

Security Properties, Vulnerabilities and Sanitization

A security policy defines "security" for a system or site. The policy consists of a set of security-related properties that the system must satisfy. This talk explores two uses of security properties in the protection of computer systems.

"Formal methods" is the name of a set of techniques used to design and implement high-assurance systems. Its hallmark is the derivation of design from specifications describing the properties that the system is to meet. Unfortunately, modern systems in widespread use are not built using these methods. The result is a very low degree of assurance with respect to security. Attackers can break into these systems with little difficulty.

The first part of this talk applies elements of formal methods to existing systems in order to make the systems more resistant to attacks. One can characterize vulnerabilities in terms of basic properties. From these properties, techniques can be developed to analyze systems for previously unknown vulnerabilities. This talk will discuss the relationship between this approach and formal methods, as well as previous vulnerability classification schemes.

A related question is how to provide vulnerability information to analysts without compromising the privacy of users on the system. The analysts need to examine logs, network data, and other information to determine if an attack occurred and, if so, what vulnerabilities were exploited. The second part of this talk discusses using security properties underlying the analysis as a basis for sanitizing the data given to the analysts.