Evaluation of Threat Modeling Methodologies

Research Review 2016

Motivation

Failure to sufficiently identify computer security threats leads to missing security requirements and poor architectural decisions, resulting in vulnerabilities in cyber and cyber-physical systems.

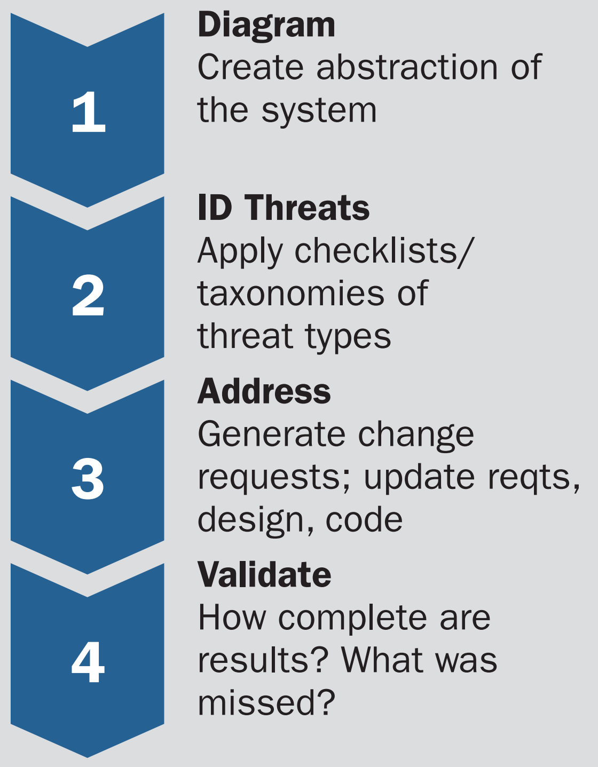
This research compares 3 practical threat modeling methods (TMMs) that pro-actively identify cyber-threats, leading to software requirements and architectural decisions that address the needs of the DoD. Its primary result is a set of tested principles which can help programs select the most appropriate TMMs, accompanied by evidence of the conditions under which each technique is most effective. These principles can be applied to better assess the confidence that can be had in cyber threat analysis.

> "…engineers have not had sufficient training nor been encouraged to have a mind-set that considers how an adversary might thwart their system… the R&D community has not given engineers the tools they need."
>
> —Greg Shannon, SEI/CERT
> Chief Scientist
> *IEEE Institute*, March 2015

The Study

Evaluate three exemplar Threat Modeling Methods, designed on different principles, to understand strengths and weaknesses of each.

"Generic" TMM



1 **Diagram**
Create abstraction of the system

2 **ID Threats**
Apply checklists/ taxonomies of threat types

3 **Address**
Generate change requests; update reqts, design, code

4 **Validate**
How complete are results? What was missed?

STRIDE

- Represents State of the practice
- Developed at Microsoft; "lightweight STRIDE" variant adopted from Ford Motor Company
- Successive decomposition w/r/t system components, threats

Security Cards

- Design principle: Inject more creativity / brainstorming into process, move away from checklist-based approaches
- Developed at University of Washington
- Physical resources (cards) facilitate brainstorming across several dimensions of thereats
- Includes reasoning about attacker motivations, abilities

Persona non Grata

- Design principle: Make problem more tractable by giving modelers a specific focus (here: attackers, motivations, abilities)
- Developed at DePaul University based on proven principles in CHI.
- Once attackers are modeled, process moves on to targets and likely attack mechanisms

Apply to two different DoD-relevant Scenarios:

