2017-02-08

Swedish Foundation for Strategic Research

SSF Call for Proposals:

Framework Grants for Research on

Cybersecurity and Information Security

The Swedish Foundation for Strategic Research announces SEK 300 million in a national Call for problem-, challenge- or application-driven research projects that meet the highest international scientific standards. The Call aims to stimulate collaborative interdisciplinary research within the area of Cybersecurity and Information Security, of relevance to present or future Swedish-based industry and to society.

Selected projects will be supported by grants of SEK 4-7 million per year for a period of 5 years (incl. overheads) to be used for salaries (senior researchers, postdocs, PhD students, etc.), expensive equipment, and other research infrastructure research tools as well as running costs per the needs of the project. Funding for the last two years will be contingent upon a successful midterm evaluation.

Background

Modern society is undergoing a digitization transformation where virtual representations of “everything and everybody” are increasingly complementing the physical world, with support and guidance for most activities in life - professional and private. While this opens many new possibilities to further development of products and services, the high level of trust expected by society will require many challenging security and safety issues to be solved.

The lion’s share of the technological world is in the process of becoming connected, requiring large amounts of both software and more or less advanced terminals. As the Internet of (other) Things are now joining computers and mobiles on the net, security and safety become increasingly important. Power grids, vehicles, and medical devices are but a few examples of sophisticated technical systems, where qualities like robustness and reliability need to stretch into the digital realm. Furthermore, for consumer products offering digital services, e.g., in people’s homes, privacy, authenticity, and integrity are key connotations of security.

Traditional IT-systems have generally been “best-effort” designs, where liability sometimes have been eliminated through compulsory user agreements, which will not be sufficient for many future systems. There is a need for proactive and learning system

design methodology that can scale to the needs of the fully-developed digital society, where high quality software provides requested services, including security. Software and systems engineering will be needed to improve anomaly detection and mitigation of security vulnerabilities, in the design phase, and throughout the life-cycles.

Digital products are necessarily modular in construction, and increasingly combine software and hardware from different suppliers as standards become available to guide the design. The number of possible security issues, however, unfortunately scales with the number of interfaces between the modules.

For new application areas, like the Internet of Things and digital healthcare, the level of attained security will likely greatly influence their success in the market.

Swedish industry has a success record of producing systems and products meeting high-quality demands from customers. In the automobile sector, our industry is world leading in safety. The ongoing digital evolution, building on software-based networking that integrate hardware and software products in new kinds of systems and services, poses new challenges for both cybersecurity and safety. Being a considerable supplier of complex systems where digitalization is increasingly important, we need to assure a low number of security-related vulnerabilities in order to stay competitive.

This call is in concert with the Swedish Government Strategic Partnership Program on Connected Industry.

Scope

The Call addresses research aiming to increase network-related security in ways that are general or that will be useful in selected application areas. It has direct relevance for functional qualities in products like identity management, safety, and privacy and may also influence non-functional qualities, including, e.g., resilience and reliability.

The need for secure communication transcends all applications. Mobile communications present particular opportunities for improvements, e.g., improved provisioning of patches. The widespread adaption of cloud technologies and virtualized systems may also be areas of special attention.

Technological prowess may not suffice for success in markets or society. Insights from the field of human-computer interaction, or the social sciences more generally, including the judicial area, might back eventual breakthroughs. This means that co-applicants from disciplines outside of N, T or M are welcome.

Security is becoming increasingly important when it comes to the digitalization of large-scale systems. These include critical infrastructures like energy grids and communication networks, as well as all parts of the transportation sector, including the automotive industry, autonomous vehicles, logistics solutions, aeronautics, maritime and space transport. For many of these areas, safety is the overriding requirement that accentuates cybersecurity as a very critical concern.

Secure system design should be scalable, proactive, and self-learning, including authentication, self-diagnostics, and anomaly detection. Increasingly, critical activities depend on secure time and position data from the improving global positioning systems.

Mathematical tools can often find critical roles in security contexts, from intrusion detection to network analysis or applied cryptography. Use of open source cryptographic libraries are generally encouraged.

Cybersecurity pertains to industrial products and production processes. It must be an integral part of industrial control and product systems, and e.g., protect the increasingly important communication with or within the factory during the life-cycle of the product through development, sales, and after-market.

Cybersecurity is also the ultimate protector of the entire modern financial sector, where technologies like the block-chain may contribute to transforming previous modes of assurance. It is also needed in public administration, and to realizations of open government.

The successful development of smart cities – complete with smart buildings and smart infrastructure – will similarly depend on maintaining system security.

Certified systems in health care need to be brought to a higher level of life cycle security. Here, many additional challenges may require simultaneous attention, and accentuate the characteristic complexity exhibited in this sector, where patient safety and the treatment of personal health data take prime importance. While digitalization may offer many simplifications in diagnostics, treatments and interactions with patients, these will likely be accompanied by immediate increases in ambitions and demands, something that should reflect upon the choices of system architecture, protocols, standards, etc.

Successful proposals should generally be developed from a system perspective, and include systems-oriented research and/or components-oriented research. Proposals should also include development, disciplinary, and methodological research necessary for the project to achieve realistic system-level demonstrations beyond current state-of-the-art. Suitable choice of demonstrators should also be used to provide proof of concept.

Research priorities should be accompanied by one or more of the topics security, safety, privacy, and trust. The international context, for example manifested through standardisation, is also central, for the purpose of facilitating the implementation of the research and developments made in the project.

