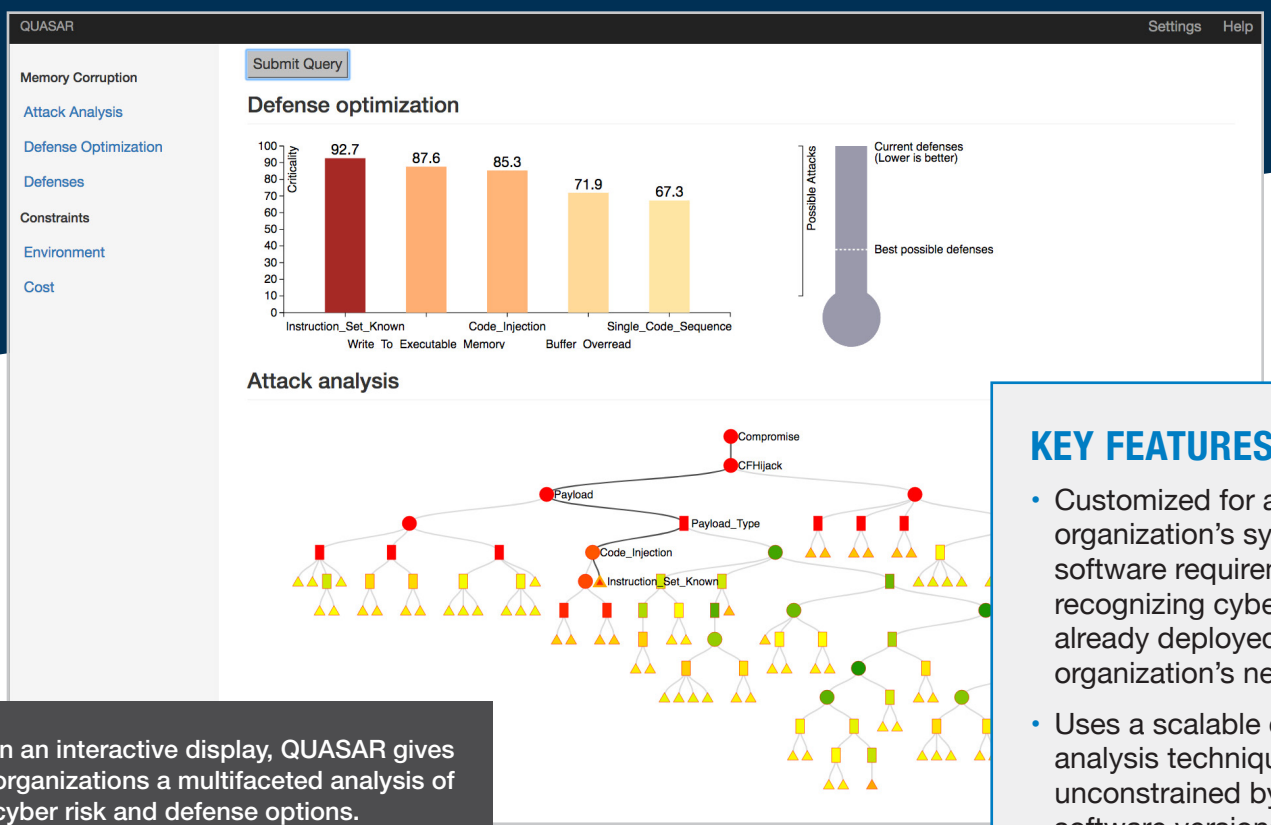
MIT LINCOLN LABORATORY

INNOVATION HIGHLIGHT

Technology in Support of National Security

WWW.LL.MIT.EDU

Quantitative Attack Space Analysis and Reasoning (QUASAR)



In an interactive display, QUASAR gives organizations a multifaceted analysis of cyber risk and defense options.

QUASAR software analyzes countermeasures to potential cyberattacks on an enterprise network. It answers a range of questions to inform decisions about cyber defenses: how do different countermeasures affect the network, what defensive investments are most valuable, how may attackers respond to certain defenses, and what gaps in defense coverage remain?

