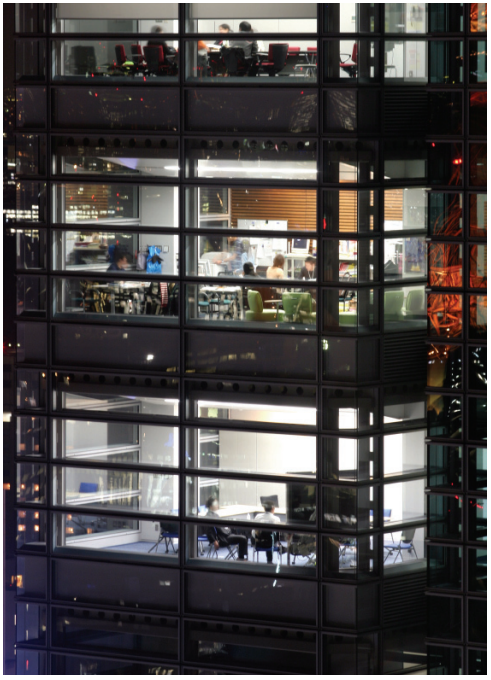
Security & Software Engineering Research Center (S^2ERC)

A CISE-funded Center

Ball State University, Wayne Zage, Director, 765.285.8664, wmzage@bsu.edu
Iowa State University, Doug Jacobson, Co-Director, 515.294.8307, dougj@iastate.edu
Virginia Tech, T. Charles Clancy, 540.251.2090, tcc@vt.edu

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

More Efficient Access Control to System Development Data



Researchers at the Security and Software Engineering Research Center (S^2ERC) have developed tools and methods that allow access to development data, information, and artifacts without sacrificing security and confidentiality. The context is one in which some participants in development projects must be granted unrestricted access to a project's data but are denied access to other data that may be present on the development network. For example, partners, customers, and subcontractors may all be co-located at the team-lead's facility, but their access to data via the host company's corporate network must be limited to project-relevant development artifacts only. Project participants who are also employees of the host company must have access to information beyond project-specific artifacts.

Current access control approaches tend to be binary and inflexible, with the result being that developers are incorrectly denied access to data, information, and development artifacts that their program or work requires. In the case of a co-located team in which not all members are employees, or where access to information is on a need-to-know basis, this wastes time and money as developers wait to be added to access control lists and networked artifacts are moved from one protected directory to another, or from one server to another. This could be the case where software components are reused from one project into another. The innovative approach taken by center researchers uses probability-of-risk rather than group membership to determine access privileges. The access control model dynamically calculates the risk of disclosing specific information based on probabilistic estimation. The access control decision can then be made by comparing the estimated risk with a pre-defined threshold.

Economic Impact: The potential reduction in development costs and scheduling is significant. Increasingly, as development projects can no longer afford to develop internal expertise for all

aspects of a product, they need to team with partners and hire subcontractors. Where access to networked information is determined by group membership, delays can be chronic, lengthy and costly, especially where access approval requires multiple approvals (e.g., where an artifact is to be reused from a previous or a concurrent project). Flexible access control has the potential to eliminate much of this delay and accelerate the development of the common knowledge and understanding required for successful development. In this way it can save significant dollars for many types of organizations.

For more information, contact Robyn Lutz, 515.294.3654, rlutz@cs.iastate.edu.

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. The Security and Software Engineering Research Center (S^2ERC) Design Metrics Team has developed a metrics-guided methodology for maximizing and maintaining software reliability. This technology provides an unbiased framework that efficient makes cost-effective determines for design improvements, code-modifications and related testing and management strategies. Applying this methodology to software designs identifies and highlights stress points within software. This helps improve overall design quality. Stress points are defined as critical components in software; points where errors in coding and programming logic are likely to occur.

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

Identifying such components 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 in engineering higher quality and reliability into the software products. This technology was awarded the Alexander Schwarzkopf Prize for Technological Innovation by the NSF I/UCRC Association in 2007. 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.

