Large-scale distributed virtualized computing infrastructures have become important platforms for many critical real-world systems such as cloud computing, big data processing, and intelligence analysis. However, due to its inherent complexity and sharing nature, virtualized computing infrastructures are inevitably prone to various system anomalies caused by software bugs, hardware failures, and resource contentions. The situation exacerbates if the system is also exposed to malicious attacks. Moreover, although some anomaly symptoms such as machine crash are easy to detect, many other anomalies (e.g., performance degradation, processing bottlenecks, memory leaks) are more subtle and harder to identify.

The views, opinions and/or findings contained in this report are those of the author(s) and should not be construed as an official Department of the Army position, policy or decision, unless so designated by other documentation.
ABSTRACT

Large-scale distributed virtualized computing infrastructures have become important platforms for many critical real-world systems such as cloud computing, big data processing, and intelligence analysis. However, due to its inherent complexity and sharing nature, virtualized computing infrastructures are inevitably prone to various system anomalies caused by software bugs, hardware failures, and resource contentions. The situation exacerbates if the system is also exposed to malicious attacks. Moreover, although some anomaly symptoms such as machine crash are easy to detect, many other anomalies (e.g., performance degradation, processing bottlenecks, memory leak bugs) are hard to detect and diagnosis, which often have latent impact to the system. In this project, we have explored various online system anomaly prediction and cause inference schemes using unsupervised machine learning methods. We tested our algorithms using extensive real system experiments and our results show that we can achieve high fidelity anomaly prediction (i.e., >95% true positive rate with <1% false positive rate) with low overhead (<1% CPU load).

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

<table>
<thead>
<tr>
<th>Received</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

<table>
<thead>
<tr>
<th>Received</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations
Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received: 

Paper


TOTAL: 2
Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

<table>
<thead>
<tr>
<th>Received</th>
<th>Paper</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/18/2015</td>
<td></td>
</tr>
<tr>
<td>14.00</td>
<td></td>
</tr>
<tr>
<td>Tsung-Hsuan Ho, Daniel Dean, Xiaohui Gu, William Enck. PREC: Practical Root Exploit Containment for Android Devices, ACM Conference on Data and Application Security and Privacy (CODASPY). 03-MAR-14, . . ,</td>
<td></td>
</tr>
<tr>
<td>05/18/2015</td>
<td></td>
</tr>
<tr>
<td>17.00</td>
<td></td>
</tr>
<tr>
<td>07/03/2013</td>
<td></td>
</tr>
<tr>
<td>11.00</td>
<td></td>
</tr>
<tr>
<td>07/03/2013</td>
<td></td>
</tr>
<tr>
<td>12.00</td>
<td></td>
</tr>
<tr>
<td>08/06/2012</td>
<td></td>
</tr>
<tr>
<td>7.00</td>
<td></td>
</tr>
<tr>
<td>08/06/2012</td>
<td></td>
</tr>
<tr>
<td>8.00</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Ying Zhao, Yongmin Tan, Zhenhuan Gong, Xiaohui Gu, Mike Wamboldt. Self-Correlating Predictive Information Tracking for Large-Scale Production Systems, IEEE International Conference on Autonomic Computing and Communications (ICAC). 15-JUN-09, . . ,</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>2.00</td>
<td></td>
</tr>
<tr>
<td>Yongmin Tan, Vinay Venkatesh, Xiaohui Gu. OLIC: OnLine Information Compression for Scalable Distributed System Monitoring, ACM/IEEE International Workshop on Quality of Service (IWoQoS). 06-JUN-11, . . ,</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>3.00</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>4.00</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>5.00</td>
<td></td>
</tr>
<tr>
<td>Kamal Kc, Xiaohui Gu. ELT: Efficient Log-based Troubleshooting System for Cloud Computing Infrastructures, IEEE International Symposium on Reliable Distributed Systems (SRDS). 05-OCT-11, . . ,</td>
<td></td>
</tr>
<tr>
<td>08/14/2011</td>
<td></td>
</tr>
<tr>
<td>6.00</td>
<td></td>
</tr>
<tr>
<td>Hiep Nguyen, Yongmin Tan, Xiaohui Gu. Propagation-aware Anomaly Localization for Cloud Hosted Distributed Applications, ACM Workshop on Managing Large-Scale Systems via the Analysis of System Logs and the Application of Machine Learning Techniques (SLAML) in conjunction with SOSP. 23-OCT-11, . . ,</td>
<td></td>
</tr>
</tbody>
</table>
08/14/2012 9.00 Hiep Nguyen, Daniel Dean, Xiaohui Gu. UBL: Unsupervised Behavior Learning for Predicting Performance Anomalies in Virtualized Cloud System, Proc. of International Conference on Autonomic Computing (ICAC). 17-SEP-12, . . ,

