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

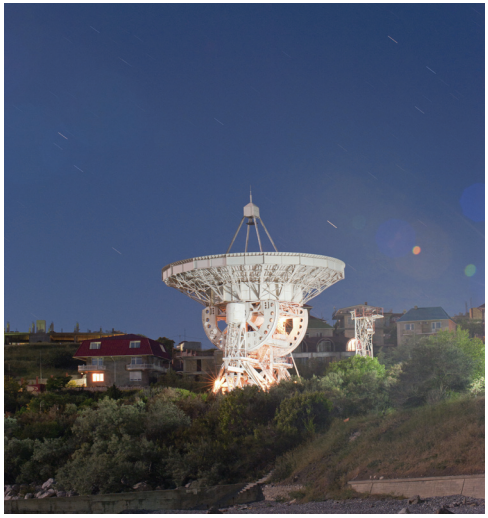
Ball State University, Wayne Zage, 765.285.8664, wmzage@bsu.edu
Iowa State University, Joseph A Zambreno, 515.294.3312, zambreno@iastate.edu
Georgetown University, Eric Burger, 202.687.4107, eric.burger@georgetown.edu
Virginia Tech, Charles Clancy, 571.858.3350, tcc@vt.edu

Scalable Modeling for Rigorous Software Specification and Testing

Modern software development processes for safety- and mission-critical systems rely on rigorous coding and testing to support dependability claims and assurance cases. The goal of researchers at Ball State University's Security and Software Engineering Research Center (S^2ERC) is to economically provide for higher software quality and dependability for large and complex software-intensive systems.

'The two foundational methods, namely sequence-based software specification and Markov chain usage-based statistical testing, were developed in the 1990s by Jesse Poore and his colleagues at the University of Tennessee's Software Quality Research Laboratory. Since their inception they have been successfully combined and applied to a variety of industry and government projects. Field applications of these methods had earlier identified the need to address complexity and increase scalability both theoretically and practically for larger and more complex applications.

When these two demonstrably rigorous methods are combined and used in the complete software development cycle it translates to a formal system model that can be used as a first pass Markov chain usage model for statistical testing. However, to reduce the specification to a manageable size, the human specifier usually must clarify the extent to which inputs of the system can be partitioned into subsets that do not interact or communicate with each other.



Selected case studies contain a range of embedded software from car door mirror electronic control units to satellite operations software. Credits: iStock

This S^2ERC breakthrough methodology overcomes this limitation by composing larger system models from smaller ones built on either disjoint or non-disjoint subsets of inputs. The constructed larger models form a basis for more rigorous automated statistical testing and software certification.

The Ball State research at S^2ERC uses theory-practice-tools. As a first step they develop a theoretical foundation for the proposed approach. They then implement the theory and algorithms in a tool that supports sequence-based specification and defines the engineering process for how to accomplish it systematically with tool support. Finally, researchers conduct case studies to evaluate its applicability and effectiveness.

While previous work in this area focuses on a clean partitioning of system inputs that results in clean system decomposition to manage complexity and scalability, the new approach relaxes this constraint by looking into two ways to control the size of the specification and testing model. This is accomplished by either limiting the number of stimuli being considered or the number of states being explored. The new modeling techniques improve on previous strategies by working out a formal and systematic process to explicitly merge towards a complete system model. This results in render analyses for system level software specification, testing, and certification.

The completed work involves merging sub-models that focus on selected system boundaries. Researchers continue to work on combining partial work products that emphasize different applications. The selected case studies contain a range of embedded software from car door mirror electronic control units to satellite operations software. Results of the case study have shed light on when and how the theory is in effect in different application contexts to handle and manage specification complexity.

> **Economic impact**: The consequences of an error or bug in new embedded systems or products can lead to product recalls, class action lawsuits, or wrongful death claims. Special efforts are in place to create products that more reliably perform as intended; not failing in the field is an essential quality. Though it is impossible to predict the extent of economic impacts that this development will enable, curbing the aforementioned consequences will save significant resources. This breakthrough demonstrates that scalable modeling for rigorous software specification and testing is not only feasible but practical. With a sound theoretical foundation and effective tool support, large and complex models of software-intensive systems can be more systematically constructed and tested statistically based on an operational usage profiles. This work has provided two distinct benefits: 1) more exhaustive analyses of systems' behavior in all possible scenarios of use prior to design and implementation, and; 2) more rigorous quantitative analysis after testing and validation prior to system deployment. Results can be used to more clearly demonstrate, document, and certify that systems are ready for their intended uses. The resulting scaled methods will prove to be better engineered, more dependable software systems, complete with audit trails of evidence to support claims related to the dependability for such systems.

