HR001118S0052
Resilient Anonymous Communication for Everyone (RACE)
Frequently Asked Questions

As of July 26, 2018

Q43: During the Proposers Day, it was announced that the program funding is $44M. We are wondering if this number includes the T&E budget? Or is it solely representing TA1 through TA3.1?
A43: The anticipated funding identified in the BAA does not include T&E budget.

Q42: Would covert computation be considered to be in scope? Very roughly, covert computation hides the fact that is a computation taking place from an external party (by embedding protocol messages in another protocol similar to your TA2). However more interestingly, even if one of the parties is compromised, it is hard to tell if the other party was participating in the computation or not.
A42: Covert computation would be in scope for TA1 to the degree that they satisfy the other metrics for TA1. They are in scope for TA2 to the degree that they satisfy the desired functionalities and metrics for TA2. As a reminder, abstract submissions are highly encouraged to help proposers determine the degree to which their solutions are in scope.

Q41: There is a difference between what was mentioned during the Proposers day and the BAA in terms of exercises, which is the correct number of scrimmages with the T&E team?
A41: The BAA will be amended to correct this. Please use the amendment for planning and costing purposes. There will be two scrimmages in Phase 1, one scrimmage in Phase 2, and two scrimmages in Phase 3.

Q40: To what extent are stronger and/or more-general adversarial models of interest? (e.g., all clients corrupted, or higher probability of servers in hostile territory being corrupted.)
A40: Adversarial models that capture the real-world security threat landscape are in scope (see the BAA for a discussion on adversary models). There is no a priori limit on the number of corrupted clients. From a security perspective, all servers are assumed to reside in the contested network environment.

Q39: What does "node refresh" rate in table 3 mean? Is this the rate at which new server nodes join? (i.e., new node joins per month according to table 3.)
A39: Node refresh rate is the maximal time over which corruption of nodes will occur. E.g., a node refresh rate of 1/month assumes the corruption rate (e.g., 10%) occurs over that month. Within that context, corrupted nodes should be removed and uncorrupted nodes should be added to maintain the security of the system.

Q38: Please clarify DARPA's definition (or difference between) "protocol encapsulation" and "protocol obfuscation"?
A38: Protocol encapsulation is a technical means to achieve protocol obfuscation.

Q37: What is meant by "ubiquitous encryption, even during computation"?
A37: Data is encrypted at all times, even during computation.

Q36: Will a bidder submit separate 36-page proposals for each TA, or one 36-page proposal for however many TAs they wish to be considered for?
A36: Submit a separate proposal for each TA, with the exception of TA 3.1. Per the BAA, TA 3.1 can be combined with either a TA 1 or a TA 3 proposal. A TA 3.1 combination proposal is allowed a 42-page limit.

Q35: Can you define "broadcast-based network services" on page 11 of the BAA?"
A35: Network services that perform a broadcast-like function.

Q34: Is it in within or out of scope to test the application with either: 1) simulated user traffic from an actual contested area or 2) an actual test with users in a contested area?
A34: Tests will be in an internal, simulated environment. The RACE program will not perform external testing.

Q33: Which TA is responsible for providing protocols to ensure resilient link operations in the presence of NAT, firewalls, and dynamic addressing? Are these functions in scope for TA2 or TA3?
A33: To the extent that such work is needed to provide RACE communication channels between RACE servers and/or clients, this is in scope for TA2. If such work is needed to create network protocols over such links in order to build the broader RACE system, this is in scope for TA3.

Q32: Can you elucidate what you mean by "entirely within the [contested] network environment? Some services can operate disconnected from upstream, but will drift, over time (DNS). Is it meant to constraint TA2 to only peer to peer services that operate within some time window or disconnection?
A32: RACE proposals should propose technologies that reside entirely within the contested network environment.

Q31: Static or adaptive adversary? For TA1, is the communication graph known? If not, do TA1 performers need to discover it? Who comes up with the things TA1 performers are supposed to compute? Should a TA1 performer be computing everything, or will the capabilities of TA1 performers be combined to build the race system?
A31: RACE proposals should propose security models that most accurately reflect realistic security concerns (and justify those decisions). The decision of what to be computed by TA1 performers is up to the proposer, with the understanding that all performers will work together to jointly build the RACE system.

Q30: Is risk assessments needed at the abstract submission stage?
A30: Abstracts should outline and address all technical challenges inherent in the approach and possible solutions for overcoming potential problems in order to provide sufficient description to enable an in- or out- of scope assessment.

Q29: Is there a typical team size you are looking for TA1 and TA2?
A29: No.

Q28: Does the channel include the physical channel (e.g., RF)?
A28: RF communications are not in scope for RACE.

Q27: For planning purposes, how many TA1 and TA2 performers should TA3 assume there are?
A27: Undecided at this time. TA3 proposals should discuss their performer assumptions and the extent to which the number of other performers greater than this assumption affect their solution and cost.

Q26: Would a secure MPC for general polynomial-time functionality be in scope?
A26: Concretely, vs asymptotically, efficient solutions are desired.

Q25: Do server nodes have limited storage capacity?
A25: Proposals should make clear their assumptions; realistic solutions are desired.

Q24: Are rigorous statistical distance proofs required for adversarial scenarios where server nodes are corrupted?
A24: Yes. See Table3 located in the BAA.

Q23: Is it assumed once a server or client is corrupted, the adversary has full control of the node including keying material?
A23: Yes.

