Evaluation of Competing Threat Modeling Methodologies

Dr. Forrest Shull

Team:

Nancy Mead, Kelwyn Pender, & Sam Weber (SEI)

Jane Cleland-Huang, Janine Spears, & Stefan Hiebl (DePaul)

Tadayoshi Kohno (University of Washington)

Tamara Denning (University of Utah)

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0004095

Cyber Threat Modeling

What is threat modeling?

Threat modeling is an activity for creating an abstraction of a software system—aimed at identifying attackers' abilities, motivations, and goals—and using it to generate and catalog possible threats.

- Threat modeling is of interest to acquisition policy, programs, and research communities.
- Dynamic threat environments mean modeling should be rigorous, routine, and automated.

State of the practice

- Comprehensive catalogs of vulnerabilities, weaknesses, controls
- Competing approaches to modeling; different strategies and application domains
- Often a focus on compliance versus true threat modeling

Goals of the research

Evaluate competing threat-modeling methods (TMMs) to

- identify and test principles regarding which TMMs yield the most efficacy
- provide evidence about the conditions under which different TMMs are most effective.

In short, allow reasoning about the **confidence** to be had in threat modeling results.

Ultimately: improve TMM effectiveness by incorporating the best parts of competing TMMs.

Cyber Threat Modeling

What is threat modeling?

Threat modeling is an activity for creating an abstraction of a software system—aimed at identifying attackers' abilities, motivations, and goals—and using it to generate and catalog possible threats.

State of practice

> "…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

Goals of research

- identify and test principles regarding which TMMs yield the most efficacy
- provide evidence about the conditions under which different TMMs are most effective

Ultimately, the goal is to improve TMM effectiveness by incorporating the best parts of competing TMMs.

Cyber Threat Modeling Subgroup (An Invitation)

- Sponsored by Mr. Jesse Citizen (DoD M&SCO)
- Scope: A forum for threat modeling experts across DoD and the cyber research community to share approaches, their successes and challenges, and to collaborate on initiatives aimed at improving the modeling of cyber threats
- Participants from across the DoD and other government agencies - connections to **cyber operations, training, sys/sw engineering**

Army:
- TRADOC
- CERDEC
- SMDC
- ARL

Navy:
- NavAir
- SPAWAR
- FLTCYBERCOM

Air Force:
- SAF/AQR
- 90th IOS
- AFRL

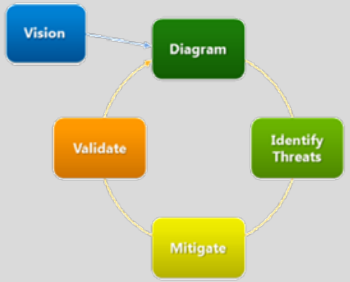
Other DoD / federal:
- STRATCOM
- OSD
- DHS S&T
- NASA
- SEI

Next meeting: **Friday, December 9** at the Mark Center.

Contact me for more details.

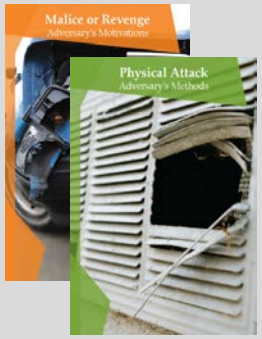
Object of Study: Exemplar TMMs

STRIDE



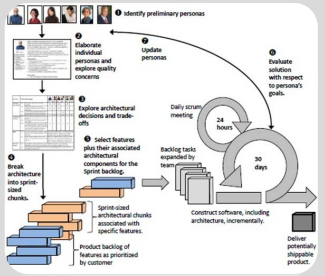
- Represents state of the practice
- Developed at Microsoft; "lightweight STRIDE" variant adopted from Ford Motor Company
- Successive decomposition of w/r/t system components, threats

Security Cards



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

Persona non Grata (PnG)



- 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 HCI
- Once attackers are modeled, process moves on to targets and likely attack mechanisms

Universal lack: empirical evaluation in the context of SDLC

Study Methodology

- 250+ subjects
  - Novice learners (SW and cyber), returning practitioners, professionals
- All applied TMMs to common “testbeds:” systems with understandable ConOps and DoD relevance

UAV (CPS)

Aircraft maintenance app (IT)