Formally Verifying Software Systems

This work has addressed these past limitations by identifying, formalizing and automating the complex processes of identifying security relevant data and its potential for leakage or corruption. In so doing, usable infrastructures are becoming more available for defining and developing provably secure software. This work advances the state of the art in software systems development for homeland security by providing guaranteed compliance with security goals. Further efforts have identified new algorithms for important problems such as security level inference and credentials discovery. This advance is being used not only in security typed languages, but are also helping the operating systems community to define policies and services tailored to the security requirements of applications. This will significantly enhance the capabilities of commercial software developers to articulate and realize security goals. The researchers are working with Motorola to evaluate how the tools can be used to make applications of embedded devices such as cellular phones more secure.

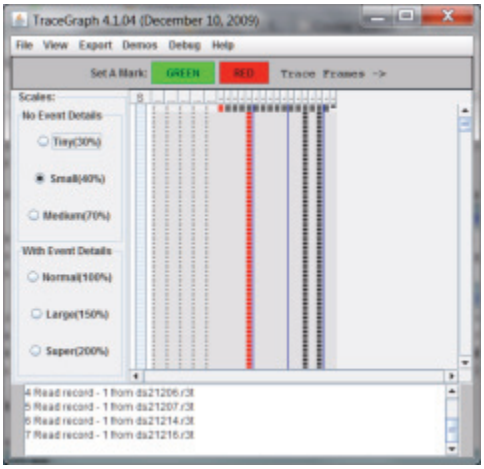
> **Economic Impact:** This work was the genesis of a stream of works that sought to explore the practical use of language-based systems. It has led to several substantive research projects targeting formal verification of computing systems at organizations such as Cornell University, University of Pennsylvania and Microsoft. The JifClipse integrated developer environment tool created as part of this project has been used and adapted by several groups, and has been distributed to industry and academics over the Internet. These projects support at least 10-20 paid student and professional researchers, and will likely impact the quality of several commercial products, e.g., elements of type-based security are being considered for several key Microsoft products.

For more information, contact Patrick McDaniel, 814.863.3599, mcdaniel@cse.psu.edu.

Spotlighting the Code

In addition to designing, coding and testing software, software engineers need to "maintain" it. "Maintenance" consists of the innumerable adaptations, enhancements and "bug fixes" that are needed over the years that a system is in service. Numerous studies have shown that 50% or more of the life-cycle budget of most software system is spent on "maintenance", largely because maintenance software engineers struggle to understand unfamiliar code, often developed by others years before.

The S^{2}ERC "Spotlighting the Code" project's "software reconnaissance" technique helps software engineers quickly locate code he needs maintenance in large systems. The technique has been very influential in subsequent software maintenance research; the original 1992 paper was judged the "most influential" ten years later based on the number of citations it had received. The open source Recon and TraceGraph tools developed by the project are still downloaded hundreds of times each year. A screen shot of TraceGraph analyzing traces from an Apache web server is pictured.



Economic Impact: According to the U. S. Bureau of Labor Statistics, in 2004, there were 760,840 software engineers working in the US. About half of these are involved in "maintenance" activities. If software reconnaissance enables software engineers locate code quickly and thus decrease maintenance time by just 1%, This would represent annual salary savings of about 200 million USD.

For more information, contact N. Wilde, 850.474.2548, nwilde@uwf.edu.

Safety in SmartHomes

With the increasing availability of low cost wireless devices such as cellular phones, medical devices, and home networking devices, it is now possible to remotely and programmatically control various devices and events at remote locations (e.g., in homes, offices and in the field). However, while offering increased flexibility and convenience to users, these devices have also raised the possibility of serious malfunction due to proximity. For example, aircraft navigation systems and medical implants are affected adversely by cellular devices and other devices that emit large amounts of radiation such as an NMR. Despite stringent emission standards, proximity of two or more devices, often of different kinds, can raise serious threats to human life. The SmartHome project has investigated, among others, issues of safety. A key contribution of this work is universal software/hardware architecture for devices that radiate. Such an architecture, obtained with the help of Digital Device Manuals, allows controllers to be embedded in various life threatening environments such as hospitals and aircraft. This helps ensure safe operation of co-located mobile and other radiating devices.

