US Glass METAL & GLAZING
THE MAGAZINE OF INFLUENCE FOR GLASS INDUSTRY LEADERS

Volume 42, Issue 11 - November 2007

Can't Hear Me Now

Window Film Offers Defense Against Wireless Hackers

by Drew Vass

day. In the West end of a typical American city, life is as usual—shoppers are coming and going from stores and cars are flowing past.

A vehicle pulls up and stops in front of a retail store. Two people remain in the car—local college students studying computer science at a nearby university. One is talking on his cell phone, occasionally laughing, perhaps catching up with an old friend; the other appears to be typing on her laptop, maybe squeezing in a few final edits for a paper due Monday.

A police officer passes by on foot and glances in the car. The young woman looks up from her laptop and smiles back at him. The loiterers appear friendly and innocent, maybe waiting for a friend to finish shopping.

Two weeks later, the retail store realizes it's been hacked. Sensitive credit card and personal information has been stolen and now the store's most precious inventory—its customers—are at risk.

Utilizing an everyday laptop equipped with a wireless antenna, two computer science majors tapped into the retailer's wireless network and extracted thousands of names, credit card numbers and other personal information.

Welcome to the Real World

This scenario may sound like something out of a movie, but similar ones occur in real life. On January 17, 2007, the TJX Companies, an off-price apparel and home fashions retailer, announced a similar hack actually occurred—creating what is now believed to be the largest data breach in U.S. history. The company's computer systems used to input and store millions of credit card numbers and personal information related to non-receipt bearing returns was compromised. The system serviced its T.J. Maxx, Marshalls, HomeGoods and A.J. Wright stores in the U.S. and Puerto Rico, and its HomeSense stores in Canada, but the damage was suspected to reach as far as the company's operations in the U.K. and Ireland as well. The company believes its perpetrators accessed the information as described in the opening (fictional) scenario. The hackers managed to siphon out everything from names, credit card numbers and home addresses, to driver's license numbers. And, like many robberies, the easiest point of entry for TJX's thieves was the windows. The only difference being—they never broke even a piece of glass and never entered the premises.

First Defense

Since the advent of wireless networking, companies and individuals alike have sought to lock down personal information through data encryption and network security programs. And these services have come a long way since their birth. While they are still the number one defense against wireless hackers, the window film industry is now offering an added layer of protection for a building's most vulnerable point of access—its glass.

While a few window film manufacturers report, or at least allude to, having signal defense films in development, Martinsville, Va.-based CPFilms currently has the sector cornered. A unit of Solutia Inc. in St. Louis, the company says it has been manufacturing a patented signal defense window film for the federal government for years, but only recently has it declassified this product and made it available to the general public.

"We were approached about eight years ago by a supplier to the federal government about making a window film to stop wireless signal leakage through windows," explains Lisa Winckler, global director of technology at CPFilms' production facility in Martinsville, Va. "Today, CPFilms manufactures virtually 100 percent of the window film used by the federal government to prevent electronic

eavesdropping and wireless signal stealing."

Developed in conjunction with the U.S. Department of Defense and CPFilms' technology partner, ASTIC Signals Defenses, LLumar® Signal Defense Security Film uses a patented combination of metal and metal oxide layers to reduce signal strength across the electromagnetic spectrum. The company reports that its film has been installed on more than 200 buildings within various federal agencies, including the Department of Defense, Department of the Treasury, Department of State and various buildings within the executive branch. And it doesn't stop at federal office buildings, as CPFilms says its product has also been installed on the residences of senior government officials.

Coincidently, the same film also protects against physical blasts and intrusions. "We are limited by confidentiality agreements to say exactly which buildings [the window film] is on," Kent Davies, president of CPFilms Inc. told a Scientificamerican.com reporter. "But immediately after 9/11, one of the senior military officials talked about a window film that seriously protected against the damage from the plane crash. You can put two and two together and assume it was also protecting against wireless signals," he added.