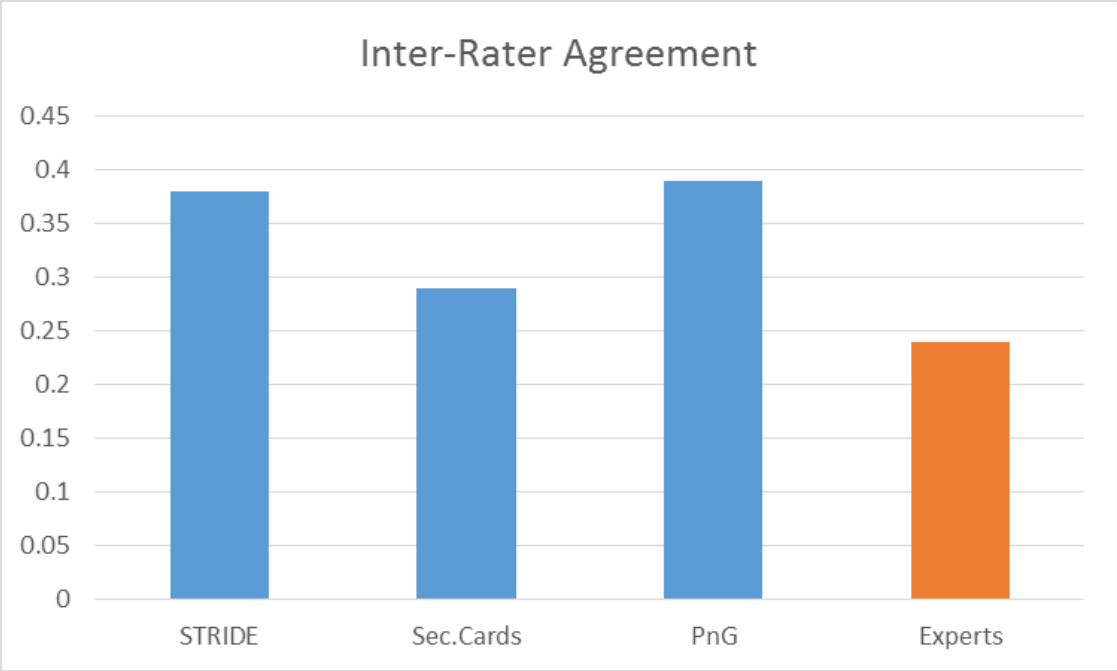
- Within-subjects design: each team learns and applies one approach on a testbed, and then learns the next and applies it on the other testbed.

The threat template, scenarios, and examples are all designed to be reusable. We would be happy to discuss replication in your context, in conjunction with training.

Results: Do Professional Threat Modelers Agree On Potential Threats in a Given System?

Sketch of analysis:

- Professionals use their day-to-day approach to list threats in testbeds
- Categorize professional and subject threats using same schema
- Analyze "inter-rater agreement" – measure of commonality of threat classification across multiple persons (Fleiss' Kappa measure)