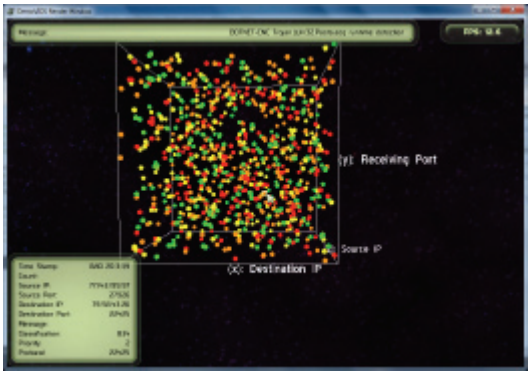
A collection of one or more devices, each described by its Digital Device Manual and reachable over a network, is a ConnectedSpace. The behavior of each device is expressed using an extended finite state machine. A set of policies may be enforced on the ConnectedSpace to ensure safe operation. Such safety policies are monitored and enforced by safety controllers. Procedures were developed for the automatic synthesis of optimal safety controllers in ConnectedSpaces. The notions of policy relaxation and safety ranking are novel to this work.

> **Economic Impact:** The procedures developed in this work have the potential for substantial economic impact in the health care and air transportation industry through the avoidance of accidents due to interference from mobile devices. Passengers are asked to turn off their cell phones to bring to nearly zero the impact of cell phone communications on flight navigation systems. The ConnectedSpaces paradigm offers an automated mechanism for turning phones off once the pilot has indicated that they must be turned off. In hospitals, mobile phones are not allowed near critical areas because they might interfere with medical devices. ConnectedSpaces modeling and implementation of its algorithms minimizes interference thereby reducing the risk of accidents due to inappropriate mobile device operation, thusly avoiding the human and economic costs that can be associated with these events.

For more information, contact Aditya Mathur, 317.494.7823, apm@cs.purdue.edu.

Visual Intrusion Detection System (VIDS)

Connectivity is the lifeline for many of the services we expect. Losing control of network nodes even for the shortest period of time can generate unpredictable consequences. Loss of connectivity can also provide an adversary with unexpected advantages which may lead to life threatening adverse events, injury, extended power outages, water contamination and subsequent losses of confidence in large portions of the economy. It is crucial, therefore, to mitigate network threats. Monitoring is an effective deterrent against misbehavior from both insiders and intruders.



The VIDS project combines the research efforts of visualization and network security to create a practical tool for network security analysis/monitoring. A visual approach offers a number of benefits over the traditional textual analysis of security data. Network-based attacks have become more sophisticated and visualization can increase the speed at which security issues are identified. Rapid identification of attacks can lead to more effective responses where decisions must be made quickly. Efficient security monitoring has always been complex, involving collecting, correlating and storing information from many sources, firewalls and intrusion detection systems. Visualization is an effective tool to address the analysis of millions of log entries by distilling large amounts of data into something meaningful. Additionally, complex relationships can be hidden within the large amount of data produced by security tools, whereas an image can convey these relationships in direct and concise forms. These images can assist security personnel in deciding on areas to investigate. Often, patterns that were not anticipated are revealed when the data are graphed. The picture depicts a VIDS three-dimensional view of alerts with various priorities, shown in the graph as spheres of different colors.

Our aim is to provide security analysts with a tool to discover patterns, detect anomalies, identify correlations and communicate their findings. Those who wish others harm are no longer necessarily geographically distant, but can be just behind the firewall. The destructive potential of cyber-attacks are real and as more high technology products are designed to communicate directly without human involvement, the attacks can cascade unpredictably.

> **Economic Impact:** 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." It is estimated that $1 trillion was lost in 2010 to cybercrime; a figure that is considered low due to unreported incidents. 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 U.S. President on Securing our Nation's Cyber Infrastructure.]

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