Number 76, January 2009

ERCIM NEWS

European Research Consortium
for Informatics and Mathematics
www.ercim.org

Special theme:

THE SENSOR WEB

Also in this issue:

television to my favourite show when I sit on the couch"; ie depending on the weight measured by a sensor in the seat, and the time of day, different TV shows will appear on the screen.

In stream applications, we need mechanisms to support long-standing queries over data that is continuously updated from the environment. This requirement is significantly different from what happens in a traditional database system, where data are stored in static tables and users fire one-time queries to be evaluated over the existing data. Given this critical difference, the pioneering architects of the data stream management system naturally considered existing database architectures inadequate to achieve the desired performance: instead they designed new architectures from scratch.

However, working from scratch makes it difficult to exploit the existing knowledge and techniques of relational databases. This disadvantage became more pronounced as the stream applications demanded more functionality. In DataCell therefore, we started at the other end of the spectrum, building an efficient data stream management system on top of an extensible database kernel. With careful design, this allows us to reuse the sophisticated algorithms and techniques of traditional databases. We can provide support for any kind of complex functionality without having to reinvent solutions and algorithms for problems and cases for which a rich database literature already exists. Furthermore, it allows for more flexible and efficient query processing by allowing batch processing of stream tuples, as well as non-consecutive processing by selectively picking the tuples to process.

The idea is that when stream tuples arrive in the system, they are immediately stored in (appended to) a new kind of table called a basket. By collecting tuples into baskets, we can evaluate the continuous queries (which are already submitted to the system and are waiting for future incoming data) over related baskets as if they were normal one-time queries. This allows us to reuse any kind of algorithm and optimization designed for a modern database system. Each query has at least one input and one output basket. It continuously reads data from the input baskets, processes this data and creates a result which it then places in its output baskets. Once a tuple has been seen by all relevant queries, it is dropped from its basket.

This description of the process is somewhat simplified, since this process allows the exploration of quite flexible strategies. For example, the same tuple may be thrown into multiple baskets where multiple queries are waiting, query plans may be split into parts, and baskets may be shared between similar operators (or groups of operators) of different queries, allowing results to be reused.

The periphery of a sensor stream engine is formed by adapters, eg software components to interact with devices, RSS feeds and SOAP Web services. The communication protocols range from simple messages to complex XML documents transported using either UDP or TCP/IP. The adapters for the DataCell consist of receptors and emitters. A receptor is a separate thread that continuously picks up incoming events from a communication channel and forwards them to the DataCell kernel for processing. Likewise, an emitter is a separate thread that picks up events prepared by the DataCell kernel and delivers them to interested clients, ie those that have subscribed to a query result.

We designed and developed the DataCell at CWI in Amsterdam, funded by the BRICKS project. It is implemented on top of the MonetDB, an open-source column-oriented database system. Currently it is a research prototype and the goal is to be able to disseminate the DataCell soon as part of MonetDB.

Link:
http://monetdb.cwi.nl/

Please contact:
Erietta Liarou
CWI, The Netherlands
Tel: +31 20 59 24 127
E-mail: erietta@cwi.nl

Martin Kersten
CWI, The Netherlands
Tel: +31 20 59 24 066
E-mail: mk@cwi.nl

On looking FORWARD

by Sotiris Ioannidis, Evangelos Markatos and Christopher Kruegel

Computer systems, networks and Internet users are under constant threat from cyber attacks. FORWARD is an initiative by the European Commission to promote collaboration and partnership between academia and industry in their common goal of protecting Information and Communication Technology infrastructures.

The past few years have been marked by an ever-increasing number of cyber attacks. Motivated by fun, fame and peer recognition, early attackers, more widely known as 'hackers', pioneered the methods used to penetrate computers, compromise accounts and invade our personal lives. Even though these early hackers usually meant no harm, their methods and techniques perfected the necessary technology required to compromise remote computers. In turn, this paved the way for professional criminals motivated by profit to start using compromised computers for a wide variety of illegal activities, such as trading of credit card numbers, online renting of compromised computers, online ordering and delivering of denial-of-service attacks, and sending spam email messages. To reduce the effects of these cyber attacks, security researchers are engaged in an arms race against the ever-increasing sophistication of cyber attackers, by creating systems that detect, and whenever possible mitigate, the effects of these attacks.

