Argonne NATIONAL LABORATORY

Vulnerability Assessment

New bottle cap thwarts wine counterfeiters

When the Roman historian Pliny the Elder wrote "*in vino veritas*" – in wine, there is truth – he must not have been drinking from a counterfeit bottle. Argonne researchers Roger Johnston and Jon Warner have created a device to ensure that modern wine connoisseurs can have faith that they are drinking what they pay for.

In the past few decades, bottles of rare premium vintages have begun to command tens of thousands of dollars apiece at auction, and thousands of other wines retail for hundreds to thousands of dollars a bottle. Although there may be no match for quality of the product inside, the ease and accuracy with which fraudsters can pass off bottles of "two-buck Chuck" with ritzy labels have allowed wine counterfeiting to grow into a booming criminal enterprise.

This work represents an offshoot of the work by the Vulnerability Assessment Team (VAT) in Argonne's Nuclear Engineering (NE). While the VAT conducts R&D on broad security issues, including nuclear safeguards, Argonne's NE division has a long history of addressing nuclear safeguards and security issues.

"As often happens," Johnston said, "R&D on one problem can lead to unexpected inventions; that is what happened here. We were working on tamper and intrusion detection projects for nuclear safeguards, courier bags, and cargo security, and also on security for pharmaceuticals. Various concepts and technologies that were developed for those projects led to the current wine application."

A new cap invented by Argonne's Vulnerability Assessment Team can detect fraudulent or tampered wine. By plugging the cap into a computer through a USB cable, a wine buyer or auctioneer can determine if the wine inside is genuine. New generations of the cap will contain a color sensor that detects a particular tiny section of a tie-dye pattern located under the cap.

"One of the biggest problems buyers of very expensive wines have at auctions is that they have no way of being absolutely sure if the bottle contains the wine it purports to without actually opening the bottle and taking a swig," said Johnston.

To combat this problem, Johnston and his colleagues in Argonne's Vulnerability Assessment Team (VAT) have created a cap that winemakers can fit over the bottle's cork. The cap contains a small circuit that completes when it is removed, triggering an electric pulse that creates electronic evidence someone has tampered with the bottle. "There's no alarm that screams at you if the wine's been opened," Johnston said, "but there's no way of getting rid of the evidence of tampering because basically, when tampering occurs, information is erased—a kind of anti-alarm."

By connecting the cap to a laptop through a USB cable, the auctioneer or the consumer can check whether or not the wine has already been opened or altered.

Each cap has a unique bottle number that is registered to the winemaker, preventing wine counterfeiters from putting the Argonne caps on their fake Bordeaux and Burgundies.

In addition to the outright counterfeiting of fine wine, buyers face another potential problem when assessing the purity of a bottle. To preserve the life of some of their wines, some winemakers will remove the cork from the bottle and blend in a small quantity of wine from a newer vintage in a process known as "reconditioning."

Although reconditioned wines may have longer shelf lives, some winemakers try to pass off their reconditioned bottles as purely the older vintage, Johnston said. With the Argonne cap, bottles cannot be reconditioned without the buyer eventually finding out.

Because the vast majority of wine fraud targets the very highest tier of wine manufacturing, the Argonne cap could become a "status symbol" among wineries potentially interested in the Argonne technology, said systems engineer Jon Warner, who works alongside Johnston in the VAT. "Our device may be able to generate a certain snob-appeal factor among winemakers; they can say, 'our wine is so good, we needed to spend money on this security device, although only a few dollars of parts are used in the device."

Johnston and Warner plan to enhance the security of the cap even further by connecting it to a high-quality color sensor chip. The top of the cork would then bear a tie-dye pattern of color swirls that the chip would have to recognize. According to Johnston, the sensitivity of the color sensor would make it extraordinarily difficult for someone to open the cap and put it back close enough to the original position to fool the sensor.

For more information, please contact:

Angela Hardin
Phone: 630-252-5501
E-mail: ahardin@anl.gov

August 2008