Jun 29, 2011, 03:06pm EDT

Hewlett Packard's Laptop Lock Takes Only Seconds To Crack

Marc Weber Tobias Contributor
Cybersecurity
I am an investigative attorney and physical security specialist.

This article is more than 8 years old.

This is the first in a two-part series about the current state of laptop lock design, how they are supposed to work, why many are not secure, and how one major manufacturer, Hewlett Packard, evidently does not have a clue about how to protect your computer by the locks they sell for doing just that.

This is the HP cable lock attached to a Lenovo laptop. It can be removed in seconds by rapping the... [+]

In 2004 I issued a security alert and wrote several articles about defective designs that were incorporated into laptop locks, Kryptonite bike locks, motorcycle locks, and many other applications that relied upon the use of what are referred to as "tubular locks." Since then, responsible manufacturers within the industry figured out that their old designs were not secure and would not protect against simple attacks by thieves. Significant changes in lock and cable designs were implemented by these manufacturers to make it more difficult to compromise their mechanisms.

Unfortunately some companies continue to market junk. These locks, often imported from China, other Asian countries, and some from Europe are poorly constructed; they use inferior materials and assembly techniques

and poor-quality cables and locking cylinders. While they may look well-made and secure, they are not. Incredibly, one of the most well-respected computer manufacturers in the world, HP, evidently decided to get into the mechanical laptop lock business without knowing even the basics that every security engineer understands about designing these products. In this article, you can see what happens when basic security engineering principles are not followed.

Tubular locks, unless specially designed, are inherently less secure than other forms of locking... [+]

I called Hewlett Packard several weeks ago to ask about their model **BV411AA** and BV411UT locks that **sell for about $40** and are recommended by the company to protect a laptop. The individuals I spoke with at HP were quite insistent when I repeatedly asked them about the security of these locks. They told me that they could not be removed from a laptop without difficulty and that the computer would be destroyed in the process. When I pushed the point with one of the extremely helpful technicians, he offered to send one of the locks for me to evaluate. This was after he told me that several different supervisors had concurred in what he was reporting: *there was no security problem with these locks*.

The lock arrived the next day and I was able to open it in seconds with a common screwdriver.

The recognized method to protect your laptop is to use a cable lock. They are produced by many different manufacturers in the U.S., Europe, and Asia and range in price from $10 to about $50. One of those manufacturers is Hewlett Packard.

All of these locks, by design, have three critical components: the actual locking cylinder, the cable, and the mechanism that links the lock and cable to the computer. In addition, every computer has what is referred to as the

Kensington security slot, which is a rectangular recessed chamber that allows the affixing portion of the lock to be inserted and secured to prevent removal without the correct key or combination. At least in theory, that is how these devices are supposed to work.

While there are no industry standards to define what constitutes security for a laptop locking device, their purpose is to prevent and deter the theft of your computer for as long as possible. Security is all about time delay and difficulty in compromising either the cable assembly or opening the lock by simulating the correct key or code. So how much time is enough? That obviously depends upon the location of your computer, visibility, access and other layers of security. Common sense would dictate that a minimum reasonable time delay to stop an opportunistic thief would be one to two minutes, and certainly not fifteen seconds.

Often the easiest way to defeat many of the cheaper security systems is to simply cut the cable. Depending upon the manufacturer, this can either be easily accomplished or can require larger wire cutters or heavy-duty bolt cutters that may be more easily detected within an office or other closed environments. Virtually any cable can be cut with the proper tools but most organizations are more concerned about covert and non-destructive compromise that can be affected quickly and silently.

There are a variety of simple ways to compromise many of these locks and cables quickly without detection. In 2004, my colleagues and I demonstrated the use of a simple ballpoint pen to impression many of the tubular locks that were so prevalent at that time. Then we figured out how to open the best combination locks by cutting a strip of metal from an aluminum beer can and probing each of the wheels. Other bypass techniques were developed that were designed to open a specific or generic type of locking mechanism. Some manufacturers learned from these attacks and began designing much more secure hardware that could not be easily bumped, picked, impressioned, shimmed, or rapped open.

