New Tool Improves Development of Secure Software

George Lawton

A research team has developed a natural language processing (NLP) tool designed to allow security policies to be automatically incorporated into the software-development process.

This would eliminate developers' current practice of trying to interpret natural-language descriptions of security policies, which can lead to inaccurate implementations.

Research scientists from North Carolina State University (NCSU), the US National Institute of Standards and Technology (NIST), and IBM designed the new Access Control Policy Tool (http://csrc.nist.gov/groups/SNS/acpt/index.html).

ACPT translates written access-control policy (ACP) requirements into a machine-readable database of policies that determine which users are permitted to see datasets within an organization's information system.

ACPs

ACPs can take many forms. For example, a university might specify that professors could access and change all grades from their classes but that students could look only at their own.

Today, a company manager, business developer, or other user writes ACP specifications in plain text and includes them with other details related to new software's desired functionality. The developer then programs the application accordingly.

Within a system, said NIST computer scientist Vincent Hu, "The policy-enforcement engine can be any system mechanism such as hardware, software, or language that is dedicated to enforcing machine-readable ACPs. Most operating systems of computing devices provide default policy-enforcement subsystems."

However, incomplete, inaccurate, or misinterpreted ACP requirements could lead to problems such as systems improperly keeping authorized users from accessing data or letting unauthorized users access restricted information, said NCSU associate professor Tao Xie.

ACPT

The ACPT uses NLP techniques to automatically translate text describing access-control requirements into a consistent, concise, machine-readable format that makes understanding the intended requirements easier for programmers, as Figure 3 shows.

Someone from an organization would start the ACPT process by feeding the text from a software specification into the tool.

The application uses NLP techniques such as shallow parsing, which identifies the parts of speech in text but does not try to understand their meaning. It combines this with semantic-pattern parsing, which analyzes the definitions of and relationships among words to determine meaning.

These techniques extract context to be used in generating machine-readable

ACPs, said NSCU doctoral candidate Xusheng Xiao. Programming teams then use this information to design ACP-compliant software.

Once the developers have incorporated software into a working system, compliance specialists use known business or operational access cases to test whether the application complies with all requested ACPs, said NIST's Hu.

The researchers are working on extending ACPT to support automated testing.

They noted that developing NLP tools can be difficult but that their work was easier because ACP requirements in software documents usually follow a certain style and use a limited number of terms.

Looking Ahead

ACPT does not guarantee that no access-control problems will occur.

NCSU doctoral candidate JeeHyun Hwang explained, "Extracting an ACP from a natural language document cannot guarantee complete accuracy of the ACP unless the natural language policy described in the document is semantically accurate, which is hard to prove. However, such extraction minimizes human errors when translating the natural language document to a machine-executable ACP."

"Currently," said Hu, "ACPT is in the beta-testing stage and we are collecting feedback." When the tool passes beta testing, he noted, it will be made available to the public for free, probably next year.

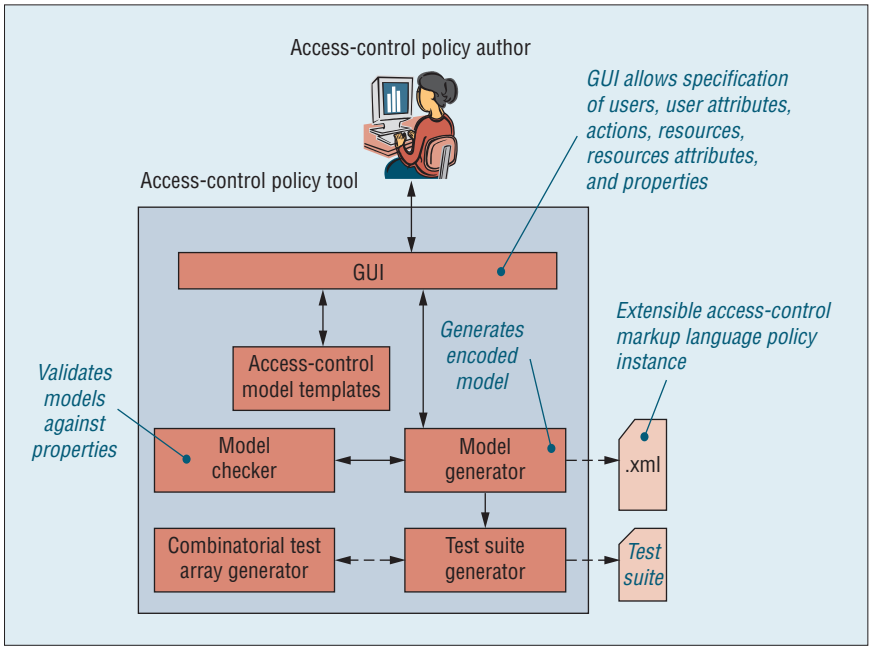

Figure 3. A research team has developed the new Access Control Policy Tool, which allows security policies to be automatically incorporated into the software-development process. ACPT automatically translates natural language text describing access-control requirements into a consistent, concise, machine-readable format. Developers would no longer have to try to interpret the text and apply the policies themselves, which can lead to inaccurate implementations. (Figure courtesy of the US National Institute of Standards and Technology)

Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.