David Brian Kern
Theft of Trade Secrets

Russell Atkinson

ADDRESS: c/o Cryptologia, Department of Mathematical Sciences, U.S. Military Academy,
West Point, NY 10996

ABSTRACT: This article provides an account of how David Kern illegally copied and decrypted technological data related to radiological devices, which had been encrypted using commercial-grade software. We discuss how the cryptographic system allowed the plaintext to be recovered, but ultimately led to Kern's prosecution and conviction for Theft of Trade Secrets under the federal Economic Espionage Act.

KEYWORDS: Economic espionage, trade secrets, Varian, radiology, FBI, Silicon Valley, Kern

David Kern walked into the engineering office of the radiology group where he worked. "What's that?" he asked when he saw the laptop computer sitting on a desk. The laptop belonged to Mark Zambetti[1], the service representative for Varian Associates. Varian manufactured the complex radiological devices which the radiology group owned and used to treat cancer at various local hospitals. Zambetti had left the computer at one of those hospitals the previous evening by mistake after a service call, and had called to have someone store it for safekeeping. One of the engineers had brought it to the engineering office. Zambetti was coming back for it this morning. When Kern was informed of this, he suggested they take a look at it to see what was on it.

The other engineers looked uneasily at each other, but Kern was their boss. One of them suggested that examining the laptop might be illegal without the permission of Varian or of Zambetti. Kern brushed off their objections, saying they were just going to take a look. Kern booted up the laptop and began to review the directory and file names. As a former Varian employee and a certified network engineer, Kern had no difficulty navigating through the directory structure and recognizing the nature of the files contained on the hard drive. It was a treasure trove of Varian technical and commercial information. He hooked up the laptop to his own computer and began to transfer the contents of the laptop's hard drive. Zambetti showed up at the lobby of the hospital while this transfer was in process. Kern kept him cooling his heels for an hour while the transfer was completed. One of the engineers then returned the laptop to Zambetti, who departed.

Kern began to examine the fruits of his labor. He soon realized that the most valuable information on the disk was Varian's "Tech Tips," a compilation of technical procedures, problems, troubleshooting techniques, and institutional knowledge about how to service or install Varian's radiological products. He opened up the viewer and selected the Tech Tips file. The program paused a moment and then closed down. Kern recognized what had happened from his

[1] Personal names, other than Kern's, have been changed to protect privacy.

days using Varian software. The program had recognized that the proper key had not been used and shut down. Kern could not read the file because the data was encrypted!

* * * * *

Thus began the fascinating case of U.S. v. David Brian Kern, the first prosecution in California under the federal Economic Espionage Act of 1996[2]. This law was passed to correct some of the omissions and inconsistent application or interpretations of other federal statutes. It creates two separate crimes: economic espionage (sponsored by a foreign power), and trade secret theft. Both involve the taking of protected, but unclassified, information related to products sold in interstate commerce. Violations under this act can be charged only with permission of a unit in the Department of Justice having responsibility over intellectual property crimes. The act is sparingly used to ensure that it is applied only in the serious types of crimes envisioned by Congress. Kern was to become only the tenth case charged under this act.

Varian Associates is one of the oldest high technology firms in Silicon Valley, predating the semiconductor age. Its product line has always focused on radiation in its various forms, and it originated the klystron tube, which is used in nuclear applications. While it has undergone several changes in name and function, the medical device group has always been a major part of the company. It was this division which had hired Kern years before. Unquestionably bright, Kern had quickly learned about the different products, both hardware and software, and about the benefits and hazards of nuclear radiation. Varian's products could save lives but, if misused or in poor repair, had the potential to be lethal. Kern also learned the economics of the products; they were very expensive and quite large. Radiologists and the technicians that support them were highly paid. Down time could be exceedingly costly to a hospital or radiology group. As a result, Varian made a good profit servicing the machines they sold, keeping them operating safely, and installing upgrades. There also arose a small cadre of specialists, mostly former Varian employees, who performed those same services in competition with Varian.

Despite Kern's technical ability, he did not succeed as a Varian employee. After being tried in several different posts, he was eventually fired for poor performance. Kern hired an employment law attorney and filed a wrongful termination lawsuit against Varian. He found employment at a radiology firm in the Sacramento area supervising the engineering department. His new employer was unaware of the lawsuit, or even that Kern had been fired. Kern almost immediately began to antagonize his coworkers. He frequently broke into the company computer network, accessing areas for which he was not authorized. He bragged about how he could do this with ease, and how much more competent he was than the company's network administrator.