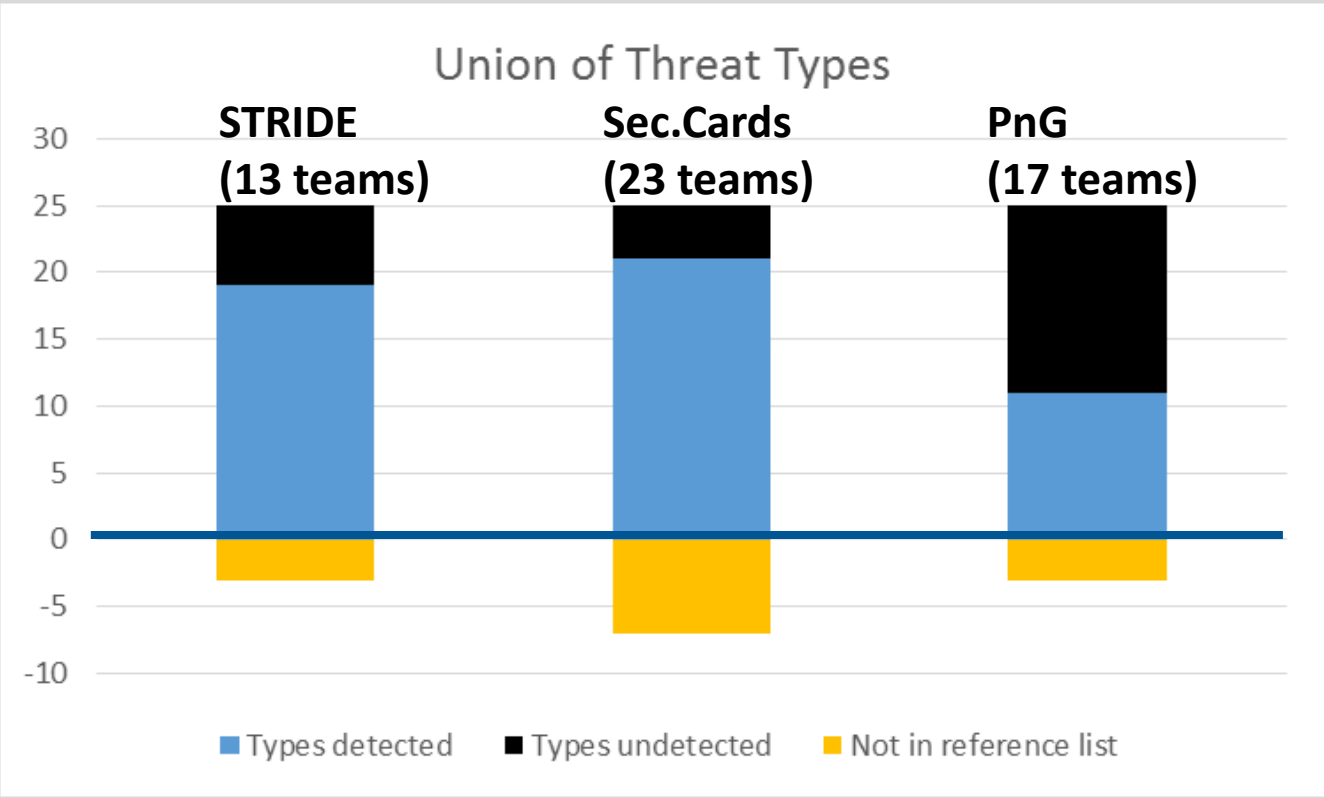


All of the IRA values indicate "fair agreement." However,

- Security Cards brainstorming tends to lead to lower levels of agreement.
- **Experts don't agree any more than other subjects.**

Most significant difference (not shown in chart): **Experts reported many fewer types of threats than other subjects** (33-40%); were more focused.

Results: Do the TMMs Help Modelers Find Important Classes of Threats?



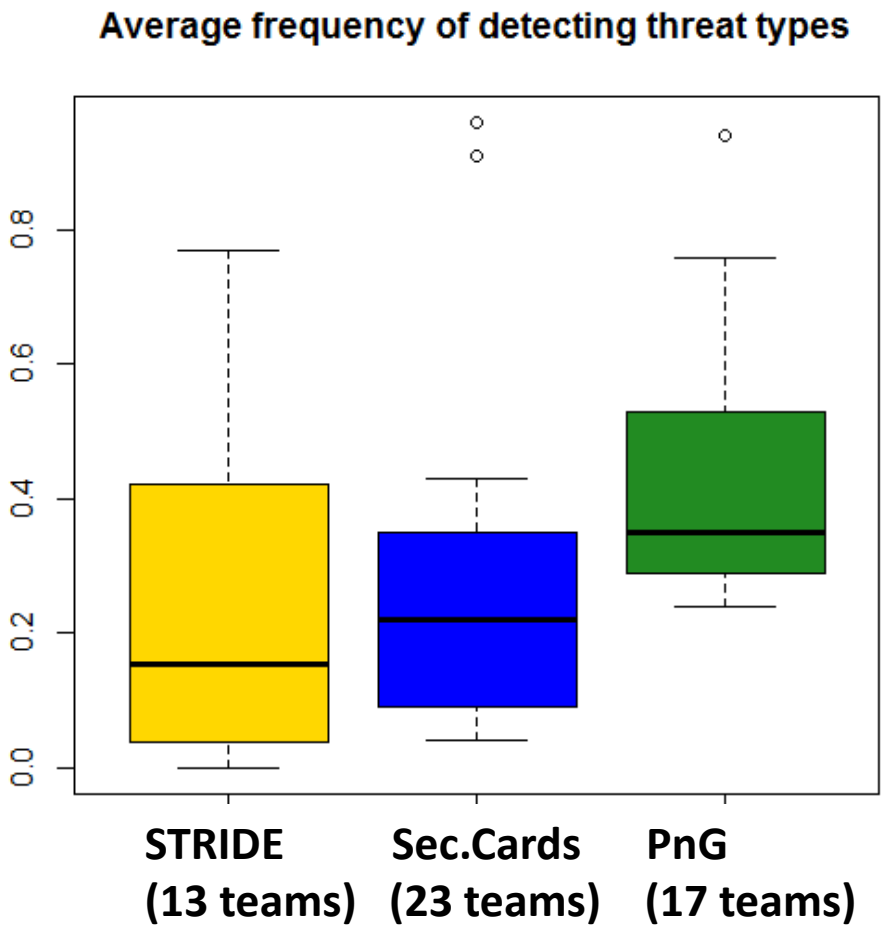
Primary measure:
How many of the threat types identified by professionals were found by our subjects?