The real problem is that the production of secure locks costs money and requires an understanding of security in the context of laptops. Many vendors are only interested in selling something that looks good, and is cheap to produce but that is really not secure because it means higher profit margins. Often the consumer does not know the difference and ends up spending money for an inferior product which offers a false sense of security.

Tubular locks, unless specially designed, are inherently less secure than other forms of locking mechanisms. The industry has moved away from tubular locks and round keys to prevent simple forms of bypass.

There is a vast difference in quality among laptop lock designs. If a consumer pays forty dollars for a lock from a company like HP, it would not seem unrealistic to believe that he should have a reasonable expectation of a certain minimum measure of quality and security. After all, the reputation of Hewlett Packard for engineering excellence cannot be questioned in many areas including computers, printers and test equipment, so nobody would question their competence in the design of laptop locks.

It has been more than six years since I looked at laptop locks and their security in depth. Because of increased corporate and government reliance upon these devices, my original disclosures about their insecurity received a great deal of media attention including the New York Times. As a result the industry, at least some of it, radically changed their designs and attention to critical components that could make the difference between a few seconds of protection and significant deterrence.

I thought it was time to survey the industry again, especially since I have been involved in laptop lock designs and received a patent to remedy one of the original problems: the ability to open many of these locks with a plastic pen.

So a few months ago I began obtaining samples from many manufacturers in the U.S., Asia, and Europe to test and to examine the current state-of-the-art. Given a number of recent high-profile thefts of computers and the resultant serious compromise of millions of individual identities, I thought this was a highly relevant topic, especially for those that travel with their laptops. What I found were many companies that are still peddling the same inferior and insecure products. Some of these locks are imported but branded by the manufactured as their own. I suspect this is what HP has done, although when I spoke with their tech support personnel in two different centers they stated that the locks were indeed manufactured by HP.

I called Hewlett Packard several weeks ago to ask about their model BV411AA and BV411UT locks that sell for about $40 and are recommended by the company to protect a laptop. The individuals I spoke with at HP were quite insistent when I repeatedly asked them about the security of these locks. They told me that they could not be removed from a laptop without difficulty and that the computer would be destroyed in the process. When I pushed the point with one of the extremely helpful technicians, he offered to send one of the locks for me to evaluate. This was after he told me that several different supervisors had concurred in what he was reporting: there was no security problem with these locks.

The lock arrived the next day and I was able to open it in seconds with a common screwdriver.

I attempted to contact HP by calling their corporate-level escalation unit in order to advise them that their locks were defective in design. That is when I ran into the HP bureaucracy machine. I was politely told that the company does not talk to the public and that “if you have something to tell us, then you will have to do it in writing.” So I sent them an email. That was three weeks ago. Of course I have never received a response.

premise that every security engineer understands. The law is directly applicable to the design of the HP lock and explains why it can be opened.

In order to attach this cable lock to a laptop, the center portion of the locking cylinder is depressed which causes the extension of the scissor-locking system to engage with the Kensington security slot. This is simple, neat, and easy for the consumer. Unlike most other locks there is no need to use a key for locking (only for unlocking); just push, and the center of the lock moves inward against the computer until it clicks into a locked position. That "click" (and the way it is accomplished) is precisely the problem.

What the geniuses at HP failed to recognize or understand is that the real security of this design rested upon a spring-loaded pin that locked into place when the center of the mechanism was depressed by the user. All that is needed to move the pin to an unlocked state is a counter-force, just like Newton described.

It is the same theory that every pool player understands when a series of balls are on the table and touching each other in a straight line. If you strike the left-most ball, the one at the right will move. Only this time it is your computer that gets stolen, not the movement of pool balls. The net result: just about anyone can figure out how to remove one of these locks in seconds without a trace and, notwithstanding what I was told by HP, with absolutely no damage to your computer.

So you are the judge: is fifteen seconds of delay worth the $40 cost of this lock? More importantly, if you had purchased this product would you believe it was secure enough to protect your computer and everything in it? Of course you would because it "looked" good enough, and was sold by a respected company.