After working there awhile he was assigned a part-time secretary. One of her first assignments was to retype stacks of pages of technical material from dark red paper into a computer data base. The material was marked as Varian proprietary material, and it was obvious that the paper was colored so as to prevent photocopying. The secretary was uneasy about this

[2] 18 U.S. Code §1831 et seq.

assignment, but Kern assured her it was nothing to worry about, as the radiology group had licensing agreements with Varian. She began the project, but it was tedious and difficult work due to the poor legibility of the print on the red paper. Not long thereafter, Kern provided her with more stacks of paper. This second batch consisted of computer printouts having text in the middle with graphics or typographic symbols around the text. Kern bought scanning hardware and software and taught her how to use the optical character recognition (OCR) program. She began to work on this project as well. She had no idea that this second batch consisted of the plaintext of the Tech Tips copied from Zambetti's laptop. Kern had somehow managed to decrypt the stolen data. It became my job to figure out how.

I was then an FBI agent working on the High Tech Squad in San Jose, California. I received a phone call from a corporate attorney at Varian. I had met her a couple of years before when I came to Varian with information I had uncovered in an unrelated case showing that an ex-employee of Varian was selling Varian engineering drawings to a competitor. That case had resulted in both a civil and criminal judgment against the former employee, and Varian had been very pleased with the outcome. The attorney told me that they had just been informed by a customer in the Sacramento area that one of their employees, David Kern, had just been fired. That company had discovered in Kern's desk and other work areas a large volume of materials that appeared to be proprietary information belonging to Varian. The information included customer information and technical reference materials. She also told me they were currently in the middle of a lawsuit against Kern for wrongful termination. She asked me if I was interested in investigating the case. I was overloaded with other case work. But I also recognized that this held the potential to be the first federal prosecution in Silicon Valley for theft of trade secrets. The previous case I mentioned, involving the copied drawings, had occurred before the passage of the Economic Espionage Act, and thus had been charged using a variety of other statutes. This was a test of the new law, and intellectual property crimes were my specialty. I told her yes.

The details of my investigation and all the legal maneuvering that goes into a complex intellectual property case make an interesting story but are beyond the scope of this article. The fact of the ongoing employment law action made it easier in many ways to investigate the case, although there were also some serious drawbacks to this. It will have to suffice to say that eventually I learned how Kern was able to decrypt the information. His technological success was to prove his undoing. The tale also holds some significant lessons for all who use, buy, or sell cryptographic products.

When Kern discovered that the Tech Tips were encrypted, he began to devise a scheme to obtain the cryptographic key. Kern was smart enough to realize that the commercial grade programs which Varian used to encrypt its products used algorithms which were too robust to break using pure cryptanalytic techniques. But he had the advantage of being an insider. He was very familiar with the technology Varian used to protect their information. Because he had used it himself, both as an employee and as a customer licensee, he knew that Varian usually used a standard commercial database program that had a third-party cryptographic "plug-in." Their vendor used a dongle, a hardware device which plugs into the parallel port of a computer. Kern figured that if he could get his hands on the dongle Zambetti used, he could decrypt the data. If he could decrypt the data, he and his engineering crew could themselves perform some service which they now paid Varian to do. He would also become much more marketable to the service companies who competed with Varian in the event he decided to move on. The dongle was worth real money.

As fate would have it, Zambetti returned to the hospital shortly thereafter to do more service work. As he worked, his laptop computer sat on the work station surface, and its carrying case was right next to him. Kern eyed the laptop; it did not have the dongle plugged in. Ralph Griffith, one of Kern's subordinates, was working with Zambetti, assisting where he could and picking up some useful tips just by watching. Kern knew the dongle had to be close at hand. There was no point in having the information on the laptop unless the technician could access it in the field. Kern took Griffith aside and gave him his orders. Kern would distract Zambetti, and Griffith was to look through the carrying case for the dongle. If he found it, he was to give it to Kern. Griffith's stomach turned over when he heard this assignment. He knew this couldn't be legal, but Kern was his boss and known for his temper. Besides, Griffith had been the one who recovered the mislaid laptop in the first place and had not prevented Kern from copying the files. He tried to argue, but Kern was firm.

