The New York Times

Special Section: Security NYT NOW

Reinventing the Internet to Make It Safer

By Nicole Perlroth

December 2, 2014 9:25 pm

SAN FRANCISCO — What if it isn't too late to start from scratch?

It was only about 40 years ago that Vinton G. Cerf and Robert E. Kahn holed up in the conference room of a Hyatt hotel in Palo Alto, Calif., and sketched out the sets of rules and protocols that laid the foundation of the modern Internet.

Despite big advances in speed, performance, memory and machines, their decisions continue to form the basis for modern digital communications — much to the detriment of security, some experts argue.

But the United States government is teaming up with computer scientists to do something about it.

Five years ago, the Defense Advanced Research Projects Agency, or Darpa, decided to explore what the Internet might look like if we could rebuild the computer systems from the ground up, employing the hard lessons we have learned about security. The idea was simple, yet seemingly impossible.

Special Section: Security

After a year of record-setting hacking incidents, companies and consumers are finally learning how to defend themselves and are altering how they approach computer

security.

The program, called Clean Slate, consisted of two separate but related efforts: Crash — short for Clean-Slate Design of Resilient, Adaptive, Secure Hosts — a multiyear project aimed at building systems that were much harder to break into, that could continue to fully function when they were breached and that could heal themselves, and MRC, short for Mission-Oriented Resilient Clouds, which applied similar thinking to computer networking and cloud computing.

While Clean Slate was designed to make machines more aware of their environment, a separate effort at Darpa, called Active Authentication, is intended to make machines more aware of their operator. The program is exploring ways that machines could recognize humans by analyzing behavior, like a typing pattern, rather than a password or a fingerprint.

The Clean Slate programs were designed to run for only four years. The Crash program finished last year, though three of its projects have continued for a fifth year. The MRC program will wrap up this year.

With the advent of cloud computing and shiny new phones, tablets and watches, it can be easy to forget that in many ways our computer systems are still very old.

“The software we run, the programming language we use and the architecture of the chips we use haven’t changed much in over 30 years,” Howard E. Shrobe, a computer science professor at the Massachusetts Institute of Technology, said in a recent phone interview.

Dr. Shrobe and others note that the Internet’s basic design decisions were made when computer hardware was significantly more expensive than it is today. Forty years later, the consequences of decisions made in those resource-constrained days remain.

“Everything was built with performance, not security, in mind,” Dr.

Shrobe said. “We left it to programmers to incorporate security into every line of code they wrote. One little mistake is all it takes for the bad guy to get in.”

Never before has the problem been laid so bare. Last spring, security researchers stumbled on a two-year-old mistake a programmer had made in a critical piece of security software used by companies like Amazon, Netflix and Yahoo as well as by the F.B.I. and the Pentagon. It was built into a range of technology from weapons systems to home Wi-Fi routers. They called it Heartbleed.

Five months later, researchers discovered another serious error, this one in a program run by 70 percent of the machines that connect to the Internet. Only this time, it had taken 22 years to discover the bug, which could be used to seize control of hundreds of millions of computers. They named it Shellshock.

Together, the Heartbleed and Shellshock bugs affected more than half the Internet, putting web vulnerabilities in the limelight. But for security experts, the bugs were just further evidence that it may be time for a do-over.

Dr. Shrobe, who oversaw the Clean Slate program for Darpa until last year, said that from the beginning he wanted the programs to be more than a thought experiment.

“It was always my intent to offer a menu of technical options that companies who make computers and computer software could introduce into the commercial stream,” he said. “We’re beginning to see some of that work take effect now.”

He points to one Crash program called Clean Slate Trustworthy Secure Research and Development, which those involved with it nicknamed Custard. It is not a full replacement of existing infrastructure but a way to

use software and other technologies to run computers in a safer mode that can sort out who has permission to conduct which operations.

"It is a huge, phenomenal step forward," said Peter G. Neumann, a computer security pioneer at SRI International, the Silicon Valley engineering research laboratory that worked with Cambridge University on the Custard project.

Dr. Neumann and Dr. Shrobe say Custard can eliminate an entire class of cyberattacks caused by buffer overflows, a common design flaw that allows hackers to send a message that overwhelms a computer's memory, causing the program to fail and allowing the attacker to inject malicious code. Over the last year, there has been significant and growing interest from companies in using Custard in their products, as well as from nonprofits, research communities and academia.

While nobody expects an entirely new Internet infrastructure to emerge in 2016, Dr. Shrobe and others say they see demand building for a long-term solution to computer security. And there may be a window to do it as the world's computing goes mobile and the Internet braces for the Internet of Things — the hundreds of millions of cars, shoes, thermostats and lampposts that will soon be online.

"Everyone has been burned by now," Dr. Shrobe said. "People are much more aware of the problem. The question is, What do you do now?"

A version of this article appears in print on 12/03/2014, on page F7 of the NewYork edition with the headline: Reinventing the Internet to Make It Safer.