Security Patching for Docker Images

Rui Shu
Work with Dr. Xiaohui Gu and Dr. William Enck
Previous Work

• Docker Container (Next evolution of a Linux packaging system)
• A study of security vulnerabilities in Docker Hub
• Submitted to CODASPY ’17 (11 pages, Sep 25th)
Previous work

Docker Image Vulnerability Analysis (DIVA) System Framework
Previous work

• In our previous work, we proposed a scalable Docker image vulnerability analysis (DIVA) framework for automatically discovering, downloading, and analyzing vulnerabilities in images from Docker Hub.

• DIVA also accesses vulnerability propagation between images.

• We use DIVA to analyze over 300,000 images and found significant and pervasive vulnerabilities in Docker Hub images.

• We also found strong correlations between top influential images and top ranked vulnerable packages, which implies that the widespread image vulnerabilities are likely the result of propagation from a small number of influential images.
Broad impact

- In January 2015, one survey of enterprises indicated that security was a top concern when deciding whether to deploy containers, it also found that of various security concerns, vulnerability and malware concerns were the greatest.

- Our work will endeavor to mitigate the security threats in Docker images, in order to prevent several security issues (e.g., privacy leakage, malicious applications).
Research Goals

• To devise an approach to dynamically patch the security vulnerabilities in Docker images.

• To ensure the correctness of the patching, which means the security patch will not bring side-effect or influence current application in Docker image. If the patching has a bad influence, we should find a way to address it.

• To achieve a high efficiency (e.g., reduce the downtime of current application, or incur a low overhead to the host)

• To make our security patching technique scalable, which means this technique can scale to a large number of vulnerable images.
Data Collection

• In our previous work, we have leveraged Clair to detect vulnerabilities in each image.

• Clair is an open-source tool from CoreOS designed to identify known vulnerabilities in container images against CVE database.

• We have collected vulnerabilities from 356,218 Docker images.

• We will collect several information of unpatched images and patched images. (e.g., we will compare data from successfully patched images and unpatched images).

• We may also compare host resource usage to identify the overhead of our technique.
Success Criteria

• The primary success criterion is the correctness of our security patching, i.e., the patch will not influence current running of image.

• In addition, we plan to reduce the overhead of patching to a low level, and make our technique be applicable to a large number of images.
Difficulties

• How to dynamically patching an application image, since the type of application in image is various (e.g., single process application and multi-thread application)

• How to reduce the patching overhead. Our technique is a dynamic security patching, for a running image (i.e., the running container), we also need to reduce the overhead of migrating data and context from current running image to patched image.

• How to scale the patching technique to large number of images. One thought is to identify similar characteristics between a group of images, this may reduce the work for duplicated patching.
Thank you!

Questions?