Drones

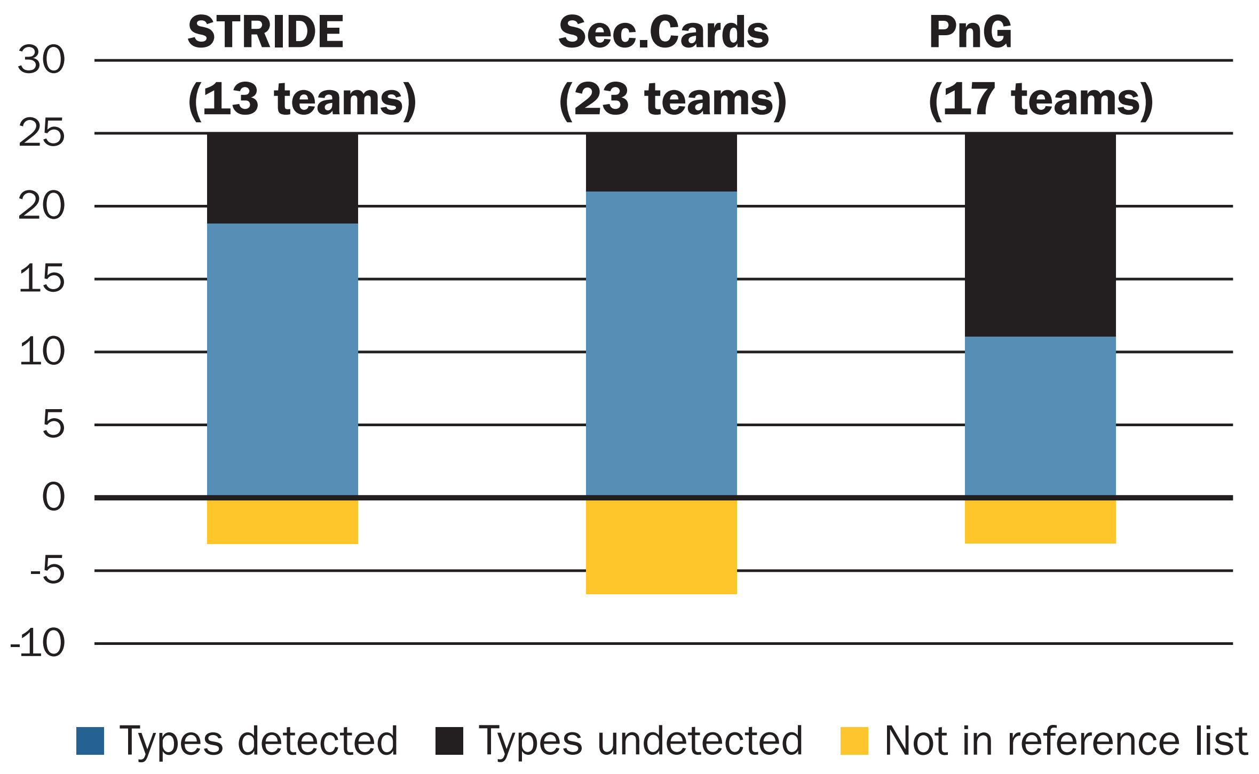
Aircraft maintenance application

"True" threats determined by professional threat modelers.

Results

We identified characteristic differences among the TMMs that affect the confidence to be had in their application on programs. Our data show substantial tradeoffs among threat types detected, number of threats missed, and number of potential false positives reported–and that no one TMM optimizes on all dimensions.

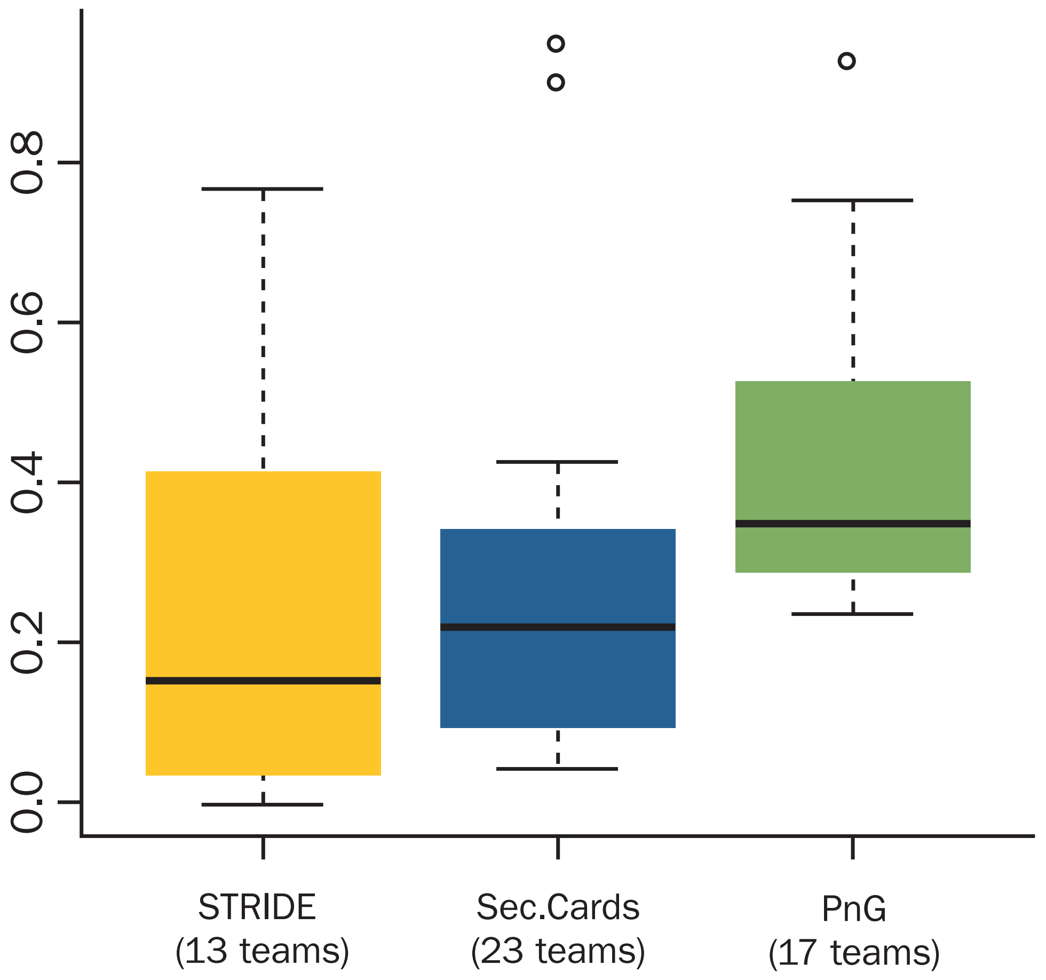
Union of Threat Types



Key results:

- STRIDE: Greatest variability in terms of how frequently it leads to types of threats.
- Security Cards: Able to find the most threat types but also substantial variability across teams.
- PnG: Was the most focused TMM (teams found only a subset of threat types), but showed the most consistent behavior across teams.

Average frequency of detecting threat types



Future Work: Creating a training course of tested threat modeling principles & practices. Looking for transition partners for case studies on DoD programs.

Long term: Our vision is to support dynamic threat models that can trace changes in the threat environment to needed impacts on system requirements, design, and code.

RESOURCES: OSD(AT&L) Working Group on Cyber Threat Modeling brings together practitioners and researchers for quarterly meetings. Ask for details.

Distribution Statement A: Approved for Public Release;
Distribution is Unlimited

Contact: Forrest J. Shull | fjshull@sei.cmu.edu