Association for Computing Machinery
US Public Policy Council (USACM)

usacm.acm.org
facebook.com/usacm
twitter.com/usacm

May 23, 2017

Statement on Computing and Network Security

Computing and network systems are integral to our economy and society, pushing forward technological progress, productivity, and innovation across the public and private sectors. Advances in computing and network capabilities bring substantial benefits in efficiency, convenience, and performance for individuals, organizations, and society. Applications, services, and infrastructure depend on the reliability and security of these systems.

What allows society to reap the benefits of computing and interconnectivity also opens the digital ecosystem to potential adverse consequences. These can result from unanticipated events and interactions, or deliberate attacks, with consequences that range from inconvenient to devastating. The significance of these consequences raises the stakes for the security of computing and network systems.

The following set of principles is intended to elaborate essential qualities for secure computational environments, based on sound scientific and technical foundations. While the complexity and rapid evolution of computational environments – including infrastructures, devices, applications, and information – will continue to present new and unanticipated challenges, these broad principles provide a strong basis for security.

1. **Trustworthiness:** Computing and network systems should be worthy of trust. Trustworthiness entails the safety, security, reliability, dependability, performance, and survivability of the system.

2. **Integrity:** Technical, physical, and administrative mechanisms should be available to protect against information manipulation that alters or masks the intended use.

3. **Confidentiality:** Technical, physical, and administrative mechanisms should be available to safeguard access to and distribution of protected information. Access to protected information should be limited to authorized entities and users.

4. **Availability:** Technical, physical, and administrative mechanisms should be available to ensure that information and resources are usable and accessible to authorized entities and users.

5. **Manageability:** Computing and network systems should be responsive to configuration and patching by intended users without impacting functionality, safety, or security**.**

6. **Transparency:** Device, software, and service vendors are encouraged to disclose to their consumers the information needed to effectively manage personal, organizational, and societal risks.

7. **Accountability:** Entities should be held accountable for the information they manage and process and for providing appropriate security protections for that information.

ACM US Public Policy Council
1701 Pennsylvania Ave NW, Suite 300
Washington, DC 20006

+1-202-355-1291 x13040
acmpo@acm.org
usacm.acm.org

8. **Holism:** A layered approach to the ubiquitous computing and network infrastructure should address systems architecture, hardware, operating systems, communications and application software, and other components that comprise user environments.

9. **Requirements based:** Establishment of an explicit statement of goals, derivative requirements, and the processes needed to fulfill them is critical to security planning and operation. Ongoing risk management programs that identify risks, and assess and respond to system vulnerabilities using accepted and known frameworks and standards, are essential building blocks of secure systems.