Assessing Security of Encrypted Messaging Applications (ASEMA)
HR0011SB20254-12
Frequently Asked Questions (FAQs)

https://www.darpa.mil/research/programs/asema

As of 18 September 2025

Q1. Does ASEMA expect the use of XAI/ML for vulnerability detection, or is the emphasis on traditional cryptographic analysis?

A1. The ASEMA SBIR expects the security risks of the applications themselves, more specifically the code that interacts with the network and the mobile operating system, to be assessed. Cryptographic protocols used by secure messaging applications (SMAs) are already well-understood and well-tested security properties, and therefore not the focus of this effort.

Q2. Are there priority operational contexts (e.g., tactical units, coalition partners) for this capability?

A2. There are no priority operational contexts for this capability.

Q3. Will performance be judged more on detection accuracy, processing speed/latency, or resilience under adversarial attack?

A3. As outlined in the SBIR, proposers are expected to detail their own proposed metrics and scope for final evaluation.

Q4. For attack-surface modeling, does DARPA expect proposals to include dynamic binary analysis of iOS/Android SMA clients, or are static reverse-engineering and fuzzing frameworks sufficient for Phase II?

A4. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

Phase I feasibility will be demonstrated through evidence of: a completed feasibility study or a basic prototype system; definition and characterization of properties desirable for both Department of Defense (DoD) and civilian use; and comparisons with alternative state-of-the-art methodologies (competing approaches).

Q5. Are there quantitative benchmarks for exploit detection coverage (e.g., % of API/system call attack paths exercised) that frameworks must meet to demonstrate measurable resilience?

A5. See previous (#4) answer.

Q6. For prototype evaluation, does DARPA require integration with real-world encrypted messaging platforms (Signal, WhatsApp) in red-team trials, or is simulated attack emulation acceptable?

A6. DP2 proposals should:

- describe a proposal to achieve the aforementioned goals;
- present a technical plan and approach, with notable risks/mitigations; and
- detail proposed metrics and scope for final evaluation.

Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q7. Would looking at types of cyber risks beyond vulnerabilities, such as backdoor access behaviors, where data may be exfiltrated from the system, or types of interactions with the OS be in scope and of interest?

A7. The program seeks novel approaches to key technical challenges, including but not limited to:

- Characterizing and modeling the attack surface of SMAs.
- Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
- Developing tools and techniques for evaluating the security features of SMAs.

The goal of this topic is to design and develop prototype models, frameworks, and methods of evaluation to defend SMAs from real-world attacks.

DP2 proposals should:

- describe a proposal to achieve the aforementioned goals;
- present a technical plan and approach, with notable risks/mitigations; and
- detail proposed metrics and scope for final evaluation.

Phase II will culminate in a demonstration that shows compelling use cases consistent with commercial opportunities and/or insertion into a DARPA program which seeks to establish automated vulnerability discovery capabilities for cybersecurity applications.

Q8. Would looking for standard vulnerabilities (memory corruption, command injection, etc.) also need to be a focus for a strong proposal?

A8. See above (#7) answer.

Q9. Are there any particular types of cyber risks that are of the most interest?

A9. See above (#7) answer.

Q10. Are the protections and security assessments sought in this topic specifically intended for mobile devices running iOS or Android operating systems?

A10. This program does not have specific requirements for what mobile devices operating systems a SMAs should be evaluated on.

Q11. Alternatively, would a response detailing security controls or mitigations implemented at the primary server level (or within the broader system architecture) be considered acceptable for this solicitation?

A11. 2. The program seeks novel approaches to key technical challenges, including but not limited to:

a. Characterizing and modeling the attack surface of SMAs.
b. Developing a framework that identifies and recommends security boundaries, protections, and mitigations for SMAs.
c. Developing tools and techniques for evaluating the security features of SMAs.