We Won't Borg You With The Details

Make SA Great Again
Dalton Ellis, Gib Filter, Neil Hartje

Introduction:

For our second project deliverable, we will discuss four points dealing with the requirements and design for secure software. The first is links to our version control internal collaboration performed between each of our team members. The second discussion point is the security requirements using misuse case diagrams. The next point is threat models for critical dataflows of Borg. The last discussion point suggested updates for project documentation.

Version Control Links:

Below are the links to our internal collaboration and project related activity. The first link is to lucidchart, where we created our misuse case diagrams. The second link is to our Google Drive folder housing Google Doc and collaborated materials, including our threat models. The last link is to our Github repo hosted by Dalton that was forked from Borg.

1. https://www.lucidchart.com/invitations/accept/792cf4c9-f29f-4514-bcbc-a34f93754cde
2. https://drive.google.com/drive/folders/0B29GWew9jSP5SXN4dWhEYW9WalU?usp=sharing
3. https://github.com/dlellis/SAProject

Security Requirements Using Misuse Case Diagrams:

A direct link to our diagrams is as follows:
https://www.lucidchart.com/invitations/accept/792cf4c9-f29f-4514-bcbc-a34f93754cde

Claim 1: Hashed, encrypted backup data reasonably protects information integrity.
Misuse Summary: Data is tampered with and decrypted messages are modified.
Requirement: Hash encrypted data to provide message authentication.

Claim 2: All encryption key weaknesses have been sufficiently mitigated.
Misuse Summary: Encryption useless due to key weakness
Requirement: User proper key generation and management techniques

Claim 3: Borg's automatic backup process minimizes the loss of data.
Misuse Summary: Natural disaster affects original data source
Requirement: Constantly update backup and use a redundant power supply

Claim 4: Borg's validation process prevents unauthenticated access to backups.

Misuse Summary: Unauthorized user gains access to backup

Requirement: Require passphrase for each backup created by a user, different from their password

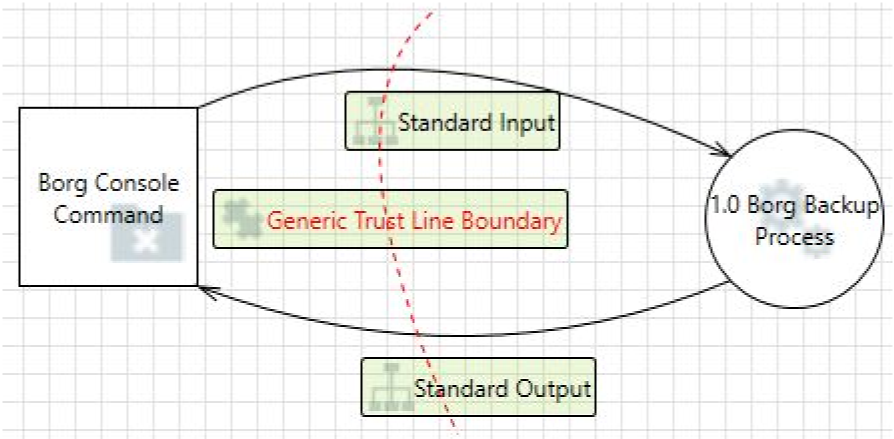
Claim 5: Encrypting data locally reasonably protects data in transit.

