

## Innovation for Innovators

Roger Smith

### Computing Beyond the Firewall

The protagonist in Vernor Vinge's 1981 short story "True Names" uses a global communication net to hack into civilian and defense networks, gain control over thousands of computers, and turn them into zombie machines to support his attack on government information stores. "True Names" is about espionage and sabotage on the global information grid, but Vinge's real prescience lies in the story's central assumption—in 1981—that "the network" would become critical to business and government operations and that it would be poorly protected from an intelligent attack (1).

Thirty years later, we face a regular stream of internet attacks like the most recent in which two virus programs worked together to extract personal, competitive, and financial data from corporate computers. On February 18, 2010 news agencies reported an attack in which the Kneber botnet used the well known ZeuS Trojan Horse to deliver itself to thousands of computers and proceeded to use these machines to collect information and spread itself to other computers. The initial estimate is that this attack yielded 68,000 data records from 2,500 different corporate networks (2). In spite of the best efforts of corporate IT managers, information security consultants, firewall engineers, and encryption specialists; criminals and state-actors continually find ways to take the information they want. This is a natural consequence of putting computers on a global network. Machines on a network are extensions of that network. The technologies that tie together the insides of a stand-alone computer are not that different from those that extend it into the global network. So it should be no surprise that remote pieces of a networked computer can interfere with the operations of our personal or corporate machines.

The dividing line between private computer, private network, and public internet is fading fast. The shift toward a globally distributed and openly accessible computer grid has been underway for years. It has grown so subtly that we have taken the early manifestations for granted. We have reached a point where most of the work we do is dependent upon and distributed between multiple users and organizations. We are already operating as part of a large network that is intentionally open to group members from various organizations as determined by the work we are sharing. We access data from the internet and corporate networks and share all of our own work via these networks. We have all become nodes in a very large Open IT infrastructure that is not clearly defined or protected.

The world of Open IT has begun. It is being executed every day by thousands or millions of employees who are just trying to get their work done as efficiently as possible. Hundreds of services to help them do this are quickly and easily available. No corporate

IT policy or firewall can stop this proliferation of data without also crippling the operations of the company.

This may have begun in the 1990s, when computers and networks became powerful enough to allow employees to telecommute. Companies created virtual teams whose members resided around the country or around the globe, coming together only through the exchange of electronic data. Enabling such distributed work required trusting all of the computers and networks with some portion of the corporate data necessary for the work to get done. IT managers may have installed encryption software and virtual private networks to assure everyone that the data was secure, but the extension of the corporate network through the open internet and into employees' privately owned machines meant that the system was open to intrusion from other users of that same network. The boundary between corporate, public, and private information devices had been taken down and the resulting open system offered an attractive target to those who saw the value of stealing information or disrupting its free exchange. Mobile communication and mobile computation opens this door even further.

How is this migration to Open IT happening and why is it necessary? Increasingly, no company can provide all of the tools that can be found on the internet and no company can survive without access to those tools. Ask yourself a few very practical questions about where you get the information services necessary to do your job.

- Where do you get the maps and directions that you use to drive to a meeting across town? MapQuest?
- How do you share documents with partners in your own and other companies? Google Docs?
- Where do you store customer contact information? Salesforce.com?
- How do you access the most current world news? NYT Online?

In each of these cases, you are using a service created for easy access to anyone that wants it. The service is generally not contracted specifically and securely by the corporation, but rather is selected for its convenience and usefulness by each employee. What is the result? Is your corporate customer list stored at Salesforce.com or LinkedIn? Do your confidential collaborative documents reside in Google Docs? Is corporate data being analyzed on servers owned by Amazon or another cloud-based provider? In most cases, the decision to do any of these is in the hands of each individual employee, not an all-powerful IT czar. Each employee usually has the power to use these services from their personal computer or their corporate computer.

Open IT in which data and computation is distributed all over the Internet is the logical end-state of these kinds of operations. This trend will only continue to grow as our need for services and our reliance on networked operations increases. If this is inevitable, we must determine how it can be carried out securely and with some level of trust? In his 2008 novel *Halting State* Charles Stross's characters wrestle with a global network in which all data from banking to government has been subdivided, encrypted, and distributed to be hosted and computed on machines everywhere on the internet. Security

is based on the theory that it is impossible for any attacker to identify the location of any single important piece of data, pull together thousands of small pieces, and break the unique encryption on each of them. In this story, there is no central data server that belongs to a single company. The entire internet is the data center for every organization and it is protected by fracturing valuable data into small pieces, distributing them anonymously, and wrapping them in trusted encryption. All business and personal operations are protected and executed in this ultimate Open IT environment, and everyone in the world trusts this system based on the encryption, distribution, and anonymity that the scheme provides (3).

*Halting State's* concept of distributed, but secure, corporate operations across the entire internet is the logical end-state when corporations and employees need many more services than can be provided internally. It appears to predict the universal use of the "Web 2.0" services that have been appearing in recent years. As quickly as IT departments expand their services, the needs of companies expand even faster. Employees looking for more efficient ways to do their jobs find answers on the internet, spreading corporate data and computation across that open network.

Every time a successful internet attack is reported in the news, there is a renewed effort in governments and corporations to lock-down networks and ban certain kinds of applications. This reaction is contrary to the direction that business operations are moving. Government, corporate, and personal activities rely increasingly on the use of the network. We must find a way to perform those operations securely across the internet, not prohibit the use of one of the most powerful inventions in human history. Given this necessity, all communications and data exchange need the kind of encryption and user authentication that Stross describes in his novel. The work we are doing on the network is too important to be done without protections. The alternative to protection is to accept an infinite series of successful attacks against our poorly protected systems, operations, and data.

Just as True Names' 1981 global information grid has become a reality, the Open IT environment described by *Halting State* in 2008 is already on its way. Our modern IT systems have to evolve away from the vulnerable design like that of Vinge's 1981 world, toward something like the more secure world of Stross's novel in 2008.

## References

1. Vinge, V. (1981). "True Names", a short story appearing in *True Names and the opening of the cyberspace frontier*, edited by James Frenkel. Tor Books, 2001.
2. Markoff, J. (February 18, 2010). "Malicious Software Infects Corporate Computers". New York Times Online.  
<http://www.nytimes.com/2010/02/19/technology/19cyber.html?hp>
3. Stross, C. (2008). *Halting State*. Ace Books.

*Roger Smith is the chief scientist and chief technology officer for U.S. Army Simulation, Training, and Instrumentation, in Orlando, Florida. He has also served as a group-level CTO for Titan Corporation and as a vice president of technology for BTG Inc. A member*

*of RTM's Board of Editors, Smith has led technology innovation for software and computer systems for military training and command systems. He holds a Ph.D. in computer science and Doctorate in business administration.*