Other aspects of effectiveness:

- Some types of threats were never uncovered by teams using some TMMs.
- Some TMMs led to many threat types from outside our expert set. (May be false positives or just unusual.)

Implications for **confidence in modeling results**: The data show tradeoffs among TMMs' reporting of threats and other items not in our reference set.

Results: How Frequently is a Given Threat Type Reported?



Comparison of different TMMs applied to the same testbed highlights additional tradeoffs:

If we know that a TMM was able to find a given threat, how confident can we be that it would be reported by a team?

- STRIDE: Greatest variability.
- Security Cards: Able to find the most threat types but also substantial variability across teams.
- PnG: Was the most focused TMM, but showed the most consistent behavior across teams.

No single TMM led to teams reporting a majority of the valid threats.

Summary and Future Directions

Bottom line: Identification of provisional characteristic differences among important classes of TMMs.

- TMMs are not equally well suited for finding all types of threats
- TMMs exhibited substantial tradeoffs among reported threats, potential false positives, and frequency of reporting
- No one TMM optimizes all dimensions of importance

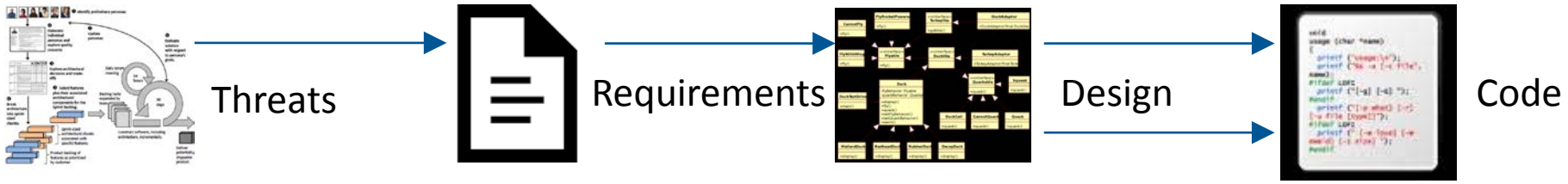
Future Work

- We are looking for research partners for the application of hybrid modeling approaches on real systems.
- Curriculum development efforts can incorporate this study, providing data while giving learners hands-on experiences.

Long-Term Vision

There is much work to be done to reach our long-term vision, which includes

- threat models as **a first-class engineering artifact supported by tools and automation**
- **dynamic models** that can be used to assess impact to the system as the threat environment changes



Contact Info

Forrest Shull

Assistant Director of Empirical Research

Software Solutions Division

fjshull@sei.cmu.edu

703-247-1372 (Arlington)

Nancy Mead

SEI Fellow and Principal Researcher

CERT Division

nrm@sei.cmu.edu

U.S. Mail

Carnegie Mellon University

Software Engineering Institute

4500 Fifth Avenue

Pittsburgh, PA 15213-2612

USA

Customer Relations

Email: info@sei.cmu.edu

Telephone: +1 412-268-5800

Web

www.sei.cmu.edu

www.sei.cmu.edu/contact.cfm

DMSCO Cyber Threat Working Group

Next meeting: Friday, December 9 at the Mark Center (remote participation enabled).

Prior presentations on milSuite:
https://www.milsuite.mil/book/groups/cyber-modeling-and-simulation-threat-sub-group/activity