TOTAL: 13

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

07/03/2013 13.00 Daniel J. Dean, Yongmin Tan, Xiaohui Gu, Ting Yu, Juan Du. Scalable Distributed Service Integrity Attestation for Software-as-a-Service Clouds", IEEE Transactions on Parallel and Distributed Systems : IEEE computer soceity, (03 2013)

08/14/2012 10.00 Yongmin Tan, Vinay Venkatesh, Xiaohui Gu. Resilient Self-Compressive Monitoring for Large-Scale Hosting Infrastructures, IEEE Transactions on Parallel and Distributed Systems: IEEE Transactions, (05 2012)

TOTAL: 2
Unsupervised Behavior Learning System and Method for Predicting Performance Anomalies in Distributed Computing Infrastructures

Patents Submitted

Patents Awarded

Awards

Graduate Students

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
<th>Discipline</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daniel Dean</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Hiep Nguyen</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Anwesha Das</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td>Peipei Wang</td>
<td>1.00</td>
<td></td>
</tr>
<tr>
<td><strong>FTE Equivalent:</strong></td>
<td><strong>4.00</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Total Number:</strong></td>
<td><strong>4</strong></td>
<td></td>
</tr>
</tbody>
</table>

Names of Post Doctorates

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FTE Equivalent:</strong></td>
<td><strong>National Academy Member</strong></td>
</tr>
<tr>
<td><strong>Total Number:</strong></td>
<td><strong>1</strong></td>
</tr>
</tbody>
</table>

Names of Faculty Supported
### Names of Under Graduate students supported

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FTE Equivalent:**

**Total Number:**

### Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: ...... 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:...... 0.00

### Names of Personnel receiving masters degrees

<table>
<thead>
<tr>
<th>NAME</th>
<th>Total Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Names of personnel receiving PHDs

<table>
<thead>
<tr>
<th>NAME</th>
<th>Total Number:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hiep Nguyen</td>
<td>2</td>
</tr>
<tr>
<td>Daniel Dean</td>
<td></td>
</tr>
</tbody>
</table>

### Names of other research staff

<table>
<thead>
<tr>
<th>NAME</th>
<th>PERCENT_SUPPORTED</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FTE Equivalent:**

**Total Number:**

### Sub Contractors (DD882)

...
Unsupervised Behavior Learning System and Method for Predicting Performance Anomalies in Distributed Computing Infrastructures

Patent Filed in US? (5d-1) Y
Patent Filed in Foreign Countries? (5d-2) N
Was the assignment forwarded to the contracting officer? (5e) N

Foreign Countries of application (5g-2):

5a: Daniel Dean
5f-1a: North Carolina State University
5f-c: 890 Oval Drive
    Raleigh                     NC   27695

5a: Xiaohui Gu
5f-1a: North Carolina State University
5f-c: 890 Oval Drive
    Raleigh                     NC   27695
Objective

Larg-scale distributed computing infrastructures have become important platforms for many critical real-world systems such as cloud computing, big data processing, and intelligence analysis. However, due to its inherent complexity and sharing nature, shared computing infrastructures are inevitably prone to various system anomalies caused by software bugs, hardware failures, and resource contentions. The situation exacerbates if the system is also exposed to malicious attacks. Moreover, although some anomaly symptoms such as machine crash are easy to detect, many other anomalies (e.g., performance degradation, processing bottlenecks, memory leak bugs) are hard to detect and diagnosis, which often have latent impact to the system. The objective of this project is to develop automatic 24x7 anomaly management to enhance the resilience of large-scale shared computing infrastructures.

