Crowd Sourcing the Creation of Personae Non Gratae for Requirements-Phase Threat Modeling

Nancy Mead, Forrest Shull, Janine Spears, Stefan Hiebl, Sam Weber, and Jane Cleland-Huang

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM17-0602

Threat Modeling

Our threat modeling definition

A threat modeling method (TMM) is an approach for creating an abstraction of a software system, aimed at identifying attackers' abilities and goals, and using that abstraction to generate and catalog possible threats that the system must mitigate.

Who does threat modeling?

Vendors such as Microsoft

- Microsoft uses STRIDE and makes it freely available

U.S. Government organizations such as DoD

- mandated for DoD
- various methods in use, some are based on NIST standards, some use checklists.

Commercial organizations such as automotive industry, finance, and so on

- various methods in use, including STRIDE, risk analysis approaches such as OCTAVE, attack trees, etc.

SEI's threat modeling research

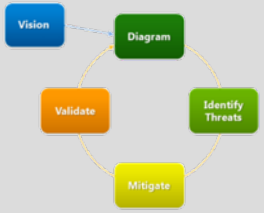
Focus on early lifecycle activities (e.g. requirements engineering, design), independent of lifecycle model.

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.

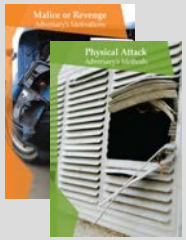
Object of Study: Exemplar TMMs

STRIDE



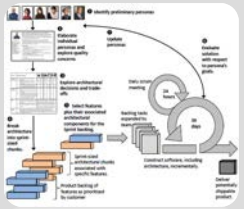
- Represents state of the practice
- Developed at Microsoft; “lightweight STRIDE” variant adopted from Ford Motor Company
- Successive decomposition of w/r/t system components, threats

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

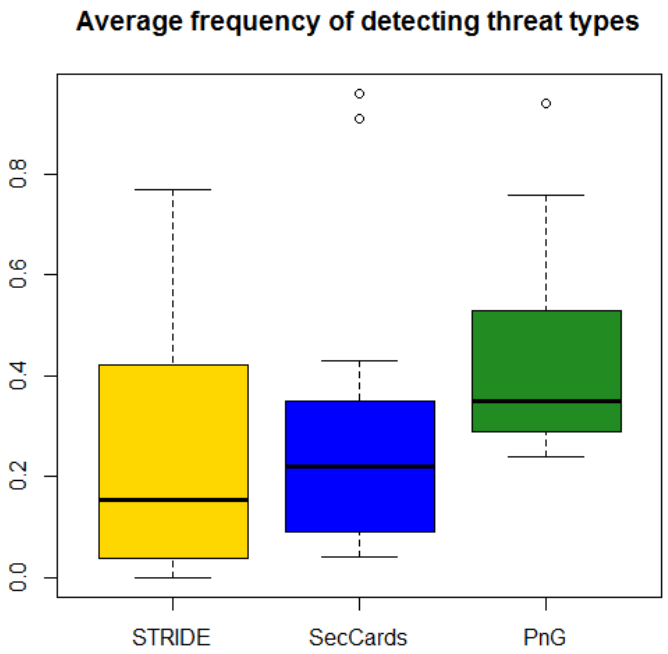
Personae non Gratae (PnGs)



- 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

One of several results: How frequently is a given threat type reported?



STRIDE (13 teams) **Sec.Cards (23 teams)** **PnG (17 teams)**

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: Great 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

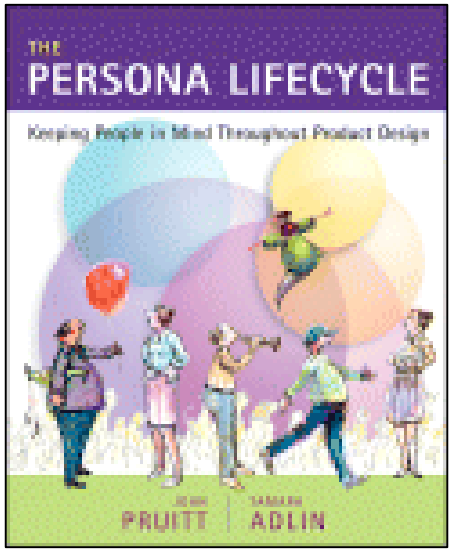
No single TMM led to teams reporting a majority of the valid threats.