KEY FEATURES

- Customized for an organization's system and software requirements, recognizing cyber defenses already deployed on the organization's network
- Uses a scalable defense analysis technique unconstrained by specific software versions or configurations
- Evaluates/prioritizes the success of different cyber defenses against potential attacks so customers can proactively secure systems
- Facilitates budget planning by providing estimates of the costs for various cybersecurity solutions
- Provides information in a user-friendly visualization

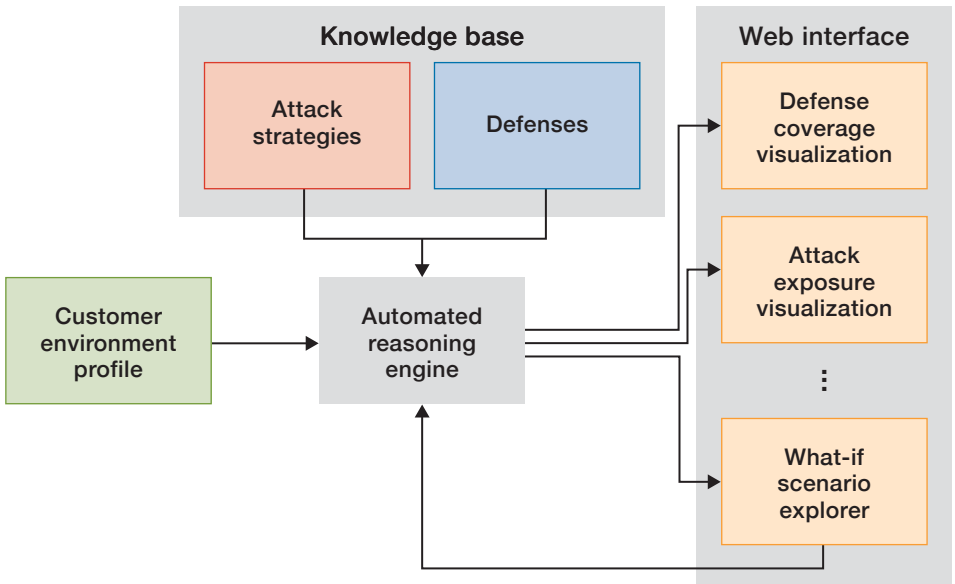
LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Quantitative Attack Space Analysis and Reasoning (QUASAR)

Cybersecurity personnel in an organization are faced with many questions when choosing defenses to best protect their network from cyberattack. What software or techniques are worth deploying? How do these defensive solutions interact with the organization's existing systems? Are there gaps in the cybersecurity coverage? What strategies might attackers use to bypass the organization's defenses?

Lincoln Laboratory researchers developed QUASAR to help cybersecurity specialists answer these and other questions about countering attacks. QUASAR has three components:

- A knowledge base of cyberattack strategies and defenses drawn from 10 years of academic publications and incident reports; this base is kept up to date with information from threat intelligence data provided by private industry and academic cybersecurity research
- An automated reasoning engine that combines the knowledge base with a high-level profile of the customer's environment to create a tailor-made mathematical model of possible attack surfaces and defenses to mitigate them
- A browser interface for visualization and interactive analysis of the tradeoffs between different defensive strategies; this visualization displays quantitative metrics about the impact that proposed defenses would have on a customer's network and recommendations for additional defenses to mitigate an attack



The three-part QUASAR architecture, tailored for an individual customer's environment, uses a knowledge base of known attack strategies and defenses to inform the automated reasoning engine that analyzes the strategies and defenses in the context of the customer's network and that inputs the results into a web interface that displays the analysis results via multiple visualizations.

QUASAR recommendations for defenses are based on an examination of the capabilities needed to mount a successful attack. This approach guides strategic reasoning for an organization's defense planners and provides insights for researchers developing new cyber defenses.

INTERESTED IN ACCESSING THIS TECHNOLOGY?

Contact the MIT Technology Licensing Office
https://tlo.mit.edu/
tlo-inquiries@mit.edu 617-253-6966

U.S. PATENT #10,819,752

INTERESTED IN WORKING WITH MIT LINCOLN LABORATORY?

https://www.ll.mit.edu/partner-us

Contact the Technology Ventures Office
tvo@ll.mit.edu

More Information

R. Skowyra et al., "QUASAR: Quantitative Attack Space Analysis and Reasoning," *Proceedings of the 33rd Annual Computer Security Applications Conference*, December 2017.

Approved for public release; distribution is unlimited. This material is based upon work supported by the Department of Defense under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the Department of Defense.