Approach

In this project, we propose to develop a new predictive anomaly management approach that can raise advance anomaly alerts to trigger just-in-time anomaly diagnosis while the system approaches the anomaly state, and perform informed anomaly correction based on the runtime diagnosis results before the system is seriously affected by the anomaly. Thus, our approach can effectively alleviate the impact of anomalies without incurring prohibitive cost to the infrastructure. We focus on developing novel techniques for predicting, diagnosing, and correcting latent anomalies in shared computing infrastructures. The latent anomalies (e.g., performance degradation, resource hotspots, memory leak bugs) often do not have salient symptoms at the beginning, which make it hard to detect by human being. Those latent anomalies are often difficult to diagnose since their symptoms are often correlated with many reasons. However, it is highly important to detect and correct those latent anomalies since they often have prolonged impact to the system. We test our techniques on not only controllable virtual computing systems running in our lab but also on production-level infrastructures such as virtual computing lab (VCL) at NCSU and real world computing infrastructure data provided by our industrial partners at Google and IBM. We also develop metrics and models to evaluate the predictability of a wide range of system anomalies so as to build taxonomy of predictable system anomalies. We also develop new prediction and containment techniques to prevent root exploit attacks on edge-devices such as smart phones, which are the most serious attacks among all the security attacks and are hard to prevent using exiting techniques.

Scientific Barriers

Statistical learning and detailed data analysis have recently been shown to be promising for automatic system status analysis. Our work leverages statistical learning and signal processing techniques to achieve online anomaly prediction. The major challenge includes how to achieve high prediction accuracy under dynamic computing environments and raise early enough alerts before anomaly happens. We have developed various online anomaly prediction techniques to achieve this goal. We developed prediction algorithms using both supervised and unsupervised learning techniques. The unsupervised learning approach allows us to achieve online anomaly prediction without requiring anomaly training data. Thus, our techniques can predict both previously known and unknown anomalies. We also developed context-aware anomaly prediction techniques that can achieve much higher prediction accuracy for dynamic systems than previous schemes. We recently extend our prediction algorithm that can consider not only system-level metrics (e.g., CPU, memory, disk usage) but also system calls. By analyzing system calls, our prediction algorithm can successfully predict all the existing root exploit attacks on the Android smart phones.

Prediction enables us to trigger timely preventions (e.g., migration, resource scaling, inserting delays in system calls) before the user perceives serious impact from the anomaly. We developed various online anomaly prevention techniques using live virtual machine (VM) migrations and elastic resource scaling. Our prediction system not only can raise advance alerts but also provide root cause inference to identify what might be the root cause of the system anomaly (e.g., CPU hog, memory leak, disk contention). We can then invoke proper prevention actions accordingly. Since prediction might raise false alarms, we also develop validation schemes to reverse incorrect preventions.

Prediction also enables us to perform in-situ anomaly diagnosis that can identify anomaly root causes onsite. The advantage is that we don’t need to reproduce the anomaly-inducing environments, which are often extremely difficult. We are developing onsite anomaly path inference and various root cause localization techniques. We can first localize the faulty components among many distributed system components. We then localize root cause functions using system call analysis. The basic idea is to learn the system call sequence patterns produced by different functions using frequent episode mining and then use those system call sequence patterns as signatures to identify root cause functions. The advantage of our approach is that we don’t require source code or any high-overhead online system instrumentations. We also develop onsite failure path inference without requiring source code.

Virtual machines provide opportunities for us to monitor and control various applications running inside the computing infrastructure. Our work leverages virtual machines to perform out-of-box monitoring and control. One challenge we have
addressed in this project is to achieve scalable runtime monitoring, which can continuously track different virtual machine (VM) execution data (e.g., performance counters, resource metrics, system calls, inter-component invocations) to provide comprehensive knowledge for anomaly prediction and diagnosis. We developed adaptive sampling and online compression techniques to achieve light-weight monitoring.

