

**Name:** COTS Based System Security Testbed - *Tiramisu*

**Presenter(s):** Yue Chen

**Objective:**

- Evaluate the security of COTS Based IT Systems with respect to how stakeholder values rely upon system confidentiality, integrity, and availability
- Help management make decisions on “how much security is enough” with tangible evidence
- Prioritize COTS system security vulnerabilities under stakeholder value context

**Rationale:**

We evaluate the security of COTS Based System through 3 steps: Step 1, Interview key stakeholders to determine how organizational values rely upon IT system security; Step 2, Enumerate scenarios how stakeholder values can be compromised by exploiting known system vulnerabilities. Step3 Model the system security threat based on analysis of all scenarios. The Step 2 and 3 are fully tool automated.

Furthermore, the ROI of security practice can be estimated by comparing the threat score before and after the security investment; the vulnerability can be prioritized by its potential stakeholder value impacts.

We have conducted two case studies on real projects at the USC Information Technology Services. The initial client feedbacks are very positive.

**Target Users:**

- Security investment decision makers
- Security managers
- System designers of security critical systems
- IT system maintainers

**Scope:** Security threat model for COTS Based System; Security ROI Analysis;

**Project Type:** Multi-year USC-CSSE research project

**Runs On:** Windows XP, 2000, 2003

**Developer(s):** Model Principle: Yue Chen

Tool Developer: Yue Chen

**Free COTS Security Evaluation Services:**

As next steps, we are looking for more real-life projects/systems to validate and mature our model. For each system, you will get a free security vulnerability list prioritized with respect to your business context after 2 two-hour-interviews. If interested, please contact Yue Chen at [yuec@usc.edu](mailto:yuec@usc.edu). He is a current PhD candidate under Dr. Barry Boehm.