SERVER LOG ANALYSIS

March 26, 2018

Scott McCoy
Dr. Todd Wilson

INTRODUCTION

New computer systems are created and used daily that affect businesses and institutions both large and small. As the prevalence of enterprise computer systems grows, so too does the profitability of attacking such systems. With the quickly changing culture of software development security holes can easily be introduced as new APIs and frameworks become available but these security risks can go months or years without being patched. This means that often times it is not a question of if a user account will be compromised but when a user will be compromised When a user of one of these systems is compromised a myriad different types of information is at risk of being stolen by attackers. Libraries risk losing their databases of research papers, businesses risk databases of customer information, and governments risk their national security.

The purpose of this project was to combat such attackers by attempting to identify compromised users and alert relevant information security personel before damage can be done. This was achieved through analyzing the log files of a server in real time in order to identify and respond to any users that exhibit suspicious behavior. The initial motivation for this project came from a university library that was having trouble with compromised user accounts that would download as many academic papers and journals as possible for resale. This would result in the affected databases being locked to the entire university until administrators were able to prove to the database provider that the attacker had been dealt with.

LIBRARIES AND RESOURCES

[talk about libraries used and other programs that were examined to inspire this one, linux features]

DATA STRUCTURES

[talk about data structures used, make diagrams]

ALGORITHMS

[talk about algorithms used]

PARADIGMS

[talk about online processing as a paradigm and why this was a necessary approach to the problem]

FUTURE WORK

[talk about future work that could be done for this project and projects that could take inspiration from this one]