

Security Alchemy

For several centuries, alchemists searched for the Philosopher's Stone—the elusive substance that could transmute common lead into gold. Alchemy flourished between the Dark Ages and the Renaissance, when there was enough motivation to pose the challenge but not enough

knowledge to solve it definitively.

Over the past 50 years, a new kind of alchemy has emerged. Its Philosopher's Stone is the computing technology that can transmute ordinary individuals into singular experts in a specific domain. Calling this new technology “stoneware” conveys its gravitas and lines up with software, hardware, middleware, vaporware, and all the other “wares” floating around these days.

An early form of stoneware was the expert system, which is built by codifying rules that human experts use to ask questions, make decisions, reach conclusions, and ultimately effect actions in a given domain. This presupposes the existence of experts in the domain and their ability to articulate explicitly the knowledge and rules that make them such.

Explicitly articulating knowledge and rules sounds simple—but as many of you know, it's not. Codifying the rules of arithmetic, a very well-defined and restricted domain, is clearly possible in spite of the difficulty that many have with long division and fractions. However, there are several domains in which we find experts but little success with the associated stoneware.

A case in point is the current DARPA Grand Challenge (see www.darpa.mil/grandchallenge/), which

requires building an autonomous vehicle that can self-navigate over a route that winds through various terrains passable by consumer-grade 4 × 4 trucks. The 2004 competition ended in disappointment for all entries—the best showing completed a scant seven miles of the 142-mile course, and only seven of the 15 teams made it farther than one mile. What's humbling about DARPA's Grand Challenge is that most of us can drive a 4 × 4 vehicle through a complex course.

Candidate stonewares that deal specifically with such cognition and control are artificial neural networks and related machine-learning ideas. Those technologies can solve non-trivial problems if the underlying systems have enough data to learn suitable categories, labels, or actions. In a way, they go beyond the promises of expert system stoneware by offering the possibility of totally automating classification and response without any human intervention.

The problem is that getting enough data can often be difficult and, even then, the learned responses work only in environments that are virtually identical to the one that produced the training data. As environments change over time, they create situations that are very difficult for machine-learning methods to handle correctly—because the data that describes those situ-

ations hasn't been seen before.

Successful stoneware for computer and network security would relieve a lot of headaches, but it's clearly neither easy nor imminent. In this context, Bruce Schneier wrote “the key to security is people, not products” (Clear Text, *IEEE Security & Privacy*, Sept./Oct. 2004, p. 88). What I've written so far is essentially in agreement with Schneier's sentiment, and in fact argues that it's a hard slog across not just security but many different application areas. However, there are significant problems with the people solution as well.

First, there aren't enough security experts to go around. A check of Monster.com's listings with keywords “computer” and “security” yields more than 5,000 hits—more than “Java” and “programming.” Another difficulty with the people solution—regardless of whether it's in-house or outsourced—is that security experts respond to events reactively. That is, someone, somewhere has to take a hit first for the response to kick in. People just aren't fast enough to respond before some damage is already done.

It's a “damned if you do, damned if you don't” situation in this age of security alchemy. Right now, we have no security stoneware, so we need people to staff consoles and read log files using technology that can amplify and empower them. On the other hand, we cannot abandon the quest for automated analyses and responses. To do so would sentence us to a purgatory of perpetual expense and compromise—something that I, for one, am not yet ready to accept. □



GEORGE
CYBENKO
Editor in Chief