Come and Get It
In May of 2007, CPFilms announced it was making its elusive film available to the public and greater details were unveiled with its declassification. Introduced as a "high-tech, clear window film for businesses and high net-worth individuals," the film is marketed as a means of securing and protecting the confidentiality of wireless and other "free space" electronic communications. Originally it was offered exclusively through the manufacturer, at a price that excluded the average homeowner. Instead, the company chose to target the retail, healthcare and financial services industries.

Just because the film is available, doesn't mean it's easily attainable, though. Some dealers say the price tag outweighs what many companies deem an extreme measure.

"CPFilms has changed their marketing strategy concerning this film. They have tried to target commercial accounts for obvious reasons while maintaining their direct government relationship," explains Mike Feldman, owner of Advanced Film Solutions a CPFilms dealer in New Port Richey, Fla. "We went to their training session back in May or June and we've had several inquiries, but haven't really closed any deals. We hear that some dealers have been able to grab sales, but who knows whether this is real or baloney."

Tommy Shoppe, a sales representative for Performance Films Distribution in Clearwater, Fla., agrees.

"CPFilms opened it up to us about eight or nine months ago, but we haven't had a great deal of success in selling it yet," Shoppe explains. "At this point, most people at least know about it, but it's a tough sale," he says adding, "It definitely takes a high level of sales expertise to close a deal on this film as opposed to the others we sell."

Shoppe says some customers do explore the option, but, at an approximate cost of $30+ per square foot, not many are willing to go there.

"One of the companies I'm working with now on a large project actually brought it up to me. They didn't end up going with it, but they were well aware of the product and wanted to explore the option," Shoppe says. He says the opportunities are there, though, but mostly (still) in the government contracting and private sector.

Foot Race
Just as hacking methods have and continue to change, so must the products that prevent them. Large corporations spend literally millions in protection and have entire departments dedicated to maintaining the latest techniques, but small businesses don't have the same resources. According to Visa USA, small businesses tend to be more vulnerable.

The credit card provider says more than 80 percent of cases opened since 2005 that involved unauthorized access to card data have involved small businesses. "With the proliferation of mobile communications technologies like cell phones, PDAs, Bluetooth devices and Wi-Fi enabled laptops, the airwaves are more flooded than ever with sensitive and confidential information, creating a prime threat for businesses of all sizes," says Arthur Money, former U.S. Assistant Secretary of Defense for Command, Control, Communications and Intelligence. "Surprisingly, while businesses spend millions on computer and Information Technology (IT) network security, they underestimate the risk of electronic signals from cell phones, wireless networks, computer terminals and other devices 'leaking' information through the windows of their buildings."

And "free space" electronic communications isn't limited to the most obvious devices either, but includes many devices you might not

suspect.

According to Money, all electronic devices broadcast radio frequency (RF) signals, whether intentionally or unintentionally. Intentional signals include those of, for instance, cell phones or wireless microphones commonly used in business meetings. Unintentional signals include those transmitted by such things as computer screens, hard drives and even keyboards. Even with encryption, windows provide intentional signals with a convenient path for leaking out of a structure and into the open air for anyone to access.

If the signal is properly encrypted, and hackers don't already have a method for decryption, your information is safe. CPFilms' LLumar® product doesn't replace the need for encryption, but decreases the likelihood of your signal making it out of the building envelope—through the windows at least.

"LLumar Signal Defense window film dramatically reduces the chance of wireless signals from leaking through windows and of hackers stealing wireless signals or conducting successful electronic eavesdropping from outside a building," Winckler says.

When The TJX Companies became aware of the hacking incident, it immediately notified the police, just as you would for a breaking and entering case. Soon, however, involvement in the investigation spread as far as the Canadian Mounted Police.

The Office of the Privacy Commissioner of Canada released news, September 25, 2007, stating that it believes the company failed on several levels to protect its customers' information.