Q22: Is it assumed the adversary adaptively corrupts existing servers over time to reach 20% corruptions?
A22: Yes

Q21: Will messages only be point to point? Or will there be group/multiparty messages?
A21: Point to point messages are the desired functionality, group/multiparty are not explicitly required for RACE.

Q20: Will programming frameworks and software stacks be determined by TA3?
A20: All TA performers will work together to create the RACE system. Proposers should discuss why their programming frameworks and software stack will be amenable for collaboration/integration.

Q19: Does TA3.1 (if combined with other TAs) need a separate SoW, Summary, LoE document?)
A19: Yes.

Q18: What is meant by "proof" in TA2?
A18: Ideally, we would like a formal security argument via mathematical principles, combined with an argument as to why the target channel (and encapsulation means) are indeed described within the argument.
We understand that there may be limitations on the bandwidth of solutions with truly formal security arguments. However, the overall goal is to demonstrate statistical closeness (or indistinguishability) of the statistics of the normal channel to the statistics of the channel when encapsulation occurs.
Since the changes of the normal channel (and statistical distribution of messages to be encapsulated) are likely to not be covered by a discrete set of simulations, we are looking for

some notion of extrapolation argument to have confidence that statistical closeness indeed occurs. These arguments should, by the end of the program, cover how an adversary may manipulate the channel to try to discover whether a particular channel contains encapsulation or not.

Q17: Does each Client have a separate broadcast channel to the servers or a single shared Channel across all clients?
A17: This is up to TA2 proposals.

Q16: How do servers send data/outputs back to the clients, over what TA2 channels and how much bandwidth is assumed?
A16: This will depend on the message passing architecture as determined within TA1. TA2 proposals should discuss how they could support different architectures.

Q15: Does TA1 have to address how Alice will reach the MPC-based tasking services, or is that a TA2 or TA3 issue? If this is highly dependent on the MPC and tasking, can it be addressed in TA1?
A15: How nodes communicate with each other is not in scope for TA1. TA performers will be expected to work with each other to construct the most efficient and secure RACE system.

Q14: Can TA2 also bid for TA3.1? The BAA mentions TA1 and TA3 can bid for TA3.1 but didn't mention TA2 (Specifically).
A14: Anyone can bid for any TA. However, TA2 proposals cannot also address TA3.1 within the same proposal (unlike TA1 and TA3).

Q13: In the proposed scenario, servers are assumed to all be in hostile territory. Is the assumption that the system should not rely at all on "external" servers in a safer environment?
A13: Yes.

Q12: What assumptions can be made about the safety of TLS or other application security (e.g. skype) layers from the network adversary DPI?
A12: Proposers should make clear their security assumptions (and motivate those assumptions, to include a risk profile in necessary). These assumptions should reflect realistic deployment scenarios. For example, see the BAA TA2 language that discusses how proposals can be tailored for specific environments so long as those choices and reasoning are made clear.

Q11: Does the size of the team matter? E.g. are bigger (multiple PI) teams preferred over small teams?
A11: No.

Q10: For TA2 how much cryptography should be assumed and utilized in proposal and during development? Should some cryptographic functions be assumed and which?
A10: TA2 proposals should provide secure communications per the BAA. Whether or not TA2 should use particular cryptographic functionalities is up to the proposer.

Q9: For TA3.1, is the executable expected to be compiled and more secure from de-compilation, or is de-compilation/reverse engineering not important to the program?
A9: Securing the output executable post-recombination is not in scope for RACE.

Q8: Confirm that TA3.1 can be bid standalone? Would distributed App for TA3.1 be single cross platform exe or multiple versions for each operating system?
A8: Confirmed. TA3.1 should support all necessary RACE executables. Android/windows/linux version

Q7: Can one propose against TA3.1 w/out proposing against TA3 or TA1?
A7: Yes.

Q6: Is "Auditable" a requirement? Is foreign participation allowed (i.e., EU University, company, etc.)?
A6: Foreign participation is allowed to the extent security and other regulations allow for it. Consult the BAA and the RACE CUI Guide.

Q5: For TA1, should solutions include key exchange protocols or is it assumed that authentication/verification has already been established?
A5: Please see BAA for metrics re: public key infrastructure. Authentication/verification may be required for newly added RACE system nodes. Please see BAA for language on cryptographic work that TA1 researchers will be responsible for.

Q4: Regarding publication clearance, does this apply to academia subcontractors of industry labs? I.e., an academic writing a paper on his/her own, but being a sub-contractor in a project led by industry lab.
A4: It is anticipated that publications from universities (performing their work as a university/on campus) will not be subject to release review. However, if there are non-university, RACE-funded authors on the paper, they may be subject to release review if their contract contains such language.

Q3: Are the mobile clients expected to always be on? Or does the system need to support a store and forward approach?
A3: This is up to proposers, who should accommodate realistic scenarios (that they justify).

Q2: The intention for TA3.1 is to covertly retrieve/assemble from shards the covert app., but what app does the retrieval? If you can already do the covert retrieval, recreation, it seems redundant.
A2: The retrieval mechanism is up to TA3.1 proposers.

Q1: Are the class of functions computed in the MPC protocol general or is it purely to send/rec messages? Does TA1 need to provide verifiability of past msgs/computation b/w Alice & Bob?
A1: TA1 proposals are responsible for supporting RACE functionalities, as appropriate, to build the RACE system. Proposals should discuss what computations they plan to support (and why those are sufficient). Use reasonable assumptions and make sure they are discussed in the proposal.