Significance

The proposed research fundamentally advances knowledge and understanding in the interdisciplinary field of applying machine learning and dynamic system analysis to improve the resilience of complex computing infrastructures. Enhancing the resilience of large-scale computing infrastructures, which is well recognized by ARO as one of its key computing challenges in future battle spaces. As more and more critical Army missions depend on IT infrastructure, it has become imperative to guarantee continuous system operation despite software/hardware failures and malicious attacks. As rapid advances in computing hardware have led to dramatic improvement in computer performance, the issues of reliability, availability, and manageability are becoming the nominating bottlenecks in IT infrastructure maintenance. The proposed research advances existing science and technology through novel techniques in support of self-evolving system modeling, online anomaly prediction, onsite anomaly diagnosis, and anomaly preventions for large-scale distributed computing infrastructure. The proposed research explores new approaches with novel applications of machine learning, speculative execution, and dynamic system analysis on system profiling, anomaly prediction and diagnosis, and development of new scalable techniques and tools to achieve resilient distributed computing systems. We will develop and make available implemented techniques and collected data, which will let other researchers and practitioners build on our results.

Accomplishments

(Feel free to use a bulleted list here)

Publications:
- "OLIC: OnLine Information Compression for Scalable Distributed System Monitoring", Yongmin Tan, Vinay Venkatesh,
Xiaohui Gu, Proc. of ACM/IEEE International Workshop on Quality of Service (IWQoS), San Jose, CA, June, 2011.
• "Self-Correlating Predictive Information Tracking for Large-Scale Production Systems", Ying Zhao, Yongmin Tan, Zhenhuan Gong, Xiaohui Gu, Mike Wamboldt, IEEE International Conference on Autonomic Computing and Communications (ICAC), Barcelona, Spain, June, 2009. (Acceptance rate: 15.6%)

Awards:
• Best paper awards, IEEE ICDCS, 1 out of 530 submissions, 2012.
• Best paper awards, IEEE CNSM, 1 out of 176 submissions, 2010.

Media coverage:
• featured highlight on NSF’s official news site, Science 360,
• Communications of ACM,
• e! science news,
• WRAL techwire,
• ScienceDaily, etc.

Collaborations and Leveraged Funding
We have been collaborating with VCL administrators to apply our techniques on the VCL infrastructure. Most of our tools have been tested on the VCL. We have been working with researchers at IBM and Google during this project. Our current leveraged funding include:
• “CAREER: Enabling Robust Virtualized Hosting Infrastructures via Coordinated Learning, Recovery, and Diagnosis”, NSF, $450K, 1/1/2012-12/31/2016, Sole PI.
• “Online Performance Anomaly Diagnosis for Cloud Computing Infrastructures”, IBM Faculty Award, $15K, 9/1/2011-8/31/2012, Sole PI.
• “CSR:Small: Online System Anomaly Prediction and Diagnosis for Large-Scale Hosting Infrastructures”, NSF, $405,000, 08/15/2009 – 08/14/2012, Sole PI.

Conclusions
We have successfully integrated our online anomaly prediction, anomaly root cause inference, and anomaly prevention components into a complete automatic anomaly prevention framework. Our system can automatically steer the system away from anomalies caused by various software bugs, resource contentions, or malicious attacks.

Technology Transfer
NCSU filed a patent application on our unsupervised anomaly prediction scheme and Google has purchased an evaluation license for our software.

NCSU filed a patent on our unsupervised behavior learning (UBL) technology. Google has entered an evaluation agreement with NCSU for licensing UBL. One startup is underway to commercialize our anomaly prediction and diagnosis techniques.
Objective

Larg-scale distributed computing infrastructures have become important platforms for many critical real-world systems such as cloud computing, big data processing, and intelligence analysis. However, due to its inherent complexity and sharing nature, shared computing infrastructures are inevitably prone to various system anomalies caused by software bugs, hardware failures, and resource contentions. The situation exacerbates if the system is also exposed to malicious attacks. Moreover, although some anomaly symptoms such as machine crash are easy to detect, many other anomalies (e.g., performance degradation, processing bottlenecks, memory leak bugs) are hard to detect and diagnosis, which often have latent impact to the system. The objective of this project is to develop automatic 24x7 anomaly management to enhance the resilience of large-scale shared computing infrastructures.