PnG Approach

What is a persona?

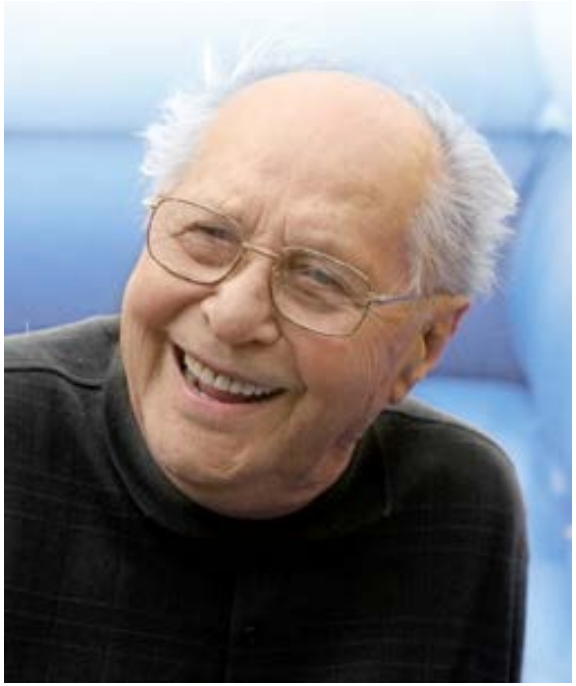
"Personas are detailed descriptions of imaginary people constructed out of well-understood, highly specified data about real people"

— John Pruitt & Tamara Adlin



J. Pruitt, T. Adlin. The Persona Lifecycle: Keeping People in Mind Throughout Product Design. Morgan Kaufman, 2006.

Example Persona



Thomas is 76 years old, a retired accountant and he enjoys spending time with his grand children. During his retirement, he enjoys reading newspapers, working in his garden and staying in touch with friends. He is a free spirit and enjoys exploration and technology, but only when it doesn't get in his way.

Developing a PnG

1. **Motivations:** What is the PnG's motivations? Monetary gain? Revenge? Recognition? "LoLs" (laughs)?
2. **Goals:** How will the PnG fulfill their motivation i.e. what do they want to do and how do they plan to get away with it?
3. **Skills:** What abilities do they have to achieve their goal? What other assets do they have e.g. access to infrastructure, relationships to those who have skills?
4. **Misuse cases:** What are the misuse cases the PnG can follow to achieve their goals?

Example Persona non Grata: Mike

”Mike” is based on the true story of Vitek Boden, who was convicted of causing the release of sewage in Maroochy Shire Council in Queensland, Australia in 2000 after hacking the associated SCADA system. See Abrams & Weiss, 2008.

Description: Mike worked as a contractor installing SCADA radio-controlled sewage equipment for a municipal authority. After leaving the contractor, Mike applied for a job with the municipality but was rebuffed. Feeling bitter and rejected, Mike decides to get even with the municipality and his former employer.

Goals: Cause raw sewage to leak into local parks and rivers and make the events appear as malfunctions. Create a public backlash against the contractor and municipality.

Example Persona non Grata: Mike (cont'd)

Skills: Extensive knowledge of SCADA equipment, including control computers, relevant programs, and radio communication protocols; access to specialized equipment.

Misuse cases:

- Steal control computer and radio equipment from his former employer.
- Using the stolen computer, construct a fake pumping control station from which to send radio signals.
- Gain remote access to SCADA system and disable alarms at pumping stations.
- Issue radio commands (using stolen radio equipment) to instruct pumping stations to release sewage.