Misuse Summary: Attacker uses man in the middle to read data in transit

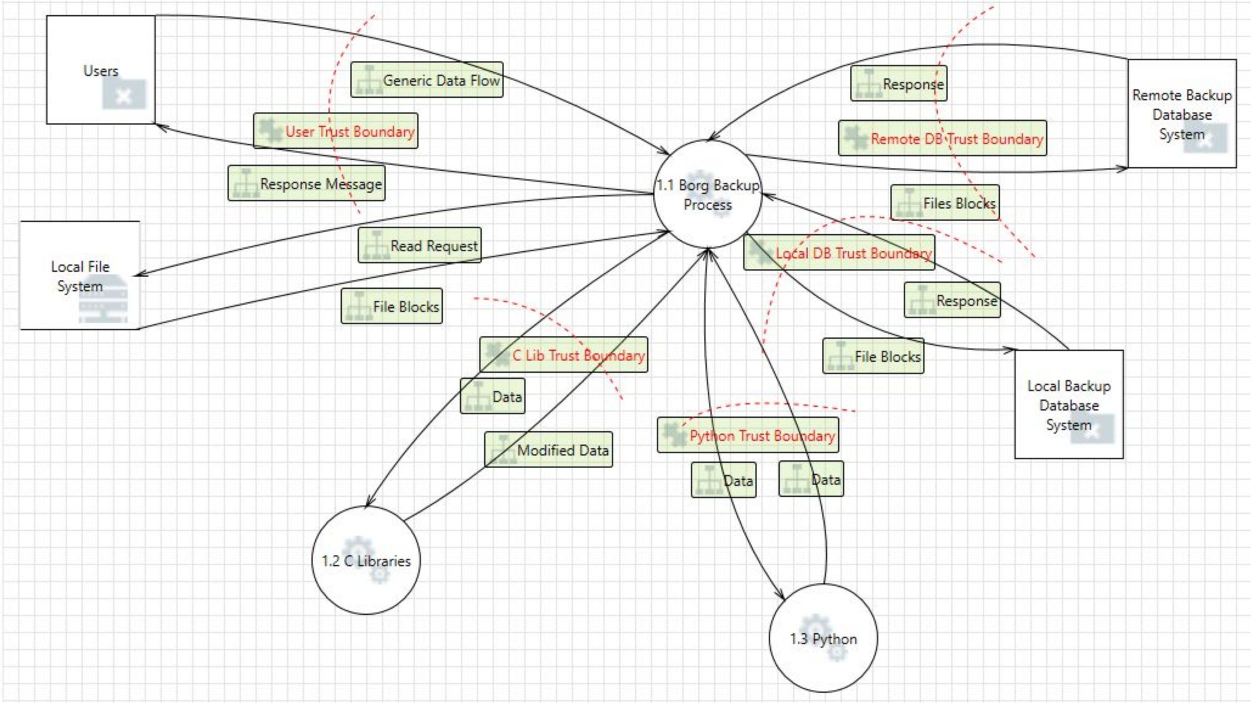
Requirement: Encrypt data locally prior to transmission

Threat Models For Critical Dataflows:

Below is the Level 0 diagram for misuse cases.



Below is the Level 1 threat diagram. Note:If an attacker can access or modify local files and other programs, then Borg is susceptible also.



A link to the full report can be found in our Google Drive folder:
https://drive.google.com/drive/folders/0B29GWew9jSP5SXN4dWhEYW9WalU?usp=sharing.

Links To Suggested Updates For Project Documentation:

A direct link to our suggested updates is as follows:
https://docs.google.com/a/unomaha.edu/document/d/1EfiMq1Kpi4haHGXoPyqSf8h8I3AnGYuzZB908Hnhhgs/edit?usp=sharing

Conclusion

This second project deliverable provides a solid foundation for our next project deliverable: Code analysis and testing for Secure Software. Having a solid understanding of where the faults in the program will most likely occur will make code analysis quicker and more productive. In this project report we discussed our group collaboration, misuse case diagrams, threat model diagrams, and suggested documentation updates. This section of the project helped us in determining the subject matter for our pull request for Borg, which is adding a logging feature to Borg.

References

[1]https://www.lucidchart.com/invitations/accept/792cf4c9-f29f-4514-bcbc-a34f93754cde
[2]https://drive.google.com/drive/folders/0B29GWew9jSP5SXN4dWhEYW9WalU?usp=sharing
[3]https://github.com/dlellis/SAProject