Mitigating Ransomware Attacks by Leveraging Isolation Techniques

Bo Chen, Ph.D., PI Research Assistant Professor Department of Computer Science University of Memphis, Memphis, TN 38152-3240 Phone: (901) 678-2277; Fax: (901) 678-1506 Email: bchen2@memphis.edu

Dipankar Dasgupta, Ph.D., Co-PI Dr. Pat E. Burlison Professor Department of Computer Science University of Memphis, Memphis, TN 38152-3240 Phone: (901) 678-4147; Fax: (901) 678-1506 Email: dasgupta@memphis.edu

1 Introduction

Ransomware attacks suddenly become very prevalent in recent years with the flourishing of crypto- currencies like bitcoin. Due to their highly anonymized nature, crypto-currencies offer ransomware makers a great mean of receiving ransom money without being identified. A recent security incident caused by a ransomware attack infected 900 systems used by the San Francisco Municipal Transportation Agency [1].

Similar to malware, ransomware utilizes all types of means (e.g., spam emails, mal-advertisements, social engineering) to propagate to a victim computing system. Then, it will either lock the victim system or encrypt the data in the victim system. Finally, it will require the victim to pay the ransom money in order to unlock the system or obtain the key for decrypting the data.

Paying the ransom money, however, may not guarantee recovery of the encrypted data. Even worse, this provides incentive to the ransomware makers to improve their ransomware and launch more advanced ransomware attacks. In general, if the victims periodically back up their data using external storage media or public cloud services, the ransomware attack would not even become an issue. However, most people today are reluctant to back up their data for the potential ransomware attacks, due to the following reasons: (i) people usually do not even think they will become ransomware victims until they are really attacked; (ii) periodically backing up data will create additional work burden; (ii) backing up data in external storage media or public cloud services requires the users to plan additional budget in purchasing hardware equipment or cloud services.

Considering the difficulty of decrypting data without knowing the key, a better ransomware defense strategy should still rely on data backup while being able to resolve the aforementioned concerns. For (i), we can raise the awareness of ransomware attacks by education or media campaign. For (ii), we can simply

automate the backup process so that user data can be automatically backed up. For (iii), we observed that for most people, their PC computers usually have a significant amount of spare space which can be utilized to back up the entire or portion of the user data. By utilizing this spare space, we can store the backup data, unbeknownst to the ransomware. A key challenge is, as ransomware may obtain root privilege by exploiting vulnerabilities in the victim system (i.e., the ransomware may have the same privilege as the user), it will be difficult to hide those backup data from ransomware.

Research objectives. In this project, we aim to resolve the aforementioned challenge by leveraging isolation techniques and cryptographic secrets, such that the backup data can be stored in the local storage medium while being able to avoid being damaged by ransomware. This is highly advantageous as it can mitigate ransomware attacks by fully utilizing all the existing computing/storage resources in the victim computing device, eliminating the need of purchasing additional storage media or storage services.

Intellectual merit. This project will significantly contribute to both theory and practice of ransomware defense and mitigation. Specifically, the project has several merits: First, it will significantly promote the research on ransomware defense and mitigation by, for the first time, exploring the spare resources (e.g., storage space) in the victim systems; Second, it incorporates the advanced computing techniques like hardware-based or software-based isolation into the computing systems. Third, the research results from this project will be incorporated to CfIA's course development (Center for Information Assurance has received several grants from FEMA/DHS for developing cyber security courses in the past few years, and has trained more than 20,000 people since 2009). This allows immediate integration of our ransomware research into training and education of cyber security professionals as well as non-technical people, which indirectly helps to prevent and defend against ransomware attacks, as keeping safe from ransomware attacks is ultimately the job of people.