Abrams & Weiss, 2008

PnG Study

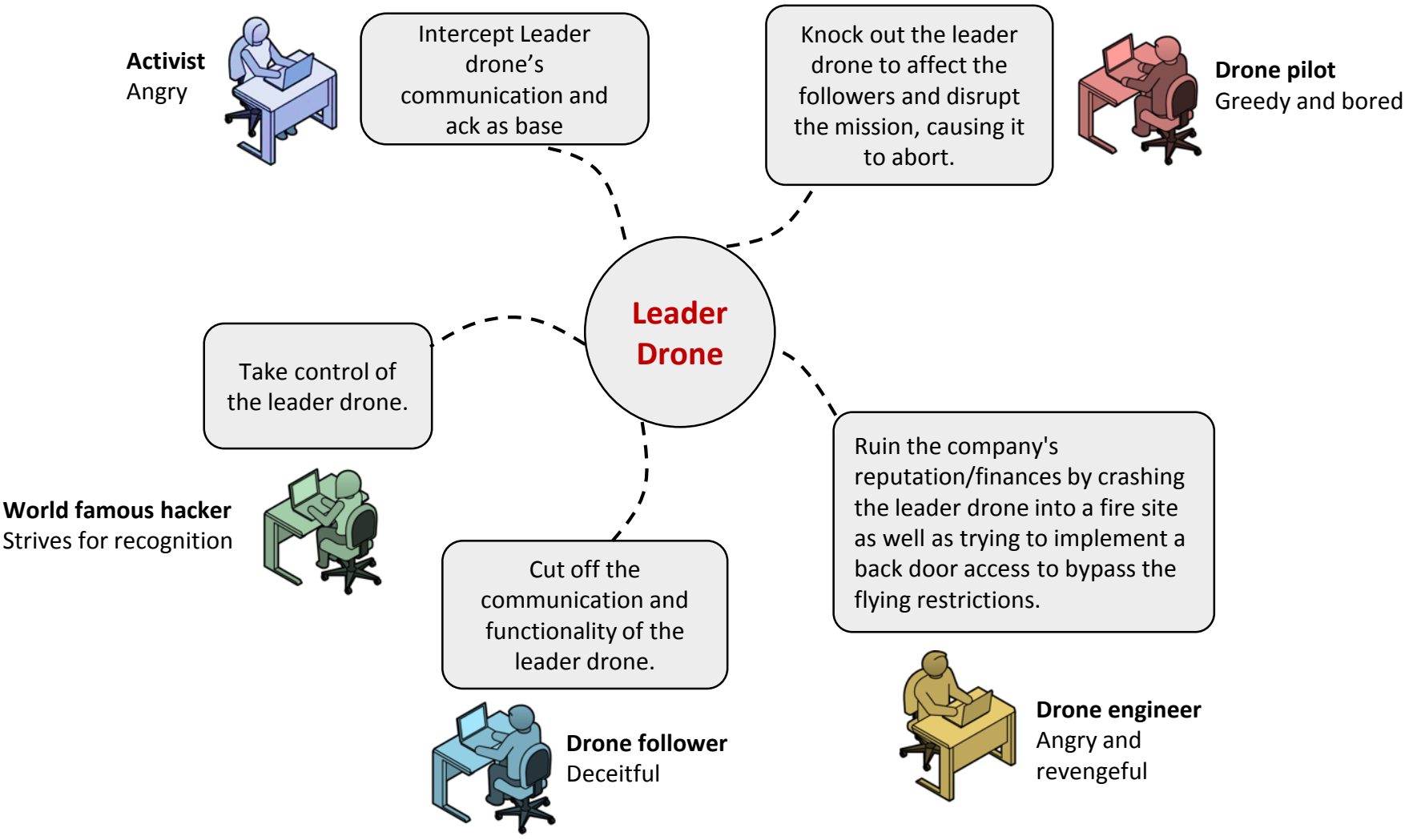
PnG Study Methodology

108 students in two introductory information security courses (undergrad and graduate)

- novice learners (SW and cyber), returning practitioners, professionals
- These are the “crowd”

All applied PnG to an Unmanned Autonomous Vehicle (UAV) system scenario, in teams of 3-4 people.

