Physicists developing novel technique that could facilitate nuclear disarmament

June 25 2014

A zero-knowledge protocol to prove that two cups contain the same number of marbles. Credit: *Nature*, http://dx.doi.org/10.1038/nature13457

A proven system for verifying that apparent nuclear weapons slated to be dismantled contained true warheads could provide a key step toward the further reduction of nuclear arms. The system would achieve this verification while safeguarding classified information that could lead to nuclear proliferation.

Scientists at Princeton University and the U.S. Department of Energy's (DOE) Princeton Plasma Physics Laboratory (PPPL) are developing the prototype for such a system, as this week in *Nature* magazine. Their

novel approach, called a "zero-knowledge protocol," would verify the presence of warheads without collecting any classified information at all.

"The goal is to prove with as high confidence as required that an object is a true nuclear warhead while learning nothing about the materials and design of the warhead itself," said physicist Robert Goldston, coauthor of the paper, a fusion researcher and former director of PPPL, and a professor of astrophysical sciences at Princeton.

While numerous efforts have been made over the years to develop systems for verifying the actual content of warheads covered by disarmament treaties, no such methods are currently in use for treaty verification.

Traditional nuclear arms negotiations focus instead on the reduction of strategic—or long-range—delivery systems, such as bombers, submarines and ballistic missiles, without verifying their warheads. But this approach could prove insufficient when future talks turn to tactical and nondeployed nuclear weapons that are not on long-range systems. "What we really want to do is count warheads," said physicist Alexander Glaser, first author of the paper and an assistant professor in Princeton's Woodrow Wilson School of Public and International Affairs and the Department of Mechanical and Aerospace Engineering.

The system Glaser and Goldston are mapping out would compare a warhead to be inspected with a known true warhead to see if the weapons matched. This would be done by beaming high-energy neutrons into each warhead and recording how many neutrons passed through to detectors positioned on the other side. Neutrons that passed through would be added to those already "preloaded" into the detectors by the warheads' owner—and if the total number of neutrons were the same for each warhead, the weapons would be found to match. But different totals would show that the putative warhead was really a spoof. Prior to the

test, the inspector would decide which preloaded detector would go with which warhead.

No classified data would be measured in this process, and no electronic components that might be vulnerable to tampering and snooping would be used. "This approach really is very interesting and elegant," said Steve Fetter, a professor in the School of Public Policy at the University of Maryland and a former White House official. "The main question is whether it can be implemented in practice."

A project to test this approach is under construction at PPPL. The project calls for firing high-energy neutrons at a non-nuclear target, called a British Test Object, that will serve as a proxy for warheads. Researchers will compare results of the tests by noting how many neutrons pass through the target to bubble detectors that Yale University is designing for the project. The gel-filled detectors will add the neutrons that pass through to those already preloaded to produce a total for each test.

The project was launched with a seed grant from the Simons Foundation of Vancouver, Canada, that came to Princeton through Global Zero, a nonprofit organization. Support also was provided by the U.S. Department of State, the DOE (via PPPL pre-proposal development funding), and most recently, a total of $3.5 million over five years from the National Nuclear Security Administration.

Glaser hit upon the idea for a zero-knowledge proof over a lunch hosted by David Dobkin, a computer scientist, and until June 2014, dean of the Princeton faculty. "I told him I was really interested in nuclear warhead verification without learning anything about the warhead itself," Glaser said. '"We call this a zero-knowledge proof in computer science,"' Glaser said Dobkin replied. "That was the trigger," Glaser recalled. "I went home and began reading about zero-knowledge proofs," which are

widely used in applications such as verifying online passwords.

Glaser's reading led him to Boaz Barak, a senior researcher at Microsoft New England who had taught computer science at Princeton and is an expert in cryptology, the science of disguising secret information. "We started having discussions," Glaser said of Barak, who helped develop statistical measures for the PPPL project and is the third coauthor of the paper in *Nature*.

Glaser also reached out to Goldston, with whom he had taught a class for three years in the Princeton Department of Astrophysical Sciences. "I told Rob that we need neutrons for this project," Glaser recalled. "And he said, 'That's what we do—we have 14 MeV [or high-energy] neutrons at the Laboratory.'" Glaser, Goldston and Barak then worked together to refine the concept, developing ways to assure that even the statistical noise—or random variation—in the measurements conveyed no information.

If proven successful, dedicated inspection systems based on radiation measurements, such as the one proposed here, could help to advance disarmament talks beyond the New Strategic Arms Reduction Treaty (New START) between the United States and Russia, which runs from 2011 to 2021. The treaty calls for each country to reduce its arsenal of deployed strategic nuclear arms to 1,550 weapons, for a total of 3,100, by 2018.

Not included in the New START treaty are more than 4,000 nondeployed strategic and tactical weapons in each country's arsenal. These very weapons, note the authors of the *Nature* paper, are apt to become part of future negotiations, "which will likely require verification of individual warheads, rather than whole delivery systems." Deep cuts in the nuclear arsenals and the ultimate march to zero, say the authors, will require the ability to verifiably count individual warheads.

More information: A zero-knowledge protocol for nuclear warhead verification, *Nature*, dx.doi.org/10.1038/nature13457

Provided by Princeton Plasma Physics Laboratory