Approach

In this project, we propose to develop a new predictive anomaly management approach that can raise advance anomaly alerts to trigger just-in-time anomaly diagnosis while the system approaches the anomaly state, and perform informed anomaly correction based on the runtime diagnosis results before the system is seriously affected by the anomaly. Thus, our approach can effectively alleviate the impact of anomalies without incurring prohibitive cost to the infrastructure. We focus on developing novel techniques for predicting, diagnosing, and correcting latent anomalies in shared computing infrastructures. The latent anomalies (e.g., performance degradation, resource hotspots, memory leak bugs) often do not have salient symptoms at the beginning, which make it hard to detect by human being. Those latent anomalies are often difficult to diagnose since their symptoms are often correlated with many reasons. However, it is highly important to detect and correct those latent anomalies since they often have prolonged impact to the system. We test our techniques on not only controllable virtual computing systems running in our lab but also on production-level infrastructures such as virtual computing lab (VCL) at NCSU and real world computing infrastructure data provided by our industrial partners at Google and IBM. We also develop metrics and models to evaluate the predictability of a wide range of system anomalies so as to build taxonomy of predictable system anomalies. We also develop new prediction and containment techniques to prevent root exploit attacks on edge-devices such as smart phones, which are the most serious attacks among all the security attacks and are hard to prevent using exiting techniques.

Scientific Barriers

Statistical learning and detailed data analysis have recently been shown to be promising for automatic system status analysis. Our work leverages statistical learning and signal
processing techniques to achieve online anomaly prediction. The major challenge includes how to achieve high prediction accuracy under dynamic computing environments and raise early enough alerts before anomaly happens. We have developed various online anomaly prediction techniques to achieve this goal. We developed prediction algorithms using both supervised and unsupervised learning techniques. The unsupervised learning approach allows us to achieve online anomaly prediction without requiring anomaly training data. Thus, our techniques can predict both previously known and unknown anomalies. We also developed context-aware anomaly prediction techniques that can achieve much higher prediction accuracy for dynamic systems than previous schemes. We recently extend our prediction algorithm that can consider not only system-level metrics (e.g., CPU, memory, disk usage) but also system calls. By analyzing system calls, our prediction algorithm can successfully predict all the existing root exploit attacks on the Android smart phones.

Prediction enables us to trigger timely preventions (e.g., migration, resource scaling, inserting delays in system calls) before the user perceives serious impact from the anomaly. We developed various online anomaly prevention techniques using live virtual machine (VM) migrations and elastic resource scaling. Our prediction system not only can raise advance alerts but also provide root cause inference to identify what might be the root cause of the system anomaly (e.g., CPU hog, memory leak, disk contention). We can then invoke proper prevention actions accordingly. Since prediction might raise false alarms, we also develop validation schemes to reverse incorrect preventions.

Prediction also enables us to perform in-situ anomaly diagnosis that can identify anomaly root causes onsite. The advantage is that we don’t need to reproduce the anomaly-inducing environments, which are often extremely difficult. We are developing onsite anomaly path inference and various root cause localization techniques. We can first localize the faulty components among many distributed system components. We then localize root cause functions using system call analysis. The basic idea is to learn the system call sequence patterns produced by different functions using frequent episode mining and then use those system call sequence patterns as signatures to identify root cause functions. The advantage of our approach is that we don’t require source code or any high-overhead online system instrumentations. We also develop onsite failure path inference without requiring source code.