Spider Web View of Threats Aimed at Leader Drone



PnG Merging Process

Step 1: Discover domain-specific concepts

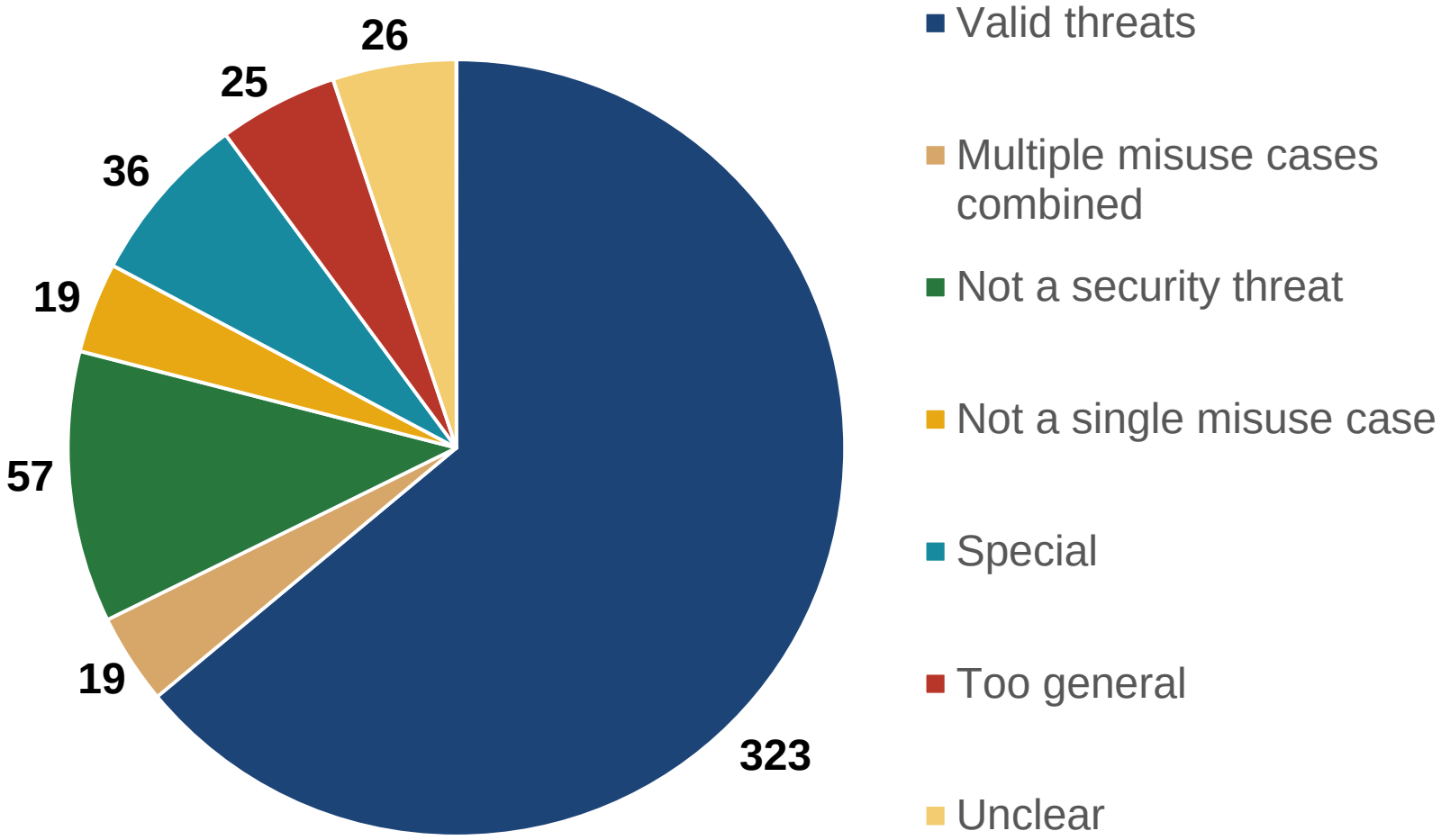
