been to parameterize things in different domains.”

Currently, the application serves results in a single stream. But the Chadwick team is considering changing this so that users could receive updates from different types of sources—such as blog writers or professional reporters—in separate streams.

The Business Side
For now, Yakovenko said, his main interest is refining Chadwick and attracting users by not charging them to work with the application initially.

In the long run, he said, there is an opportunity to generate revenue using branded Chadwick portals and licensing commercial versions of the application. For example, a sporting-goods business might offer a portal that covers a local team to promote sales of the store’s products.

Sergei Burkov, cofounder of Google Moscow and an Internet entrepreneur, said he invested in Chadwick because it addresses an interesting technical problem and focuses on a narrow domain—basketball—which makes obtaining good results easier.

Once the basic engine has been refined, Burkov said, there will be plenty of opportunities to make money by licensing it to various companies.

He explained, “From a business perspective, sports is one of the most popular pastimes. Quite often, people are not in front of TV sets and want updates while driving or at work. This is the solution to that real problem.”

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’ 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.

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.”
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)