Fulfilling the above, application areas for strategic cybersecurity and information security research and innovation in this Call include, but are not limited, to:

- Smart grids
- Transportation
- Communication networks
- Smart Buildings and Smart Cities
- Industrial Control Systems
- Public Administration and Open Government
- Healthcare
- Finance and Insurance

Projects proposals must meet SSF's two main criteria: high scientific quality and relevance with a practical impact in application. New, innovative ideas are welcomed, and all applicants must also consider the conditions for upscaling in applications.

Strategic relevance

The proposed research shall aim to provide enabling technologies for future applications, products or services, or in solutions to important application problems.

The criterion of strategic relevance further means that the proposal shall demonstrate a clear vision of utilisation/exploitation of the research results in Sweden in the medium to long term. This includes providing effective measures for translation and innovation. It is recommended that the PI:s involve partners that can continuously support utilisation/ exploitation efforts of research results. Three percent of the grant will be reserved by SSF for such directed activities.

Another central part of the relevance is graduate student education and the attractiveness of the corresponding PhD:s in industry and society.

Eligibility

All projects should be based on a credible collaboration between, typically, two to four applicants with different kinds of relevant complementary scientific expertise. The applicants should be from one or different research group(s), not necessarily co-localised - and may be from different departments or universities for added interdisciplinary value. All applicants should take active part in the project and their activities should be at least partly financed by the project budget.

The proposal must be submitted by a main applicant who has the capacity to assume responsibility for the project during the entire grant period. The applicants must be employed by a Swedish university, university college, university hospital, or by a public or private non-profit research institute. At least one of the applicants must be employed by a university or university college.

While project participation from industry, public authorities or other relevant organisations is an evaluation criterion, such participants cannot be funded by the SSF grant, but may participate on their own budget. Although SSF-grants may not be transferred to universities outside Sweden, they may be used for, e.g., visits by foreign-based scientists to applicants working in Sweden.

The proposal budget should be in the interval of SEK 4 to 7 million per year for five years. A maximum of 25% of the grant may be used for salary for the main applicant and/or the co-applicants, but only to cover up to a maximum of 25% of the salary of each applicant. Junior participants (PhD students, postdocs or other junior researchers) may be funded by 100% of the salary. A maximum of 10% of the grant may be used for covering cost of expensive equipment and other research infrastructure.

Please note:

- each applicant is allowed to be represented in one application as a main applicant.
- each applicant is allowed to be represented in one application as a co-applicant.
- any one person is allowed to have maximum two framework grants simultaneously (with an overlap in time of up to three years) as a main applicant.

Applications not conforming to these conditions will not be considered. It is the responsibility of the main applicant to inform all the co-applicants and to check the proposal for compliance with the rules before submission.

Proposal and submission

A complete application must contain, among other data specified in the portal, a clear purpose statement, a full description of the research plan and full details of the relevant expertise of the participating groups. It should contain a clear account of the strategic significance of the research in the medium to long term, including a plan for utilisation/exploitation efforts that should commence in parallel with the research activities, already from day one in the project.

Each proposal shall clearly describe the state of the art within the area(s) addressed. It is also important for the proposal to give a clear picture of the resources available and to demonstrate that the proposed constellation of research groups will be effective in view of its objectives.

A Letter of Intent from the Head of the main applicant's department is compulsory.

The proposal must be written in English and submitted via the SSF portal at: http://apply.stratresearch.se. *Note that in order to get a complete view of all data required for submission it is necessary to consult the portal.* Please log on to the portal well in advance of the deadline. Please also submit the application in due time before the deadline. When the application is submitted, the system will reject it if some data field is missing. As long as this is done before the application deadline it is possible to submit and re-submit as many times as necessary.

All applications must be submitted by **14:00 hours (2:00 pm CET) on June 6, 2017**. No additional material will be considered after this deadline.

Evaluation

Applications will be assessed by an evaluation committee consisting of generalists and specialists from industry, academia, and research institutes. In a first selection, the applications will be judged primarily with regard to scope (as described above), relevance, and potential impact. Furthermore, applications that are judged unable to compete in the final step of the evaluation, or that are considered too incomplete to be meaningfully assessed, will not pass this first step. The selected applications will be sent on international peer review. The results of this expert review will be taken into account by the evaluation committee in order to produce a recommendation on which SSF will base its decision.

The applications will be reviewed using the following criteria:

- Conformity to the scope and eligibility as outlined above.
- Scientific quality; originality, strengths, weaknesses, degree of interdisciplinarity and feasibility of the research plan.
- Strategic relevance, with clear purpose and potential impact of the proposed research to Swedish industry and/or society, including explicitly formulated utilization/exploitation plans, with participation of industry or other branches of society in the project.
- Composition and gender balance of the research team. Qualifications of the applicants, previous achievements (science, innovation, and entrepreneurship), international experience and networks, and leadership/management of research teams.

Timetable

- Last date for applications: June 6, 14:00 CET at the latest
- Decision by the SSF Board: February 2018
- Project start: March 2018

No additional material submitted after deadline will be considered.

Please note that the Foundation is subject to the Principle of Public Access to Official Records (Offentlighetsprincipen). Thus, applicants should avoid submitting material that they do not wish to be made public, e.g., information that could prevent patenting.

Contact persons at SSF:

Olof Lindgren, Scientific Secretary, tel.: +46-8-505 81 669, e-mail: olof.lindgren@stratresearch.se

Joakim Amorim, Research Programmes Manager, tel.: +46-8-505 81 665, e-mail: joakim.amorim@stratresearch.se, tel. 08-505 81 665