Virtual machines provide opportunities for us to monitor and control various applications running inside the computing infrastructure. Our work leverages virtual machines to perform out-of-box monitoring and control. One challenge we have addressed in this project is to achieve scalable runtime monitoring, which can continuously track different virtual machine (VM) execution data (e.g., performance counters, resource metrics, system calls, inter-component invocations) to provide comprehensive knowledge for anomaly prediction and diagnosis. We developed adaptive sampling and online compression techniques to achieve light-weight monitoring.
Significance

The proposed research fundamentally advances knowledge and understanding in the interdisciplinary field of applying machine learning and dynamic system analysis to improve the resilience of complex computing infrastructures. Enhancing the resilience of large-scale computing infrastructures, which is well recognized by ARO as one of its key computing challenges in future battle spaces. As more and more critical Army missions depend on IT infrastructure, it has become imperative to guarantee continuous system operation despite software/hardware failures and malicious attacks. As rapid advances in computing hardware have led to dramatic improvement in computer performance, the issues of reliability, availability, and manageability are becoming the nominating bottlenecks in IT infrastructure maintenance. The proposed research advances existing science and technology through novel techniques in support of self-evolving system modeling, online anomaly prediction, onsite anomaly diagnosis, and anomaly preventions for large-scale distributed computing infrastructure. The proposed research explores new approaches with novel applications of machine learning, speculative execution, and dynamic system analysis on system profiling, anomaly prediction and diagnosis, and development of new scalable techniques and tools to achieve resilient distributed computing systems. We will develop and make available implemented techniques and collected data, which will let other researchers and practitioners build on our results.

Accomplishments

(feel free to use a bulleted list here)

Publications:

  (acceptance rate: 29/119 = 24%)

- "PerfCompass: Toward Runtime Performance Anomaly Fault Localization for Infrastructure-as-a-Service Clouds", Daniel Dean, Hiep Nguyen, Peipei Wang, Xiaohui Gu,
  Proc. of USENIX Workshop on Hot Topics in Cloud Computing (HotCloud), Philadelphia, PA, June, 2014. (acceptance rate: 22/72 = 30.5%)

- "Insight: In-situ Online Service Failure Path Inference in Production Computing Infrastructures", Hiep Nguyen, Daniel J. Dean, Kamal Kc, Xiaohui Gu

- "PREC: Practical Root Exploit Containment for Android Devices", Tsung-Hsuan Ho, Daniel Dean, Xiaohui Gu, William Enck, Proc. of the ACM Conference on Data and
Application Security and Privacy (CODASPY), San Antonio, TX, March, 2014. (full paper, acceptance rate: 16%)


Simulation of Computer and Telecommunication Systems (MASCOTS), Miami Beach, Florida, August, 2010. (Acceptance rate: 29%)

- “Self-Correlating Predictive Information Tracking for Large-Scale Production Systems", Ying Zhao, Yongmin Tan, Zhenhuan Gong, Xiaohui Gu, Mike Wamboldt, IEEE International Conference on Autonomic Computing and Communications (ICAC), Barcelona, Spain, June, 2009. (Acceptance rate: 15.6%)

Awards:
- Best paper awards, IEEE ICDCS, 1 out of 530 submissions, 2012.
- Best paper awards, IEEE CNSM, 1 out of 176 submissions, 2010.

Media coverage:
- featured highlight on NSF’s official news site, Science 360,
- Communications of ACM,
- e! science news,
- WRAL techwire,
- ScienceDaily, etc.

Collaborations and Leveraged Funding

We have been collaborating with VCL administrators to apply our techniques on the VCL infrastructure. Most of our tools have been tested on the VCL. We have been working with researchers at IBM and Google during this project. Our current leveraged funding include:

- “CAREER: Enabling Robust Virtualized Hosting Infrastructures via Coordinated Learning, Recovery, and Diagnosis", NSF, $450K, 1/1/2012-12/31/2016, Sole PI.
- “Online Performance Anomaly Diagnosis for Cloud Computing Infrastructures”, IBM Faculty Award, $15K, 9/1/2011-8/31/2012, Sole PI.
- “CSR:Small: Online System Anomaly Prediction and Diagnosis for Large-Scale Hosting Infrastructures”, NSF, $405,000, 08/15/2009 – 08/14/2012, Sole PI.

Conclusions

We have successfully integrated our online anomaly prediction, anomaly root cause inference, and anomaly prevention components into a complete automatic anomaly prevention framework. Our system can automatically steer the system away from anomalies caused by various software bugs, resource contentions, or malicious attacks.