"The company collected too much personal information, kept it too long and relied on weak encryption technology to protect it—putting the privacy of millions of its customers at risk," says Jennifer Stoddart, Privacy Commissioner of Canada. Though TJX failed to confirm the exact circumstances, the commissioner's office says TJX believes the intruder(s) may have initially gained access via the wireless local area networks at two of the company's U.S. stores. According to the commissioner's office, an investigation revealed The TJX Companies failed to keep up by not acting quickly enough in converting from a weak encryption standard to a stronger one.

TJX did convert to a newer standard, but the process took two years to complete, during which time the breach occurred. And, as it turns out, it wasn't a single Saturday-afternoon incident. The initial hack may have started at a storefront, but the commissioner's office reports that information was stolen from mid-2005 through December 2006, and involved transactions dated as far back as 2002. TJX has confirmed it believes the access was ongoing.

Windows are for Shopping

Every retail space in the world with a glass front knows the value of allowing customers a glimpse of its merchandise. This is the sort of eavesdropping every store welcomes. The type of eavesdropping the TJX Companies experienced is what they want to prevent. CPFilms says its product doesn't interfere with shoppers' view, but it does interfere with wireless signal transmissions by providing upwards of 35 decibels (dB) attenuation.

The concept of keeping elements in to prevent theft is a new concept. And if you're worried about electronic eavesdropping and hacking, you can't stop there. Hackers aren't limited to what leaks out of a building. Infrared and laser-microphones are also being used to intrude. In the case of "unintentional signals," a beam of infrared or laser light is projected through a building's windows to intercept acoustic signals from conversations, and even computer key strokes, from as far as hundreds of yards away.

"People are using laser technology to intercept information off of computer systems. They're literally sitting in front of a place and shooting it through a window," says Rob Heber, a CPFilms representative. "This film also addresses that issue."

Eavesdropping isn't just a concern of the government either. There are people in the world who face an everyday battle for maintaining privacy and have the money to invest in this sort of product—celebrities. One window film dealer, who chose to remain anonymous, says many celebrities are beginning to take notice of this product. Why? It seems the paparazzi isn't just pointing cameras these days, they're utilizing laser and IR microphones to dig up celebrity gossip. While he requested the names be kept private, he was able to cite two major film celebrities who are either contracting for or at least exploring the option.

Keep the Noise Down Will You?

There is yet another issue CPFilms' product deals with—interference. With the growth of wireless communications, the number of cell towers, Wi-Fi access points and radio, TV and microwave transmission antennas has grown exponentially, increasing the presence of electromagnetic energy. The "free space" inside a home or office can only be filled with so many signals before it becomes saturated. And with saturation comes interference. While the film is designed to keep RF signals in, a sort of side benefit is that it also keeps

them out.

"Our product also serves as a barrier that protects businesses against excessive electromagnetic interference from outside sources that can disrupt, inhibit and, in some cases, completely shut down basic, everyday electronic communications," explains Kent Davies, president of Solutia's CPFilms business. "In fact, most insurance policies don't protect against data loss due to electromagnetic interference, so the investment in window film may be the best way a business can protect itself," he adds.

The price tag for all these benefits may be high, but it might not be a hard sell to make with The TJX Companies these days. Sales figures in its recent quarterly results were all followed by an after-tax charge related to the intrusion. For the fiscal year ending January 26, 2008, the company expects to record $130 million in total related expenses.

The TJX companies declined to comment on what measures it's taking to help ensure there are no future incidents. It also declined to acknowledge whether the company has any knowledge of signal defense films, or not. CPFilms readily admits it's familiar with TJX, however.

Winckler says, "Yes, we are familiar with the incident, but, at this time, we can not comment specifically on existing or prospective customers."

Since the product is optically clear, the only answer future hackers may get is if and when they park in front of a T.J. Maxx store and, possibly, find themselves … without a signal.

Pentagon Admits to Using Signal Defense Film

In a United States Department of Defense (DOD) news briefing held Saturday, September 15, 2001, Rear Adm. Craig R. Quigley, deputy assistant secretary of Defense for Public Affairs, revealed the use of window film to eliminate acoustic and electronic eavesdropping.

