and the physical aspect of the process can create significant problems.

As consumer services are discontinued the opportunity to discover the best methods to destroy large amounts of data has presented itself. The data is stored in several different ways on various storage systems. The total amount of data being destroyed is several petabytes in size. The data is protected by several online methods including RAID, block replication, and file replication. The data is accessed by block, file, and object methods.

The destruction methods that are under investigation include RAID reconfiguration, data over-write at the file level, data over-write at the block level, and physical destruction of disk drives. Overwriting seems to be an acceptable and sufficient data destruction method in most cases[1]. The main concerns are proof that the data has been destroyed and efficiency of the process to reduce the time required for data destruction.

An examination of the methods of data destruction and how they can be applied to each data storage system should produce a set of techniques for efficient data destruction on the types of devices being operated on. The assumption is that a combination of the destruction techniques excluding physical destruction will be the least time consuming and most economical.

The method of reporting proof of data destruction will have to be developed to the satisfaction of the auditors of the process. Data sampling from the storage devices and tracking of all storage devices that go through the data destruction process is expected to be necessary. Additional data may need to be provided in the proof of destruction.

We expect to be able to meet our goal of protecting customer data and privacy while economically destroying data from decommissioned storage systems.

References

1. Kissel, R., Scholl, M., Skolochenko, S., and Li X., Guidelines for Media Sanitization NIST Special Publication 800-88