For more information, contact Lan Lin at Ball State University, llin4@bsu.edu, Bio http://cms.bsu.edu/academics/collegesanddepartments/computerscience/facultyandstaff/faculty/linlan, 765.285.8641.

A Trust Prediction Model for the Internet of Things (IoT)

The IoT paradigm promises to be a disruptive technology that will revolutionize our day-to-day lives. These IoT systems consist of dynamic networks of omnipresent "things", which are encapsulated as software services, which vary from refrigerators, thermostats, toasters, to baby monitors. As our dependence of such the IoT systems is expected to grow significantly in near future, the trust of such systems needs to be a major consideration and evaluated apriori.

Due to the time-sensitive nature of these IoT systems and the associated trust, predicting the trust of these systems before they are created is a research challenge that must be soon solved. This S2ERC research effectively addresses this prediction challenge by creating a trust model based on the principles of machine learning, service computing, software services and associated quality of service (QoS), and the context of such IoT Systems. This model advocates the "trust-by-construction approach" - where trust from the onset is an integral part of the design of such IoT systems. Preliminary results indicate that the proposed trust model is accurate and robust, and generalizable to many application domains.

Learning thermostats are one example of IoT systems. Credit: iStock

One of the factors that cause security vulnerabilities in the IoT systems is that systems are too often developed by composing many independently developed software services; some of which can be malicious and untrustworthy. A majority of the prevalent techniques used to compose these IoT systems consider neither the notion of trust from the beginning nor the context of the constituent software services. These approaches also, too often ignore the personalized trust requirements of end users. Although these assumptions do simplify the composition of IoT systems, in practice, the behaviors of "things" (and hence,

the associated software services) in IoT systems is highly depend on their contexts and on the personalized trust requirements of users.

The proposed model can assess trust of the individual software services and composed IoT systems and identify the minimum information required by each service to enforce better access control to sensitive data and detect anomalies. Furthermore, the proposed model will continuously adapt itself, in response to changes in the contexts of the IoT systems. It will also suggest alternative compositions with optimum QoS and functionality. Hence, this model will allow the developers of IoT systems to prune unwanted alternatives in the early developmental stages and will not only increase the confidence about these systems but also will reduce the associated costs.

Major benefits of this research will be for companies who are building or looking to build IoT systems by assembling multiple third party services. These IoT systems impact encapsulated software services. In such situations, ensuring that each IoT end point is safe and trustworthy is of paramount importance. This breakthrough trust model has the potential of helping several companies build a variety of IoT-based services and systems on top of a trusted security model that can deal with dynamic ensembles of "things." In addition, due to the strong theoretical underpinnings of this research, companies will be able to assess the trust of their IoT systems to obtain high confidence in their solutions.

> **Economic impact**: One of the key factors to challenging the full potential of IoT is its security aspect. Because the scale of IoT is extremely large, the damages that can accrue due to IoT security flaws can be massive. Hence, a simple to use, yet highly secured IoT solution is a MUST to facilitate largescale commercial adoption of IoT. A step towards that vision is this validated trust prediction model. The model will not only enforce the "trust-by-construction" approach for developing the IoT systems, but also will conserve the design efforts by eliminating infeasible alternatives in the early stages of development cycles. In addition, a tool suite that employs this model will make the process of analyzing the trust of individual services and their ensembles semi-automatic, thereby, increasing the productivity of the developers and engineers. The pruning of inappropriate choices and automation will result in significant cost savings while developing the future generation of IoT systems.

For more information, contact Rajeev Raje at Indiana University-Purdue University, Indianapolis, rraje@cs.iupui.edu, Bio http://cs.iupui.edu/~rraje/, 317.274.5174 and/or Dimuthu Gamage, dcundupi@cs.iupui.edu, Bio http://cs.iupui.edu/graduate/students/dimuthu-undupitiya-gamage, 317.702.3489.