Addressing Uncertainty in Cyber-Security Experts’ Perceptions of Risk

Jon Garibaldi
Simon Miller, Uwe Aickelin

Structure
• Aims
• Information Security Risk Assessments
• CESG Initial Exercise
  ▫ Results
• CESG Main Exercise
  ▫ Results
• Current/Future Work
• Summary

Aims
The objective of this research is to:
• Understand the practicalities of decision making
• Examine the variation that occurs between experts and groups of experts
• Assess whether aggregation can be used to aid decision making

Information Security Risk Assessments
Information Security Risk Assessments:
• Assess the risk to a computer system and the information it contains
• Of increasing importance as cyber crime affects more of our every day activities

Information Security Risk Assessments
Failure to carry out appropriate risk assessment can result in:
• Over defending – Excessive cost and effort are expended, out of proportion with the danger posed
• Under defending – Lack of sufficient precautions leads to increased risk

Information Security Risk Assessments
Assessment is made more difficult because experts may have different areas of expertise/experience
• This leads to a variation in opinion, resulting in different outcomes
• For the user, inconsistent results are not desirable
• By combining the opinions of experts we may produce a more stable output
CESG Exercises

The CESG exercises focus on assessing the risk of technical attack for a security architecture.

- A scenario was created by CESG detailing a realistic proposal for an information system
- Experts were then asked to rate the risk aspects of the system presented

Scenario

- New EU subsidies designed to reward efficient production of fruit and vegetables
- A new system is required that can interact with untrusted endpoints to collect data required for payments

Scenario

- An office automation system that enables statistics to be gathered from rural areas and enables payments to be made
- Must support the interchange of information between payment agencies and the European Union

Initial CESG Exercise

In the initial exercise 6 technical experts from CESG:

- Created 10 “Attack Vectors” (AVs) for the scenario
- Individually ranked the AVs in order of difficulty
  - without the benefit of a detailed description of the system

Results - Group Agreement

The results show:

- There is some variation in the assessments
- But, there is a definite consensus of opinion
- Even though the scenario was lacking in detail
Main CESG Exercise

In the main exercise 39 experts from 7 groups of the cyber security community:

- Ranked 10 AVs for a refined version of the scenario
- Rated the “hops” that make up each AV by answering a series of questions

Questions included:

- ‘How likely is it that there is a publicly available tool that could help with this attack?’
- ‘How mature is this type of technology?’

Participants gave their answers in the form of intervals

Results - Overall Agreement

The width of the interval denotes the uncertainty

Future Work

Having examined the variation in AV ranking, our attention turns to the hop data:

- Use the hop data to assess AVs
- Model the hop data using fuzzy sets
- Using the models, create an expert system to undertake parts of the decision making process

Summary

- Conducted 2 risk assessment studies with CESG
  - First objective measurement of domain
- The results have shown:
  - While there is variation in opinion, there is a definite consensus of opinion
  - Some groups are more consistent than others
- Future work will focus on the hop data that has been collected