Institute for Cyber Security Overview

Ravi Sandhu
Executive Director
Professor of Computer Science
Lutcher Brown Chair in Cyber Security

October 2019

ravi.sandhu@utsa.edu
www.ics.utsa.edu
www.profsandhu.com
MISSION
Excellence in graduate-level sponsored research

2007-2012
Founded by start-up funding from State of Texas

2012-2017
Graduated to a self-sustaining operation

2017-2022
Major expansion by winning NSF C-SPECC grant

- FlexCloud & FlexFarm
  - World class research laboratories
  - Sustained production of PhD graduates and sponsored research

In collaboration with:
- College of Engineering
- College of Business
- College of Education
- Open Cloud Institute
- Cyber Center for Security & Analytics

Partnership with 4 NISD High Schools:
- Harlan, Woodson, Taft, Business Careers
Holistic Cyber Security Research

Objectives

Enable
Enforce

POLICY
What?

ATTACKS
Why?

Respond
Defend

Mechanisms

PROTECT
How?

DETECT
Complement
Holistic Cyber Security Research

Requires

Institute Level Effort
World Class Laboratories
Global Collaborative Connections

© Ravi Sandhu

World-Leading Research with Real-World Impact!
ICS Major Research Thrusts

APPLICATION DOMAINS
Cloud Computing, Internet of Things (IoT), Social Media, Big Data, Mobile Platforms, Enterprise, Insider Threat, Scientific Infrastructure, Smart Homes, Smart Cities, Smart Cars etcetera

FOUNDATIONAL TECHNOLOGIES
Access Control, Policy, Malware, Forensics, Blockchain, Artificial Intelligence, Machine Learning, Data Provenance, Formal Methods etcetera

WORLD CLASS LABS
FlexCloud
Flex Farm

Goal: Broaden and Deepen
Facts and Figures

PAST SYNOPSIS
- PhDs graduated: 27
- External funding raised: $22M

CURRENT STATUS
- Faculty affiliates: 22
  - College of Sciences: 8
  - College of Engineering: 7
  - College of Business: 6
  - College of Education: 1
- Current PhD students: 29
  - College of Sciences: 19
  - College of Engineering: 7
  - College of Business: 2
  - College of Education: 1
  - Domestic vs Foreign: roughly 50-50
• This slide was intentionally left blank.
Institute for Cyber Security: Galahad Project

James Benson
Technology Research Analyst

October 2019

James.Benson@utsa.edu
www.ics.utsa.edu
https://gitlab.com/utsa-ics/galahad
• Research Data Center (RDC) was opened in the summer of 2012.
• Total square footage for servers is 1,632 sq. ft.
• The entire MS RDC is 3,558 sq. ft.

• Our equipment consists of over:
  • 1,300 threads,
  • 10TB of RAM,
  • 370TB of storage, and a
  • 10GB backbone.
• Galahad was Star Lab’s solution for IARPA VirtUE program - Virtuous User Environment (VirtUE).

• 4 Original Contenders:
  • Star Labs;
  • Raytheon BBN;
  • Siege Technologies;
  • and Next Century

• Galahad is unique in that it was transitioned from Star Labs to ICS; We have open-sourced it. To create a turn-key opensource deployment tool to share it with others.
• Objective: Detection and mitigation of threats attempting to exploit, collect, and/or effect user computing environments (UCE) within public clouds

• Cloud service providers have not offered any “game changing” security solutions
  • Adversaries can leverage an arsenal of capabilities used to succeed
  • Providers cannot necessarily be trusted

• Current end-point security solutions and analytical approaches are not tuned for cloud environments
To combat threats in a public cloud, isolate, protect what is controlled, and maneuver

- Do not attempt to establish trust
- Do not require special cloud services, e.g., dedicated servers
- Impede the ability of adversaries to operate within AWS by making it more difficult to co-locate
- Force adversaries to consume more resources thereby increasing the accuracy, rate, and speed with which threats maybe detected
- Facilitate the creation of role-enabled security models
- Reduce attack surface area, hardened kernel, real-time sensing, limit resources.
Galakhad VirtUE

Containers for easy packaging and security configuration

A nested hypervisor to facilitate regular, recurring live migration of Unity VMs inside AWS

© James Benson
Sensing/control Capabilities

• Valor:
  • Network communications,
  • Virtual memory remapping,
  • Physical device access

• Unity/VirtUE:
  • Process creation,
  • Storage usage,
  • Network access
  • Libraries loaded by Win processes
  • Attempted access to privileged resources

• Docker:
  • Start/Stop services
  • Enable/disable ports
Galahad Components

- **UNITY**
  - Windows App(s)
  - Wine Server
  - Wine Instr.
  - syslog-ng client
  - Local Storage
  - SYSLOG
  - PROCESS KILLER
  - NET_BLOCK KERNEL MODULE
  - LINUX KERNEL
  - LSM
  - GAIUS
  - INTROSPECTION MONITOR

- **VALOR**
  - Excalibur
  - Heartbeat Listener
  - RethinkDB

- **EC2 INSTANCE**
  - EC2 INSTANCE
  - Windows App(s)
  - Wine Server
  - Wine Instr.
  - syslog-ng client
  - Local Storage
  - SYSLOG
  - PROCESS KILLER
  - NET_BLOCK KERNEL MODULE
  - LINUX KERNEL
  - LSM
  - GAIUS
  - INTROSPECTION MONITOR

- **UNITY**
  - syslog-ng client
  - Local Storage

- **UNITY**
  - syslog-ng client
  - Kibana
  - ElasticSearch

- **Admin**
  - Wine Server

© James Benson
Questions?