Step 2: Identify attack targets

Step 3: Visually display attack mechanisms

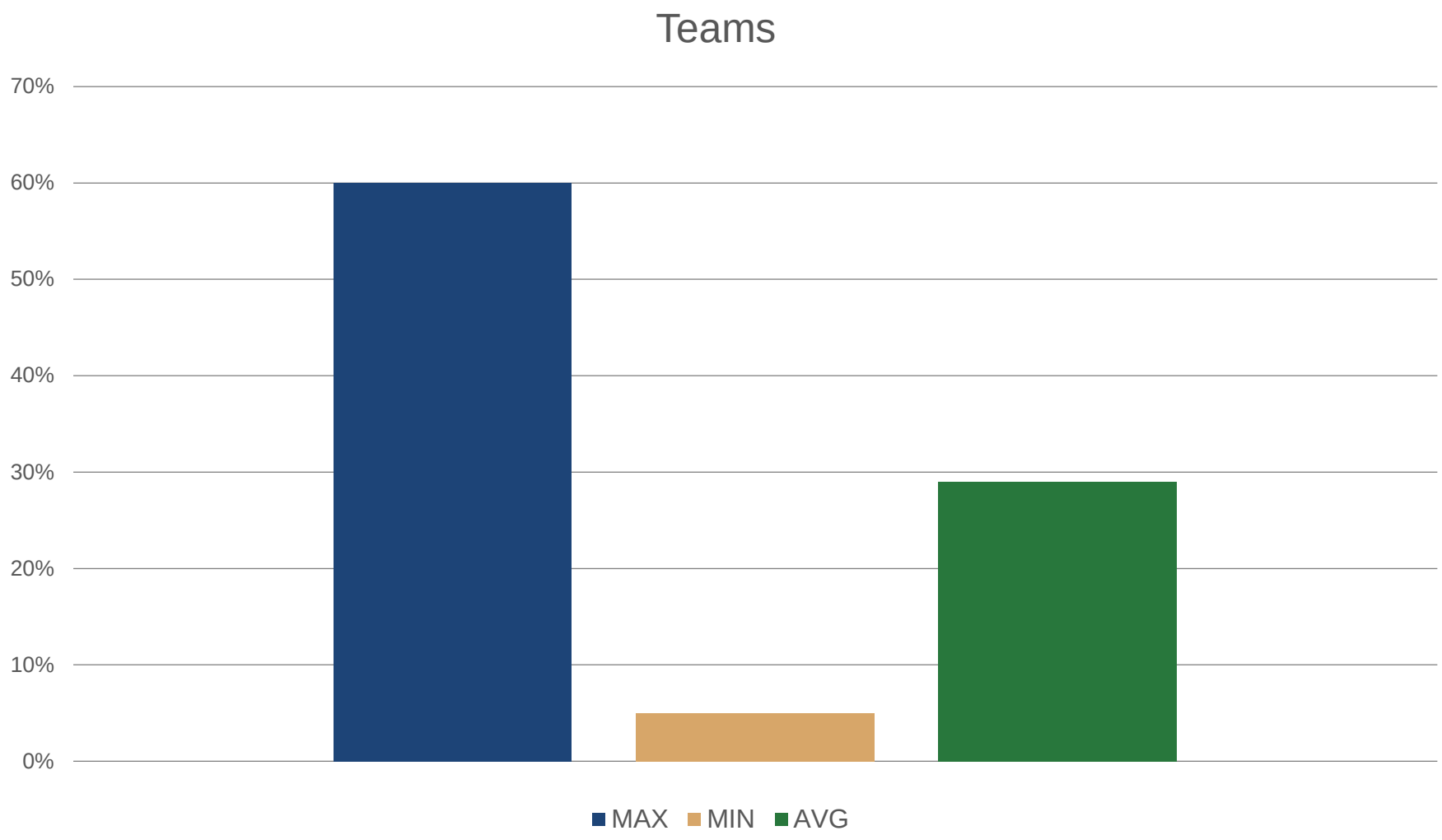
Step 4: Merge individual threats into new PnGs