To stay ahead in this arms race, FORWARD brings together European

researchers in network and information systems security to identify (i) the most probable security threats in the near future, and (ii) those research areas that must be pursued to address and mitigate these emerging threats. By mobilizing a critical mass of researchers in Europe and by complementing them with a select team of researchers from Asia and America, FORWARD is working towards establishing a research agenda for cyber security in Europe and identifying possible new areas and threats that must be addressed. FORWARD researchers have focused their activities on three critical domains:

- Malware and Fraud: malware is perhaps the one arena in which attackers have clearly demonstrated an increased sophistication. In its race to evade antivirus signatures and systems and stay below the detection 'radar', malware has evolved to be agile, stealthy and highly sophisticated.
- Smart Environments: the increasing miniaturization of computing systems is driving the penetration of intelligent appliances in every human activity. As computing and communicating devices become increasingly widespread, so does the potential of attackers to disrupt our daily lives in a wide variety of ways.
- Critical Systems: Our daily functions, if not our lives, depend on a wide variety of traditional and emerging infrastructures, such as the power grid and communications networks. As it becomes more common to connect critical infrastructures to the Internet using off-the-shelf technologies, the vulnerability of these utilities increases to breaches and attacks from the outside world.

By mobilizing cyber security researchers in Europe and by consolidating their efforts along those major research axes, FORWARD will identify those research directions that will help lead to a safer and more secure cyberspace for all European citizens.

For more information about the activities of FORWARD or if you are interested in participating, please contact Christopher Kruegel or visit our Web site.

Link:
http://www.ict-forward.eu

Please contact:
Christopher Kruegel
Vienna University of Technology, Austria
E-mail: chris@seclab.tuwien.ac.at

Sotiris Ioannidis
FORTH-ICS, Greece
Tel: +30 2810391945
E-mail: sotiris@ics.forth.gr

Enhancing Authentication in eBanking with NFC-Enabled Mobile Phones

by Diego A. Ortiz-Yepes

In the past few months, a mobile phone-based authentication mechanism for eBanking has been developed at the IBM Zurich Research Laboratory. At the core of this mechanism, we have used NFC and CAP. The latter, Chip Authentication Program (CAP), is a specification developed by MasterCard that provides mechanisms for customer authentication based on smart cards compliant with EMV (Europay - MasterCard - Visa). The former, Near-Field Communication (NFC), is an emerging technology related to RFID that is already being incorporated into commercially available mobile phones, allowing them to communicate over very short distances (in the order of a few centimetres) with other NFC-enabled devices. This ability, when employed in tandem with CAP — as we have done in our authentication mechanism — greatly enhances the overall usability of the authentication system.

Our NFC-based authentication mechanism relies on dual-interface smart cards, that is, cards with both contact and contactless interfaces. These cards might also be used for other financially related purposes, eg as debit or credit cards. In fact, this situation is desirable in order to avoid burdening the customer with an additional card for eBanking purposes.

The customer authentication mechanism works by having the customer produce an appropriate response to an unpredictable challenge generated by the bank. In order to do so, she must use her card and its PIN, which is used to authenticate the customer to the card. More precisely, when the customer wishes to engage in eBanking, she visits the Internet site of her bank, which requests her customer ID, eg her account or contract number. Once such an ID has been received by the bank, it replies with a challenge, which consists of an unpredictable number of between 6 and 8 digits. Having received this challenge, the customer starts the phone application by touching her bank card to the back of the phone (see Figure 1). She then selects the log-in mode and types in the server-issued challenge. Prior to generating the corresponding response, the phone requests that the customer provide her PIN in order to authenticate herself to the card. Once the customer has been authenticated by the card, the phone sends the challenge to the card obtaining a cryptogram in return. Using this cryptogram – a bit-string cryptographically bound to the challenge and the internal card state – the phone generates a numeric code, ie the response, which is displayed to the customer. Subsequently, she sends the response to the bank server by typing it into the PC. When the response is received by the bank, the latter checks whether it corresponds to the previously issued challenge. If this is the case, the bank presents the customer with her account(s) summary, as well as some appropriate transaction options.

The mechanism outlined above replaces the Personal Card Reader (PCR) required by some authentication schemes currently in use, yielding a