TimesPeople

EE brings chaos to secure-server quest

By Bernard Cole

As printed in Electronic Engineering Times, October 21, 2002 and at iApplianceWeb.com

To hear Eric "Doc" Uner tell it, he owes his position as co-founder and chief software architect at secure-server maker Bodacion Technologies Inc. to his lifelong affinity for challenges that make him feel miserable and stupid.

He says he has been willing to take on some difficult jobs simply because the problem set or the methodology has fascinated him. But he also acknowledges the rush "when you solve a difficult problem or take an advanced mathematics course and finally get it, with all the pieces falling into place."

That compulsion led him to pursue two areas of intellectual fascination-embedded design and chaos theory-that seem diametrically opposed but that have dovetailed nicely in the secure servers his Barrington, Ill., company sells and the services it provides.

In embedded design, the fascination for him is that seemingly intractable problems resolve themselves once you define the problem properly, identify the sources of error or instability and eliminate those sources. His interest in chaos theory was spawned by his weakness for college math courses that were "GPA killers."

Uner relates that he had finally mastered a brain-bruising math course and was scouting for another to make him "feel really miserable." A professor handed him a complex problem and challenged him to solve it.

"He told me to take a new course he was teaching if I wanted to know how to remove the complexity and get to the core of the problem quickly," Uner said. "That was my introduction to chaos theory, and I have been hooked ever since."

But for most of his professional life, electrical engineering has been his staple-in particular the experience that he garnered at Motorola working on embedded networking and systems. "We were operating in an environment as it related to quality and reliability that was totally unlike the real world," Uner said. "We were protected in our choice of tools, building blocks and methods by the company's six-sigma program."

When he left Motorola in 1995 to go it alone, he started out as a contract developer on embedded projects across a broad range of markets, including military and government contracts. Eventually, said Uner, much of the business involved building server systems that had a greater degree of reliability than most commercial offerings.

To address security requirements, Uner applied the full range of embedded tools to similar problems in servers. "Just because a particular tool or feature was designed for one thing does not mean that it cannot be re-purposed or adapted for another," said Uner.

At the same time, his company began running their own Web hosting service, built using the reliability techniques learned at Motorola. That's where they ran headlong into the problem of security.

"We were getting tired of getting out of bed at 2 a.m. to deal with a constant stream of hacker attacks and security break-ins," said Uner. So were many of their customers, many of whom came from the military/aerospace industry. "We found that traditional techniques for securing operating systems would not work - nor would any of the new technologies emerging for security if the core OS was inadequate to the job, " he said.

The solution that Uner, and his team of developers came up with brought together their expertise in embedded systems and Uner's fascination with chaos theory. it not only solved their immediate security problems with their Web sever but also spawned a commercial product, the HYDRA, and transformed the company into a provider of secure servers to the federal government, military and commercial sectors.

Their solution was conceptually simple but complex to implement. They decided to do what a landlord might do when a tenant leaves: change the locks.

The problem in a sever is that there is not just one lock, not one key and not one door. Instead, there are hundreds or thousands, and for each the process has to be repeated at three levels. At the application layer, it is necessary to create secure digital signatures, customer ID's and order numbers. At the presentation layer, to protect the ciphers used by Web browsers, it is necessary to use data perturbation techniques to distort the keyword data just enough to guard against hacking without rendering it unusable. And at the session layer, it is necessary to identify a user across multiple connections.

Further, to make these systems truly hacker-proof, Uner and his co-workers thought the keys and the doors had to be changed not just occasionally, according to some predictable schedule, but randomly, each time a transaction occurred, across all doors and keys in, say, the application-layer neighborhood.

"It was also important to do this dynamically and in the background so as not to disrupt the normal operation of the server," said Uner. The only OS's capable of the deterministic and real-time operations necessary were some of the more mature RTOSes.

"The so-called random-number generators that are the staple of most computer designs are not really random-a weakness that hackers exploit fully, " said Uner.

Enter chaos theory. Uner realized chaos theory might be applied to create truly randomized sequences that for all practical purposes would be unbreakable. The solution he and his co-workers have come up with is still proprietary but has been demonstrated in the HYDRA commercialization to a variety of governmental and military organizations and commercial companies.

Uner says his company's claim of a virtually crack-proof server system has been validated by both government agencies and commercial entities in the demonstration orchestrated by the National Security Agency's SPOCK program, a government-industry consortium that investigates and tests commercial and government products that support dependable security architectures.