Kern initiated an animated discussion with Zambetti in a remote corner of the radiology room. Griffith looked into the laptop bag, and quickly found the dongle. He removed it and signaled Kern. Kern met up with Griffith and took the dongle to the engineering lab. He plugged it in and booted up the desktop unit. He had also copied the stolen files onto two other computers. Kern opened the Tech Tips file. Success! The reader displayed the text in the clear. Now the real test: Kern unplugged the dongle and tried a different section of the file. The new portion was still displayed in the clear. The program did not use the dongle "on the fly," i.e., seeking new key sequences as it decrypted each section. The key was apparently generated only once and stored in the computer's random access memory. As long as he did not turn off the computer or quit the program, Kern could read the entire file at his leisure without the dongle. He quickly plugged the dongle into each of the other two computers in turn, and launched the reader-decryption program on each. He then returned to the radiology room and, with Griffith's assistance, put the dongle back in the bag. Months later Zambetti was still totally unaware that the dongle had ever been taken.

Kern still faced considerable challenges. Varian's technical team had insisted on additional protections from the plug-in vendor. The program had been altered to disable the print and write-to-disk functions, so that the decrypted information could not be saved in plaintext form or printed out on paper. Furthermore, they had anticipated the possibility of someone trying to copy the information to the clipboard (used in Windows to transfer data from one document to another). They had the vendor insert code that closed the program if the user attempted to write to the clipboard or if he hit the Alt-Tab keyboard combination used in Windows to change from one active program to another (such as a word processor). This meant that the only way the information could be viewed was using the specialized viewer they provided, and only on the screen. The information would be of little use to Kern if he could not save the file in plaintext so he could manipulate it and store it in non-volatile form. As it was, if the computers were switched to another program, if the power failed, or if any of a number of interruptions occurred, he would be unable to access the data again without the dongle. Kern, however, again using his familiarity with Varian's techniques, was ready for this. He knew these protective functions were designed under Windows 3.1. Kern had Windows 95 loaded on his machines, along with a commercial program known as Print Screen. This program restored the functionality of the now little-used Print Screen key to mimic its original purpose under DOS. When the user hits that key, the Print Screen program prints out on paper a pixel-by-pixel representation of whatever is shown on the computer screen. Kern dragooned his entire engineering team into helping him over the next few weeks, opening every Tech Tip, then pushing the Print Screen key to print it out. This is why Kern had loaded the data onto three computers before stealing the dongle - so he could share the tedium with his subordinates. Together they produced the massive stacks of papers which his secretary had been assigned to scan.

While the dongle did not prevent Kern from accessing the encrypted data, it served its purpose in a way. By forcing Kern to engage in what lawyers call asportation - the physical carrying away of a stolen item - and by forcing him to go to extraordinary lengths to obtain it, the protections made it possible to prove two key elements in trade secret theft. First, information must be "reasonably" protected to qualify as a trade secret under the federal statute. Although defense attorneys always argue that the trade secret was not protected in a reasonable fashion ("if the defendant was able to steal it, it must not be a crime"), the prosecutors were confident Varian's efforts were sufficient under the law. Second, and more important, Kern's actions clearly demonstrated criminal intent. Kern could not argue, at least not with any credibility, that he did it by accident, or that he thought it was allowed under the terms of his existing license. It looked like a theft, it smelled like a theft - it was a theft.

Kern's dishonesty and arrogance led to his being turned in and prosecuted. He lost his employment action and the ensuing counterclaim by Varian for theft of trade secrets, because he "took the Fifth" and refused to answer questions during discovery. The civil judge refused to allow him to introduce any evidence in his own behalf if he would not give Varian's attorney a chance to hear his testimony. He is liable for a $3.5 million judgment for Varian's damages and legal fees. He lost his job and gave up his retained attorneys in the civil and criminal cases. He represented himself on the civil case and obtained a public defender on the criminal case. On January 13, 2000 David Kern pleaded guilty to one count of trade secret theft. He was sentenced on April 4, 2000 to a year and a day in federal prison by U. S. District Judge David F. Levi.[3]

There are lessons to be learned here by the cryptographic community. A theoretical cryptologist may dismiss this case as of little relevance with the thought, "Kern stole the ciphertext and the key; of course he could decrypt the information." Such a simplistic view misses the whole point and distinguishes the theoretician from the applied cryptologist. A useful cryptographic application must take into account how the normal user behaves and what the level of threat will be in the field. Failure to do so is poor cryptology.

