New NIST guidelines aim to help IT system developers build security in from the ground up

May 22 2014

A new initiative by computer security experts at the National Institute of Standards and Technology (NIST) seeks to bring widely recognized systems and software engineering principles to bear on the problem of information system security.

The goal, according to computer scientist Ron Ross, a NIST Fellow, is to help establish processes that build security into IT systems from the beginning using sound design principles, rather than trying to tack it on at the end. "We need to have the same confidence in the trustworthiness of our IT products and systems that we have in the bridges we drive across or the airplanes we fly in," says Ross.

Civil engineers employ the principles of physics and engineering to build reliable structures, Ross says. Similarly, systems security engineering processes, supported by the fields of mathematics, computer science and systems/software engineering, can provide the discipline and structure needed to produce IT components and systems that enjoy the same level of trust and confidence.

NIST has launched a four-stage process to develop detailed guidelines for "systems security engineering," adapting a set of widely used international standards for systems and software engineering* to the specific needs of security engineering. The agency has released the first set of those guidelines for public comment in a new draft document, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems.**

The NIST engineering-driven guidelines are meant to be broadly applicable to systems design in both the public and private sectors, for small and large systems, and for many different types of applications including general-purpose financial systems, defense systems and the industrial control systems used in power plants and manufacturing.

The current draft—and the first stage of the planned process—describes the fundamentals of systems security engineering, elements and concepts and covers 11 core technical processes in systems and software development. Later public drafts will add material in supporting appendices, for example, on principles of security, trustworthiness and system resilience; use case scenarios; and important nontechnical processes such as risk management and quality control procedures. NIST expects to publish the final, complete version of the engineering guidelines by December 2014.

More information: The initial public draft of Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems is available at csrc.nist.gov/publications/PubsDrafts.html#800-160 . Public comments on the current draft are requested by July 11, 2014, and should be sent to sec-cert@nist.gov.

*International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronic Engineers (IEEE) standard 15288:2008, Systems and software engineering—System life cycle processes.

**R. Ross, J.C. Oren and M. McEvilley. Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems.

NIST Special Publication 800-160. Initial Public Draft. May 2014.

Provided by National Institute of Standards and Technology

Citation: New NIST guidelines aim to help IT system developers build security in from the ground up (2014, May 22) retrieved 12 May 2024 from https://phys.org/news/2014-05-nist-guidelines-aim-ground.html