Project Summary

Increasingly, the government agencies, commercial organizations and people of the United States depend on computer networks and systems. But it is becoming clear that the *availability* of these systems, the *integrity* of the data the systems maintain, and the *confidentiality* of the data are all imperiled by real threats. There are almost daily reports of attacks that result, among other losses, in many credit card numbers being stolen, of worms that cause severe loss of service, and of threats to individuals' privacy; many attacks are not reported. And, the threat is likely to become much worse, particularly when well-funded organizations become interested and skilled in attacking systems.

The security of the United States' systems is not materially improving despite the significant resources being directed to the problem through Government funding, commercial research, and many products and services aimed directly at improving security. There are intrinsic vulnerabilities in system designs and implementations that are exploited by attackers; systems are improperly misconfigured; and it is generally agreed that the complex systems in use today are simply too difficult to manage by a undermanned and not sufficiently skilled administrative staff. Furthermore, the situation will become exacerbated as the complexity of systems inevitably increases and as the frequency and severity of attacks also increases.

The research focus of the proposed Center for Computer Security Research (CCSR) will be the *fundamental science and technology needed to create and maintain the Nation's systems against the attacks of the future*. UC Davis has assembled a senior and experienced team of researchers to be the CCSR, including: research universities (Stanford, Colorado, Georgia Tech, Idaho), California teaching universities committed to security and network education (Sacramento, San Jose), a research institute (SRI International), and commercial organizations with long standing interest in computer security research and products (Symantec, NetSquared).

The *education focus* of CCSR will span the levels from middle school to PhD training, with the goal of making computer security an important and hands-on topic at all of these levels. The *broader impact* focus will be to produce the science needed for effective products and services in the face of the increasing threat to the security of the Nation's systems. The CCSR will produce prototypes that will be tested in a real world setting, and made available to researchers and commercial organizations.

Four important thrust areas will be drivers for CCSR:

(1) The realization of systems that can withstand a large-scale attack, such as a worm. Most of these attacks have been observed for "wired" networks, but threats against wireless and optical networks are also likely to occur. CCSR will produce a design methodology that works with existing (i.e., *legacy*) systems that are likely to contain vulnerabilities, as well as providing a basis for the design of systems which are less likely (but not guaranteed) to have vulnerabilities. The challenges, assuming vulnerabilities are present, are to predict the kinds of attacks that can arise given likely vulnerabilities: detect the presence of attacks; distribute reduced alerts throughout the network; decide on a response to stop an attack in progress, where the response must respect the policy associated with individual enterprises; recover components to a working state; and, even, remove vulnerabilities. A unified approach is required that makes use of models associated with all of these activities, which CCSR proposes to develop. CCSR will also develop methods to evaluate the effectiveness of a design in coping with attacks, using formal methods based on the models to be developed and experimental evaluation. The latter will entail the creation of testbeds, the synthesis of test data (both background/normal traffic and attack traffic), and new methods to test such designs safely on a live network.

(2) Detection and response to malicious insiders. For most organizations the insider threat has a greater impact than that from outsiders, although most of the current research is focused on outside attacks. CCSR's approach to the insider problem will focus on the aggregation of alerts from the parts of a system that can provide logs of activities, especially applications such as information systems. New approaches are needed to aggregate logs and also to identify what kinds of access are likely to be associated with insider misuse; the latter problem will involve data mining methods to accomplish policy discovery. As with thrust (1), response to misuse will also be studied, including the use of deception.

(3) Automation of security management. The current human-intensive practice to security administration is too error prone, too time consuming, and too unreliable to provide effective response to security incidents. CCSR will develop methods to provide human administrators with information needed to allow them to identify the presence, cause and possible responses to incidents. This thrust and thrust (1) clearly share a body of techniques but the emphasis for thrust (3) is on providing the information to a human administrator to enable him/her to make decisions that are appropriate to the enterprise being managed; the emphasis in thrust (1) is on automatic handling of attacks. CCSR will develop models of vulnerabilities, attacks, system components, all with the requirement that their instantiations provide a human administrator with accurate and timely information about the security state of the system. Information visualization methods will be developed to provide information about the state of very large systems in a form that is human understandable.

(4) Privacy enhancement. Sharing of sensitive information can be in conflict with users' preferences for privacy. The need to respect privacy is becoming very important, for example, in the widespread availability of medical records and other sensitive material. Models will be developed to allow users to express privacy requirements. In addition, CCSR will develop analytical methods to determine if a system design might violate such policy and on-line methods to determine if a policy is being evaluated in execution. Cryptographic techniques, specifically privacy-preserving protocols will also be developed.

These areas suggest applications that are representative of pressing security needs, are the subject of current research, are considered to be difficult and are currently far from being solved, and, most important, are best approached through a unified methodology rather than piecemeal. Consequently, the CCSR will develop a unified body of techniques that will apply to the variety of security applications associated with current systems and threats, but also with what is expected to be the technology of future systems and threats. The CCSR research agenda will include the research areas, with the goal being to develop a methodology that links the areas and provides the basis for guidelines on the synthesis of systems that use this methodology in the face of specific threats. In particular, the CCSR will develop models that relate to (a) vulnerabilities, (b) threats, (c) policy, (d) design paradigms, e.g., architectures in support of attack prevention, detection, and response, (e) recovery from incidents, (f) vulnerability removal. These models will provide formal descriptions in support of verification (for example to demonstrate that a response model does not act in a manner to deprive enterprises of resources needed to support services) and testing. For the latter, a testbed will be developed that will use attack models and traffic models to generate realistic test data.

By involving approximately 30 PhD students, the **education** program will address the need for educators with expertise in computer security. Through the broad research program, an extensive security curricula, covering the space between middle school and graduate school will be developed and distributed. CCSR's emphasis on experimental systems will produce systems that have the potential of being modified in a classroom setting to meet different needs and new threats. The testbeds CCSR will produce can be used to evaluate threats in a safe but realistic setting. At the middle and high school levels, where currently computer security is not addressed, CCSR will develop instructional material that introduces the topic and provides hands-on instruction on the threats and techniques these students can only currently observe through the media. CCSR will also create material to introduce students to the *ethical* demands attendant to computer security, emphasizing the importance of defenses against threats.

Technology transfer of the research and tools CCSR will develop will be achieved through numerous workshops and a website that is kept current. Through the commercial partners and advisory board, the real-world applicability of the research will be assured. Furthermore, it is the expectation of CCSR that the commercial partners will apply the research to commercial products that they might develop alone or in collaboration with other organizations.

The **intellectual merit** of the CCSR lies in the creation of a unified collection of models that can guide the development of secure systems and the validation of these systems through practical formal methods and testing in realistic settings. The **broader impact** lies in the education plan that provides real support in security education spanning the space between middle school and PhD production. Also, the CCSR will provide useful principles and working prototypes to the community of users; the transfer is through making the techniques and tools available, but also through the industrial partners who are eager to build products based on CCSR's principles and prototypes.