

@ Georgia Tech Research Institute engineers have developed a series of prototype systems that use special, high-strength permanent magnets to quickly erase a wide variety of storage media.

BELOW: Senior research technologist Christopher Shappert, standing, and senior research scientist Michael Knotts image a hard disk drive platter using magnetic force.

Protecting Sensitive Data

Researchers develop fail-safe techniques for erasing magnetic storage media.

BY JOHN TOON

After a U.S. intelligence-gathering aircraft was involved in a mid-air collision off the coast of China four years ago, the crew was unable to erase sensitive information from magnetic data storage systems before making an emergency landing in Chinese territory.

That event underscored the need for simple techniques to provide fail-safe destruction of sensitive data aboard such aircraft. Working with defense contractor L-3 Communications Corp., scientists at the Georgia Tech Research Institute (GTRI) have developed a series of prototype systems that use special, high-strength permanent magnets to quickly erase a wide variety of storage media.

Developed so far for VHS tapes, floppy drives, data cassettes, and small computer hard drives, the techniques could also have commercial applications for banking, human resource and other industries that must also protect sensitive information.

"This is a very challenging problem," says Michael Knotts, a research scientist in the GTRI's Signature Technology Laboratory. "We had to verify that the data would be beyond all possible recovery even with unlimited budget and unlimited time. Commercial devices on the market for data erasure just couldn't fill the bill, because

they were magnetically too weak, they were physically too large and heavy, or they didn't meet stringent air safety standards."

During the project, the researchers developed testing procedures that use a magnetic force microscope (MFM) — a variation on the atomic-force microscope (AFM) more commonly used to provide detailed images of surfaces at the nanometer scale. The MFM mapped the very small magnetic perturbations created by data stored on the media, helping determine how well data patterns had been destroyed.

"If you erase the data by whatever means, you should see a surface devoid of any specific pattern or periodicity," Knotts explains. "Our goal was to see a random distribution of magnetization that would indicate a clean disk."

During the three-year project, Knotts and collaborators Don Creyts, Dave Maybury, Candy Ekangaki, and Tedd Toler explored a broad range of possible destruction techniques, including burning diskettes with heat-generating thermite materials, crushing drives in presses and chemically destroying the media.

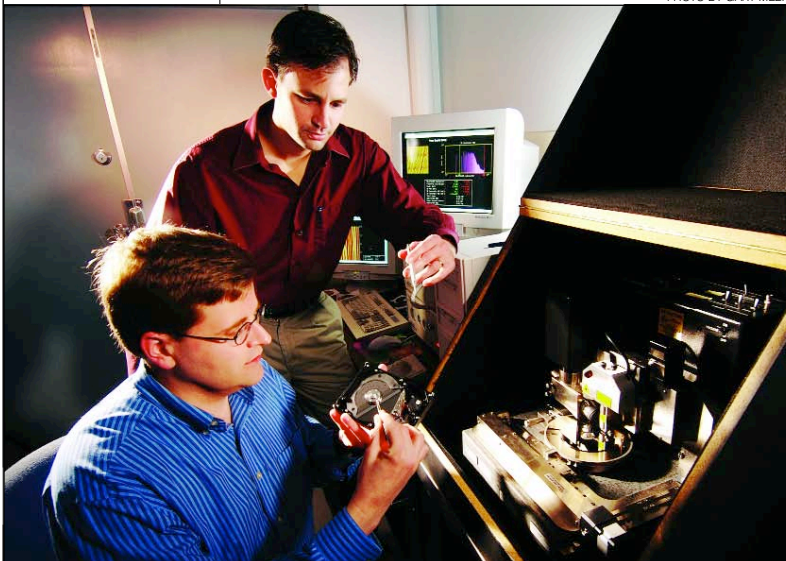
The researchers had to select techniques and equipment that would:

- Be light enough for aircraft use and operate independently of aircraft electrical systems;
- Be mechanically simple to ensure reliable operation;
- Produce no harmful gases or flame;
- Provide mechanisms to prevent inadvertent erasure.

During their first year of work, the researchers learned that data could remain on diskettes that had been subjected to high heat, and had to abandon thermal destruction techniques because of the fire and harmful gases they generated. That left only magnetic techniques.

In developing techniques for complete erasure, the researchers first had to learn how different data storage drives operate, then assess the magnetic field levels necessary for complete erasure. To do that, they obtained a number of commercially available micro-drives, cut the media into sections, subjected them to varying magnetic fields, and then tested the sections with the MFM.

