6a.010.DU - Log-Based Anomaly Detection Through Correlation & Behavior Analysis for Cybersecurity

Year 6 - Deep Dive Video

6a.010.DU_Deep Dive Video (27:02 minutes)

Project Description

Anomaly correlation analysis for cybersecurity aims to discover correlated cyber activity patterns that exhibit notable departure from common patterns. For example, botnet is a distributed software that runs coordinated programs over target websites to perform malicious tasks like skewing website statistics, price scraping, spam distribution, DOS attack, etc. Discovering bot activities can help prevent significant economic losses for many enterprises that rely their business on websites. Although log data have been commonly leveraged for cyber anomaly detection, current methods are typically batch-based and not able to perform real-time detection on large-volume streaming data. Moreover, low-level or hardware-related information is usually part of the analysis, where such information is sometimes sensitive and needs additional effort to collect and pre-process. To overcome these limitations, our project aims to formulate general methods that discover anomalies based on application-level logs, such like Apache logs for website servers. The application-level logs are provided by applications that host certain network services, usually nearly structured and readily available for data analysis. The objectives of this project mainly include: 1) design novel methods to discover correlated anomalies from large-volume streaming log data; 2) design methods to understand the purpose of those anomalies, providing rich information for better management decision.

Project Team

Team Member	Role	Email	Phone Number	Academic Sites/Industry Members
Xiaohua Tony Hu	PI	Xiaohua Tony Hu	(215) 895-0551	Drexel University
Zheng Chen	Student Researcher	zc86@drexel.edu	(215) 939-5997	Drexel University
Chris Page	IAB Project Mentor	Not available	Not available	**Funded by:** GlaxoSmithKline (GSK)

Project Deliverables

	Deliverable
1.	A software that simulates bot/botnet visits on a website.
2.	A novel Lanczos-iteration based algorithm to detect correlated anomalies from streaming server log data.
3.	A novel Markov-chain based behavior model to detect single anomalies from streaming server log data.
4.	Scientific publication.

Project Documents

For viewing/editing options, please click left arrow next to document name.

You will see different options depending on your access level.

Attention Project PIs

PIs are responsible for keeping up the content of their project page and have the ability to EDIT the page.

- To **EDIT**, click the edit "pencil icon" in the top right-hand corner of this page
- To **PUBLISH** your changes, click the blue "Publish" button in the lower right-hand corner of this page
- If you need help or have questions, please contact Site Admin: Sally.Johnson@louisiana.edu

Table of Contents

Spaces

- All Spaces

CVDI 2017 IAB Fall Meeting

CVDI 2018 IAB Fall Meeting

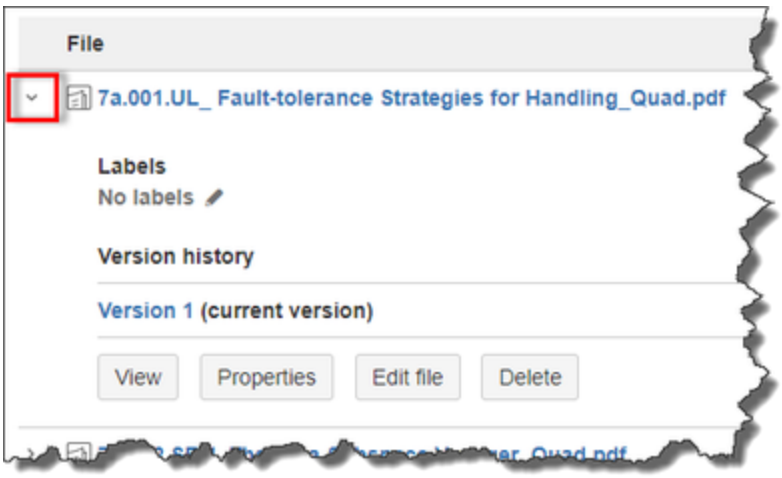
CVDI 2018 IAB Spring Meeting

CVDI 2019 IAB Fall Meeting

CVDI 2019 IAB Spring Meeting

CVDI Calendar

CVDI Leadership (All Sites)



File	Modified
6a.010.DU_Executive Summary_REVISED.docx	Oct 11, 2017 by Sally Johnson
6a.010.DU_Poster_PDF.pdf	Oct 11, 2017 by Sally Johnson
6a.010.DU_Poster_PPT.pptx	Oct 11, 2017 by Sally Johnson
6a.010.DU_PPT Presentation.pptx	Oct 11, 2017 by Sally Johnson
6a.010.DU_Quad Chart.pptx	Oct 11, 2017 by Sally Johnson
6a.010.DU_Executive Summary_ORIGINAL.docx	Oct 11, 2017 by Sally Johnson
11-10-2017 11-28-32 AM.png	Nov 10, 2017 by Sally Johnson
6a.010.DU_Log-based Anomaly Detection_Poster_2017 Fall Meeting.PPTX	Nov 13, 2017 by Sally Johnson
6a.010.DU_CVDI Mid-Year Report.docx	Jan 04, 2018 by Sally Johnson
6.010.DU_Poster_2018 Spring Meeting.PPTX	Mar 16, 2018 by Sally Johnson

Drag and drop to upload or browse for files

Download All

Project Comments

- CVDI Marketing Materials
- CVDI Reports & Document Library
- CVDI SITE (Drexel University)
- CVDI SITE (Stony Brook University)
- CVDI SITE (Tampere University)
- CVDI SITE (University of Louisiana at Lafayette)
- CVDI SITE (University of North Carolina at Charlotte)
- CVDI SITE (University of Virginia)
- IAB - Industry Advisory Board
- Year 6 - Funded Projects (7/1/17 - 6/30/18)
- Year 7 - Funded Projects (7/1/18 - 6/30/19)
- Year 8 - Proposed Projects