Step 5: Check for redundancy

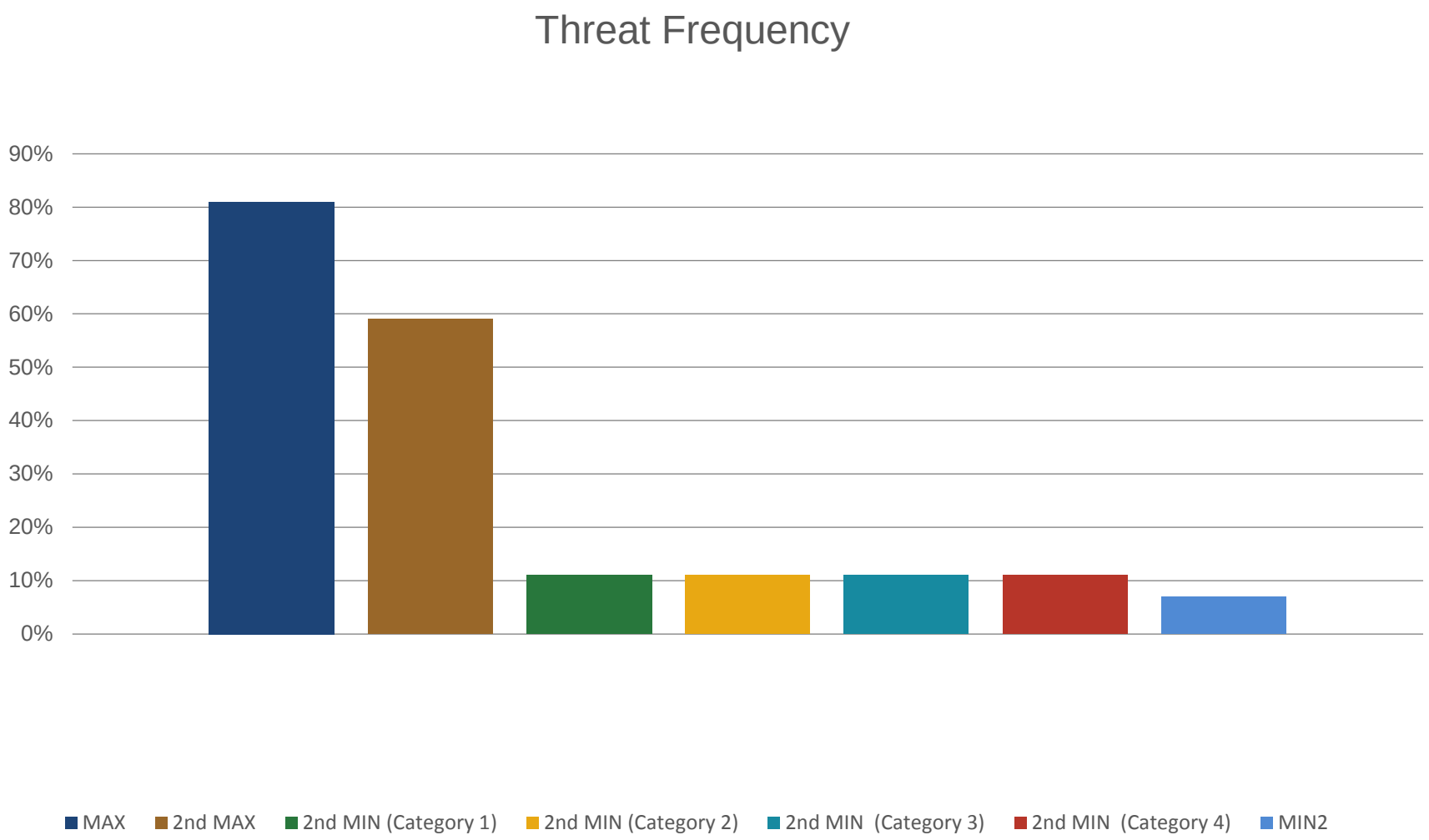
Student PnG Analysis Insights – Overview



Student PnG Analysis Insights – Valid threats



Student PnG Analysis Insights – Valid threats



Discussion

Threats to Validity

- Only one case study was explored.
- Crowd was information systems students, not necessarily IT professionals.
- Presented only one example, which was not evaluated quantitatively.

Conclusion and Future Plans

- Machine Learning could be used to analyze individual PnGs created by a crowd.
- Our approach resulted in PnGs that could serve as input to the requirements process.
- Approach was illustrated in one project domain, but not fully evaluated with users.
- Plans are to develop specific tooling to support all aspects of our process.
- Experiment in diverse domains and projects.

Questions?