PHOTO BY GARY MEEK



CONTACT

Michael Knotts at
404-385-4534 or
michael.knotts@
gtri.gatech.edu

LEFT: Research engineer David Maybury models a magnetic data destruction circuit using 3D finite element analysis.

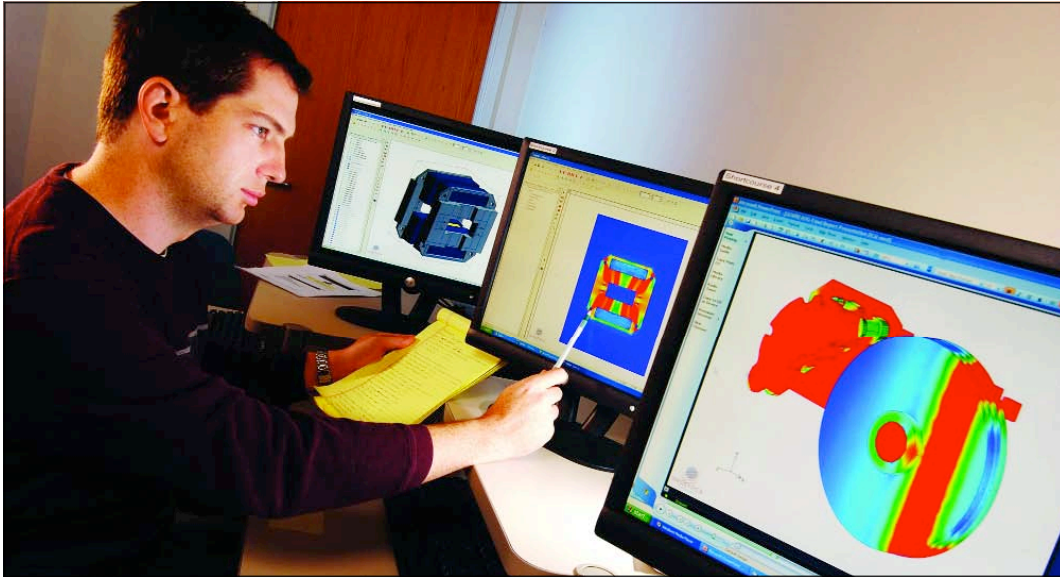


PHOTO BY GARY MEEK

“We had to understand how the data is laid out on the disk so we could know where to look for the patterns, and we had to do a lot of measurements to determine exactly what kind of magnetic field is needed to destroy all data,” says Knotts. “We had to do a lot of destructive testing to determine that, and our lab is littered with the carcasses of dead hard drives to prove it.”

Producing a magnetic field sufficient to destroy data patterns required the use of neodymium iron-boron magnets custom-designed for the project and special pole pieces made of esoteric cobalt alloys. The magnets, which weigh as much as 125 pounds, had to produce fields sufficient to penetrate metallic housings that surround some drives.

“We developed models for magnetic circuits that we could run through optimization codes to design the best shape to get the field that we needed,” Knotts says. “It takes quite a magnetic field to get through the steel enclosures on some of the drives. We are producing magnetic fields comparable to those used in magnetic resonance imaging equipment, so these are not your ordinary refrigerator magnets.”

Mechanically, the researchers faced challenges in reliably moving data storage devices through the magnetic fields. In some cases, aircraft crews would simply insert removable media into a motorized mechanism that pushes them past the magnets, while for other media, crews would have to twist a knob and pull drives out of their enclosures and through a magnetic field. To prevent accidental erasure, each technique requires several deliberate steps.

With success in erasing removable media and small hard drives, the researchers are moving onto a final phase of the project, which will involve large computer hard drives partially encased in thick steel caddies.

Beyond Department of Defense applications, the magnetic erasure techniques could have applications to the commercial world, where banks, human resource agencies and other organizations must ensure complete destruction of data in computer equipment being discarded.

Knotts admits he’ll be a bit sad to see the project end.

“This was certainly an unusual project,” he says. “It’s not often that we get paid to crush equipment in presses, blow things up and set off fires in microwave ovens.”

@ Read online at: gtresearchnews.gatech.edu/reshor/rh-ss06/guard-dog.htm



PHOTO BY JOHNNY LYE, COURTESY OF ISTOCKPHOTO.COM