Enhancing the security of cloud server configuration with hash chains

Gautam Kumar
Computing and Software Systems
University of Washington Bothell
gautamk@uw.edu

I. Executive Summary

Information security is a difficult problem, especially in cloud computing environments where threats to information security are difficulty to identify and mitigate. One such problem is managing the sensitive configuration information.

In traditional enterprise deployments developers often stored configuration within code or on config files along with code. This was considered a safe practice because the hardware and Operating System where code deployment occurred was owned and managed by the enterprise themselves. These systems were usually behind a strong firewall so threats were much easier to mitigate.

In cloud computing environments, where hardware and the underlying software hypervisor are shared amoung thousands of customers who could potentially be using the resources of a single data center, Threats to security are much more complex and we need a layered strategy to secure our systems. In this environment storing sensitive configuration information on disk could potentially be dangerous.

One of the ways developers have secured systems in this environment is to use a centralised trusted server to store and retrieve sensitive configuration information. The goal of this project is investigating ways to improve the security and allow for forward secracy using Hash Chains[1].

II. Project Description

The project description must include the activities that you plan for your research. Provide sufficient background so that a reviewer can understand what you are going to do. Provide a sufficient survey of related work so that a reviewer understands what work has been done before and where your work will fit in the state of the art (for example, if reputation systems have been built for well-connected networks, but they rely on assumptions that no longer hold in a new type of network, tell the reviewer about the existing state of the art and identify why your new reputation system must be created because the old ones won't work in the new network). You also must include a section on Broader Impacts that describes why your topic is important to the world and a section on Intellectual Merit that describes why the problem you are addressing is technically rigorous.

References

[1] Biming Tian, Song Han, T. S. Dillon, and Sajal Das. A self-healing key distribution scheme based on vector space secret sharing and one way hash chains. In *World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008. 2008 International Symposium on a*, pages 1–6.