Technology, T-14-9804
D. Wiggins

Research Note
9 January 2002

Big Brother — Real-Time Behavioral Monitoring

A new form of carrier-class behavioral-pattern monitoring has emerged that is capable of monitoring an individual or even an entire country across all communication platforms and protocols, from Web to wireless.

Core Topic
Security and Privacy: Security Tools, Technologies and Tactics

Key Issue
What new vulnerabilities will arise through the deployment of emerging technologies and products?

Israel-based Xacct Technologies has won numerous awards during the last three years for its intelligent business infrastructure platform and data gathering technologies. For example, Red Herring has named it one of the "Top 50 Companies Most Likely to Change the World."

A closer look at Xacct's technology reveals some startling implications and opportunities for abuse. Promoted as a comprehensive, real-time data collection, correlation, aggregation and account provisioning solution, Xacct's technology uses "smart agents" to record information and transmit data to a central event manager, storing the usage data in a commercial database. Direct access to servers is not required, and Xacct claims that more data often can be gathered by interrogating traffic near the device than what the device itself provides.

Data is captured from all seven layers (physical to applications) of the Open Systems Interconnect Protocol stack. The type of data that can be recorded goes well beyond that collected by other systems, such as the FBI's Carnivore e-mail monitoring technology, to the point where virtually every type of communication can be recorded. Xacct uses its proprietary Net-Stream Recognition Technology, which supports the monitoring of more than 750 protocols and 3,000 attribute combinations. Protocols such as HTTP, FTP, NNTP, H.323 (network conferencing standard for voice and video), SMTP and others are monitored from devices such as switches, routers, Web servers, voice over IP gateways, application servers and even wireless networks such as general packet radio service (GPRS), Code Division Multiple Access, WAP and the Universal Mobile Telecommunications System (UMTS) to obtain traffic and application data.

Xacct's carrier-class technology is deployed as a business infrastructure solution that provides multisource, multilayer data collection, as a convergent software platform that captures and transforms raw network data, such as that from GPRS, UMTS and IP networks, into actionable business and intelligence information. Because protocols such as GPRS are always on, it's possible for a carrier to offer information back to a user based on his or her location and previous behavior. Going a step farther, Xacct can collect and process this data in real time, combining behavioral events with positional events. With the upcoming penetration of third-generation wireless standards, this presents some interesting legal perspectives as to how the information should or should not be used.

Xacct has more than 70 customers worldwide, including Bell Canada, Boeing, BT Group, Cable & Wireless, Motorola, Siemens, NTT/Verio and Korea Telecom. It has been working with hardware vendors such as Siemens, Cisco Systems, Compaq Computer and Sun Microsystems to enable its facilities directly at the hardware level. Many of these companies have access not just to usage pattern data, but also to specific user information. By associating this information with usage and behavioral data, an enormous amount of information can be extracted.

In November 2001, the FBI sent a 32-page document to U.S. telecom companies requesting that changes be made to land-based and wireless networks that would enable the FBI to monitor IP-based technologies well beyond what its controversial Carnivore can accomplish. Although this request was already being formulated prior to the Sept. 11 terrorist attacks, the new U.S. Patriot Act gives the FBI much broader powers than the 1994 Communications Assistance to Law Enforcement legislation, under which the request to the carriers was made.

Irrespective of the complex legal, moral and privacy issues surrounding such monitoring, it's clear that carriers technically can perform monitoring at this level, whether for customer relationship management, billing or security purposes. In the United States, a court order is required to monitor a U.S. citizen; for non-U.S. citizens and monitoring outside of the United States, such restrictions do not apply. Because a large amount of global Internet traffic travels through the United States, it's possible for Xacct's technology and others like it to monitor real-time patterns of traffic from other countries, raising alerts and focusing attention on specific communications from those countries.

Xacct has confirmed that while security is not its primary market, it can leverage thousands of man-years of experience in building communications and intelligence networks to enable any carrier

or major Internet hub such as MAE East to offer real-time intrusion alerts and to identify potential risks via pattern recognition and data gathering. When asked if Xacct's technology could help carriers to provide the type of data that the FBI has requested, Xacct's vice president of technology, Eran Wagner, stated that "We provide them with a weapon; they could abuse the use of the weapon, but it's up to them."

Bottom Line: Although national security is presently at the forefront of many governments' agendas, it must not compromise the privacy of individuals, enterprises or countries. Governments must ensure that putting such monitoring as Xacct's technology in place does not enable the abuse of this monitoring. As a caution and irrespective of platform, protocol or device, no one should assume that his or her communications are private unless they are highly encrypted.