In retrospect, it is easy to criticize the cryptographic implementation. It seems obvious now that this particular program, which is designed to be portable, cannot be entirely secure in the field since the user must carry the dongle with him. It will thus almost always be available to anyone who gets their hands on the computer itself. In fact, most users probably leave the

[3] USDC, Eastern District of California, case no. 2:99CR00015-01

dongle plugged in all the time. In an office environment the design may make more sense. The dongle could be locked in a safe or file cabinet, and even if it is left in the port, the surrounding environment is relatively secure. At least the program should have used a password as an additional layer of protection. The program should also have been designed to use the dongle "on the fly," or at least have had a timekeeping procedure that periodically checked to see if the dongle was there, and shut down if it was not. A simple physical (hard) key locking the laptop would have prevented this theft, at least if the hard key was not also left with the computer.

To be fair to the designers, however, the protections they provided were reasonable under all the circumstances known to them at the time. Passwords are much more easily guessed or found by brute force "cracking" than the long random keys stored in a dongle. The stories are also rampant of people writing down their password and keeping it on or near the computer. A dongle has advantages over a password. The disabling of the print, Alt-Tab, and save features was also thought out quite well. That would have sufficed but for the cleverness of David Kern and the introduction of commercial software products that were not easily foreseen at the time of design. The primary design consideration was protection not against the outsider who steals the computer, but against the dishonest employee (who has the dongle) so that he could not readily copy the material in any usable form. This case is eerily predictive of the problems now encountered by the entertainment industry in audio, video and related fields. The use of cryptography to bind information to the display device so that the legitimate user can perceive it but not copy it, or change its form, is proving exceptionally difficult. In this case, the protections served their intended purpose by requiring Kern to engage the help of several others. This resulted, quite predictably in my view, in the scheme being discovered. Varian has since cured all the problems identified here.

In more general terms this case is illustrative of what I consider to be the flaws in the positions of both sides in the current debate over cryptographic export laws. As a veteran of 25 years in the FBI with experience working espionage and trade secret cases, I know that the security of encrypted information is almost totally independent from the cryptographic strength of the algorithm used or the length of its keys, at least in the commercial arena. Secrets entrusted to even the most modest commercial cryptographic software products, for all practical purposes, cannot be recovered cryptanalytically in a useful time frame and useful volume by anyone from whom they are intended to be kept. I am excluding intelligence agencies of major nations. Anyone who is legitimately worried about those agencies should probably be using something other than a commercial product. Many products are so inconvenient that ordinary users defeat them by failing to employ them at all, by leaving a password (or dongle) accessible, or by printing out a plaintext version and leaving that handy for when they forget their password. If the government really wanted to protect American know-how, rather than focus on the export of encryption products, it should encourage use of techniques that protect against the genuine threat - the corrupt insider - such as pre-employment background investigations, reform of employment laws now favoring the employee, use of the need-to-know principle, and hard locks and keys.

The real threat comes from insiders, those people who have legitimate access to the information or to the space where it is kept. This is just as true in the commercial venue as it is in classified circles. Kern is typical. The common thief is indeed much more common than the cryptographer with access to massive computing power and the ability to intercept private communications in large volume. Insiders are human, and they display all the frailties of humanity: greed, vengefulness, ideological conviction, and carelessness. Corporate executives tend to fear "economic espionage" by their competitors, but as a security manager, I know that a company is much more likely to be victimized by its own employees, licensees, partners and vendors. People like David Kern will always exist and always be willing and able to steal, sell, or give away secrets to which they gain access. The best protection the government can provide to the nation's intellectual property is to punish the individuals who betray those who once trusted them. The David Kerns of the world belong in jail.

About the author

Russell Atkinson retired from the FBI in 1999 after 25 years as a Special Agent and Legal Advisor. He is now employed as a Senior Security Manager for a major Internet firm. He received a B.A. in mathematics from the University of California, Santa Barbara, and a J.D. from Boalt Hall of Law, University of California, Berkeley.