Technology Transfer
We have deployed and tested most of our techniques on the virtual computing lab (VCL) at North Carolina State University. We also tested our system on a cloud computing testbed (HGCC cluster) in our lab that consists of 15 blade nodes. Recently, we have filed provisional patent and several software licenses on our technologies. Several big companies including Google have indicated their interests in licensing our technologies.

**Future Plans**

We will extensively test the current framework with various real world applications and malwares. We hope to provide a detailed study on which kind of malicious attacks can be captured by our framework. We will continue to develop more robust and practical online anomaly/malware prediction techniques to capture malicious activities. We will also develop malicious software sandboxing techniques that allow us to capture malicious activities without compromising the protected system.

**Objective**

Large-scale distributed computing infrastructures have become important platforms for many critical real-world systems such as cloud computing, big data processing, and intelligence analysis. However, due to its inherent complexity and sharing nature, shared computing infrastructures are inevitably prone to various system anomalies caused by software bugs, hardware failures, and resource contentions. The situation exacerbates if the system is also exposed to malicious attacks. Moreover, although some anomaly symptoms such as machine crash are easy to detect, many other anomalies (e.g., performance degradation, processing bottlenecks, memory leak bugs) are hard to detect and diagnosis, which often have latent impact to the system. The objective of this project is to develop automatic 24x7 anomaly management to enhance the resilience of large-scale shared computing infrastructures.

**Approach**

In this project, we propose to develop a new predictive anomaly management approach that can raise advance anomaly alerts to trigger just-in-time anomaly diagnosis while the system approaches the anomaly state, and perform informed anomaly correction based on the runtime diagnosis results before the system is seriously affected by the anomaly. Thus, our approach can effectively alleviate the impact of anomalies without incurring prohibitive cost to the infrastructure. We focus on developing novel techniques for predicting, diagnosing,
and correcting latent anomalies in shared computing infrastructures. The latent anomalies (e.g., performance degradation, resource hotspots, memory leak bugs) often do not have salient symptoms at the beginning, which make it hard to detect by human being. Those latent anomalies are often difficult to diagnose since their symptoms are often correlated with many reasons. However, it is highly important to detect and correct those latent anomalies since they often have prolonged impact to the system. We test our techniques on not only controllable virtual computing systems running in our lab but also on production-level infrastructures such as virtual computing lab (VCL) at NCSU and real world computing infrastructure data provided by our industrial partners at Google and IBM. We also develop metrics and models to evaluate the predictability of a wide range of system anomalies so as to build taxonomy of predictable system anomalies. We also develop new prediction and containment techniques to prevent root exploit attacks on edge-devices such as smart phones, which are the most serious attacks among all the security attacks and are hard to prevent using exiting techniques.

Scientific Barriers

Statistical learning and detailed data analysis have recently been shown to be promising for automatic system status analysis. Our work leverages statistical learning and signal processing techniques to achieve online anomaly prediction. The major challenge includes how to achieve high prediction accuracy under dynamic computing environments and raise early enough alerts before anomaly happens. We have developed various online anomaly prediction techniques to achieve this goal. We developed prediction algorithms using both supervised and unsupervised learning techniques. The unsupervised learning approach allows us to achieve online anomaly prediction without requiring anomaly training data. Thus, our techniques can predict both previously known and unknown anomalies. We also developed context-aware anomaly prediction techniques that can achieve much higher prediction accuracy for dynamic systems than previous schemes. We recently extend our prediction algorithm that can consider not only system-level metrics (e.g., CPU, memory, disk usage) but also system calls. By analyzing system calls, our prediction algorithm can successfully predict all the existing root exploit attacks on the Android smart phones.

Prediction enables us to trigger timely preventions (e.g., migration, resource scaling, inserting delays in system calls) before the user perceives serious impact from the anomaly. We developed various online anomaly prevention techniques using live virtual machine (VM) migrations and elastic resource scaling. Our prediction system not only can raise advance alerts but also provide root cause inference to identify what might be the root cause of the system anomaly (e.g., CPU hog, memory leak, disk contention). We can then invoke proper prevention actions accordingly. Since prediction might raise false alarms, we also develop validation schemes to reverse incorrect preventions.

