Security & Software Engineering Research Center (S^2ERC)

A CISE-funded Center

Ball State University, Wayne Zage, Director, 765.285.8664, wmzage@bsu.edu

Iowa State University, Thomas Daniels, Co-Director, 515.294.8375, daniels@iastate.edu

Virginia Tech, T. Charles Clancy, 703.518.2973, tcc@vt.edu

Center websites: http://www.serc.net and http://www.cyber.vt.edu/s2erc

Design Metrics Technology

Improvements in the software development process depend on the ability to collect and analyze data drawn from the various phases of the development life cycle. Stress points are defined as critical components in software; points where errors in coding and programming logic are likely to occur. The Security and Software Engineering Research Center (S^2ERC) Design Metrics Team has developed a metrics-guided methodology for maximizing and maintaining software reliability. The technology provides an unbiased framework that efficiently makes cost-effective determinations for design improvements, code-modifications, and related testing and management strategies. Applying this methodology to software designs identifies and highlights stress points within software. It helps improve overall design quality.

Satellite-related projects are one type of technology benefiting from design metrics.

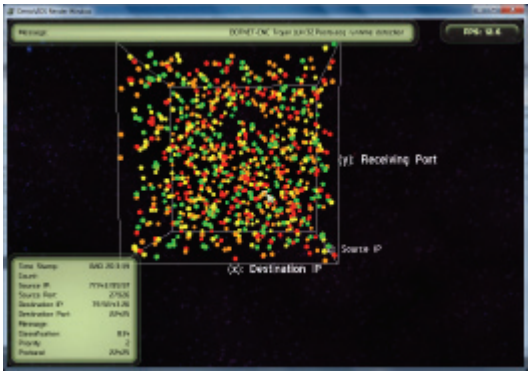
Identifying stress points in advance and applying mitigating approaches results in improved resource allocation. In the coding phase, the technology can identify stressful components and provide change impact analyses. In testing, metrics can assist in determining where testing efforts should be focused and the types of test strategies that are needed. In twenty years of metrics validation on a wide variety of projects ranging from missile defense, satellite, accounting, and telecommunications systems to interactive games, the design metrics have identified at least 75 percent of error-prone components with very few false positives. Applying this design metrics technology is assisting developers engineer higher quality software products. In 2007, this technology was awarded the Alexander Schwarzkopf Prize for Technological Innovation by the NSF I/UCRC Association. The S^2ERC Design Metrics Team continues to learn more about enhancing reliability and dependability of critical software systems.

Economic Impact: Software unreliability often is due to design faults. While software can fail for reasons other than faulty design, these design mistakes occur in various forms, including design inconsistencies and semantic errors. Historically, identifying error-prone components early in the life cycle reduces software failures and their associated costs.

For more information, contact Wayne M. Zage, 765.285.8664, wmzage@bsu.edu.

Visual Intrusion Detection System (VIDS)

Network-based attacks have become more sophisticated and visualization can increase the speed at which security issues are identified. Losing control of network nodes even for the shortest period of time can generate unpredictable consequences. Loss of connectivity can provide an adversary with unexpected advantages that may lead to life threatening adverse events, injury, extended power outages, water contamination, and subsequent losses of confidence in large portions of the economy.



The screenshot depicts a VIDS three-dimensional view of alerts with various priorities, shown in the graph as spheres of different colors.

The destructive potential of cyber-attacks is all too real. Those who wish others harm are no longer necessarily geographically distant, but can be just behind the firewall. As more high technology products are designed to communicate directly without human involvement, the attacks can cascade unpredictably. It is crucial, therefore, to mitigate network threats. Monitoring can be an effective deterrent against misbehavior from both insiders and intruders.

Efficient security monitoring has always been complex, involving collecting, correlating, and storing information from many sources, firewalls, and intrusion detection systems. S^{2}ERC researchers aim to provide security analysts with a tool to discover patterns, detect anomalies, identify correlations, and communicate findings. The VIDS project combines the research efforts of visualization and network security to create a practical tool for network security analysis/monitoring. The visual approach offers a number of benefits over the traditional textual analysis of security data.

Complex relationships can be hidden within the large amount of data produced by security tools. Visualization can help analyze millions of log entries. Often, patterns that were not anticipated are revealed when the data are graphed. Visualization requires the distillation of large amounts of data into meaningful displays. These can assist security personnel decide which areas to investigate.

> **Economic Impact:** It is estimated that $1 trillion was lost in 2010 to cybercrime; a figure that is considered low due to unreported incidents. Assisted by VIDS, analysts protect our essential digital infrastructure, identified by President Obama, as "the backbone that underpins a prosperous economy and a strong military and an open and efficient government. Without that foundation we can't get the job done." If analysts using a system such as VIDS can avoid just 1/1000 of the value of these cybercrimes, then the savings could amount to $1 billion. [May 2009 remarks by the US President on Securing our Nation's Cyber Infrastructure.]

For more information, contact Dolores M. Zage, 765.285.8646, dmzage@bsu.edu.