Lee Evey, Pentagon renovation manager, was addressing questions from various members of the press regarding damages sustained in the attacks of September 11, 2001, and the resulting renovations, when a question was posed regarding the use of blast-resistant window film. Evey was in the process of answering when Quigley cut-in to address the specifics.

An excerpt from the conversation as recorded and distributed by the DOD is as follows:

Evey: We are putting in blast-resistant windows concurrent with the renovation as we go around the building. We're putting in, where we don't use blast-resistant windows, tempered glass windows that should they fragment, fragment into tiny little pieces, not great shards that fly for a distance.

Q: Some people have said the Mylar that's on older windows has helped them, in the older sections.

Evey: Yes ma'am.

Q: But it hasn't been put along the press room. Do you know any reason why—(laughter)—

Evey: Ma'am, I assure you, I couldn't talk to that. (Laughter.)

Q: Do you think it will be now, because a lot of people in the press office work with—

Evey: I don't know—

Evey: I don't install the Mylar, so I wouldn't—

Quigley: Can I—can I interrupt for a second?

Evey: Yes sir.

Quigley: Let me—let me address that. You get a little ancillary blast protection from the Mylar. That's not its principle purpose.

Q: Right.

Quigley: It's—it's almost coincidental. The principle purpose is to stop electronic and acoustic eavesdropping and for—we're going to assume that there's no classified, national security information that's in the press window section. So, in all other offices in the building, that wouldn't be true. So, it minimizes the opportunity for a simple, effective acoustic eavesdropping. And that's—yes, you get a little bit of blast protection, but—but that's not its real purpose.

Point of Least Resistance

Modern construction techniques incorporate a number of materials that help attenuate radio frequency (RF) and infrared (IR) transmissions. Walls, floors, doors and ceilings all typically contain some form of material that makes the overall solid structure less permeable than its glass.

"Most modern building materials do a halfway decent job [of attenuation]," explains Ron Waranowski, chief technology officer for ASTIC Signals Defenses LLC in Owens Mills, Md. "The goal is to pull the perimeter [transmission] around a building down, where a perpetrator can gain access from," he says. "Foil-backed drywall, aluminum window frames, insulation that's got foil on it, flooring, rebar and concrete—all of that stuff has pretty decent attenuation characteristics. The hole in the bucket, as far as RF/IR is concerned, is the glass," he explains.

It was for this reason the U.S. Department of Defense (DOD) established a need for a protective layer against eavesdropping and, when it did, Waranowski's company responded with the right answer.

"Historically, we're the organization that fielded the calls from the U.S. Department of Defense," he explains. "They had a question about window film technology and the ability to have a clear window film to attenuate RF/IR energy. My partner researched it and came up with a couple of films, submitted to DOD and they pretty much fell out of their chairs. We worked with Lisa Winkler over at CPFilms and that was the start of it."

ASTIC and CPFilms' share the patents for signal defense films.

"As of March of this year, we granted the commercial right for SD1000 to be distributed by CPFilms into the commercial markets here in the domestic U.S.," Waranowski says.

"The actual manufacturing and development is handled by CPFilms. They can take ten to 20 layers of metal oxide, one ten-thousandths of a human hair in thickness, and apply it to where your visible light transmission is still approaching 70 and your RF attenuation is 35- to 40-dB."Where conventional information security methods aim to encrypt signals, rendering them useless for hackers lacking the ability to decrypt, signal defense films prevent hackers from accessing the signal to begin with by providing a physical barrier.

"What's interesting about this technology is—it's a combination of information technology security and physical security," Waranowski says. "It's not software; it's physical technology. You can't have a guy that's drinking Redbulls and staying up 48 hours trying to figure out how to get in.

It ain't gonna happen," he says. "It would take the next Einstein to figure out the physics of it and how to penetrate that."

Drew Vass is a contributing editor for **USG**lass magazine.