Prediction also enables us to perform in-situ anomaly diagnosis that can identify anomaly root causes onsite. The advantage is that we don’t need to reproduce the anomaly-inducing environments, which are often extremely difficult. We are developing onsite anomaly path inference and various root cause localization techniques. We can first localize the faulty components among many distributed system components. We then localize root cause
functions using system call analysis. The basic idea is to learn the system call sequence patterns produced by different functions using frequent episode mining and then use those system call sequence patterns as signatures to identify root cause functions. The advantage of our approach is that we don’t require source code or any high-overhead online system instrumentations. We also develop onsite failure path inference without requiring source code.

Virtual machines provide opportunities for us to monitor and control various applications running inside the computing infrastructure. Our work leverages virtual machines to perform out-of-box monitoring and control. One challenge we have addressed in this project is to achieve scalable runtime monitoring, which can continuously track different virtual machine (VM) execution data (e.g., performance counters, resource metrics, system calls, inter-component invocations) to provide comprehensive knowledge for anomaly prediction and diagnosis. We developed adaptive sampling and online compression techniques to achieve light-weight monitoring.

Significance

The proposed research fundamentally advances knowledge and understanding in the interdisciplinary field of applying machine learning and dynamic system analysis to improve the resilience of complex computing infrastructures. Enhancing the resilience of large-scale computing infrastructures, which is well recognized by ARO as one of its key computing challenges in future battle spaces. As more and more critical Army missions depend on IT infrastructure, it has become imperative to guarantee continuous system operation despite software/hardware failures and malicious attacks. As rapid advances in computing hardware have led to dramatic improvement in computer performance, the issues of reliability, availability, and manageability are becoming the nominating bottlenecks in IT infrastructure maintenance. The proposed research advances existing science and technology through novel techniques in support of self-evolving system modeling, online anomaly prediction, onsite anomaly diagnosis, and anomaly preventions for large-scale distributed computing infrastructure. The proposed research explores new approaches with novel applications of machine learning, speculative execution, and dynamic system analysis on system profiling, anomaly prediction and diagnosis, and development of new scalable techniques and tools to achieve resilient distributed computing systems. We will develop and make available implemented techniques and collected data, which will let other researchers and practitioners build on our results.

Accomplishments

(feel free to use a bulleted list here)

Publications:

• “Self-Correlating Predictive Information Tracking for Large-Scale Production Systems", Ying Zhao, Yongmin Tan, Zhenhuan Gong, Xiaohui Gu, Mike Wamboldt, IEEE International Conference on Autonomic Computing and Communications (ICAC), Barcelona, Spain, June, 2009. (Acceptance rate: 15.6%)

Awards:
• Best paper awards, IEEE ICDCS, 1 out of 530 submissions, 2012.
• Best paper awards, IEEE CNSM, 1 out of 176 submissions, 2010.

Media coverage:
• featured highlight on NSF’s official news site, Science 360,
• Communications of ACM,
• e! science news,
• WRAL techwire,
• ScienceDaily, etc.

Collaborations and Leveraged Funding

We have been collaborating with VCL administrators to apply our techniques on the VCL infrastructure. Most of our tools have been tested on the VCL. We have been working with researchers at IBM and Google during this project. Our current leveraged funding include:

• “CAREER: Enabling Robust Virtualized Hosting Infrastructures via Coordinated Learning, Recovery, and Diagnosis”, NSF, $450K, 1/1/2012-12/31/2016, Sole PI.
• “Online Performance Anomaly Diagnosis for Cloud Computing Infrastructures”, IBM Faculty Award, $15K, 9/1/2011-8/31/2012, Sole PI.
Conclusions

We have successfully integrated our online anomaly prediction, anomaly root cause inference, and anomaly prevention components into a complete automatic anomaly prevention framework. Our system can automatically steer the system away from anomalies caused by various software bugs, resource contentions, or malicious attacks.

Technology Transfer

NCSU filed a patent application on our unsupervised anomaly prediction scheme and Google has purchased an evaluation license for our software.