Gallery: Essential Gear For Smart Travel

12 images

View gallery →

The problem is that designing locks is not one of HP's core businesses or within their expertise. I would imagine that someone in accounting decided they could save money by buying these cheap locks from offshore for a couple of dollars and sell them for five times that amount. Unfortunately, the consumer may be left without a laptop because I can only assume that HP never bothered to do a security analysis on this product before offering it for sale.

There are many different lock designs, both key and combination, that are available in the marketplace. Corporate risk managers need to understand the differences, how these locks work, and which are vulnerable. In my next article I will explore specific designs and show how to defeat lots of them. It is incumbent upon anyone that relies upon these locks, especially in the commercial and government sectors, to understand how to evaluate them and to make sure that what you are buying is indeed secure. In the case of the HP models BV411AA and similar designs, they are not.

If you leave your notebook computer in an unsecured environment such as a coffee shop, conference center, library, or even your work area at the office, then you may need to protect it and keep it from being easily stolen or removed. Today the value of your computer hardware is almost irrelevant in

The tech that sent me a sample called the following week to ask if I would be placing an order. I told him that the locks had a serious security defect, could be opened in a few seconds, and that someone should call me. He said that he would route this to a product specialist who surely would follow-up. Nope. I guess the HP rule is still in place: they don't talk to customers the likes of me about such things! And incredibly, the technician I spoke with never asked me how I could open the lock he had sent to me and told me was so secure!

So, here is the problem: HP is selling a lock to protect your computer that can be opened in about fifteen seconds with a common 3" screwdriver with a plastic handle. Watch the video that my associate, Tobias Bluzmanis and I produced that demonstrates just how simple this is.

The lock is struck at a certain angle with the head of the screwdriver and it opens. How is this possible?

Evidently the engineers at HP never heard of Sir Isaac Newton, the famous English Physicist, and his Third Law of Motion which states that "for every action, there is an equal and opposite reaction." This is a really simple

comparison to what is stored on your hard drive. The ramifications of losing your laptop can be catastrophic and can also place you or others at risk of identity theft or compromise of confidential information and can result in significant liability and damages for your organization or government agency as well as the potential violation of state and federal privacy statutes.

The recognized method to protect your laptop is to use a cable lock. They are produced by many different manufacturers in the U.S., Europe, and Asia and range in price from $10 to about $50. One of those manufacturers is **Hewlett Packard**.

All of these locks, by design, have three critical components: *the actual locking cylinder, the cable, and the mechanism* that links the lock and cable to the computer. In addition, every computer has what is referred to as the Kensington security slot, which is a rectangular recessed chamber that allows the affixing portion of the lock to be inserted and secured to prevent removal without the correct key or combination. At least in theory, that is how these devices are supposed to work.

While there are no industry standards to define what constitutes security for a laptop locking device, their purpose is to prevent and deter the theft of your computer for as long as possible. Security is all about time delay and difficulty in compromising either the cable assembly or opening the lock by simulating the correct key or code. So how much time is enough? That obviously depends upon the location of your computer, visibility, access and other layers of security. Common sense would dictate that a minimum reasonable time delay to stop an opportunistic thief would be one to two minutes, and *certainly not fifteen seconds*.

Often the easiest way to defeat many of the cheaper security systems is to simply cut the cable. Depending upon the manufacturer, this can either be easily accomplished or can require larger wire cutters or heavy-duty bolt cutters that may be more easily detected within an office or other closed environments. Virtually any cable can be cut with the proper tools but most

organizations are more concerned about covert and non-destructive compromise that can be affected quickly and silently.

There are a variety of simple ways to compromise many of these locks and cables quickly without detection. In 2004, my colleagues and I demonstrated the use of a simple ballpoint pen to *impression* many of the tubular locks that were so prevalent at that time. Then we figured out how to open the best **combination locks** by cutting a strip of metal from an aluminum beer can and probing each of the wheels. Other bypass techniques were developed that were designed to open a specific or generic type of locking mechanism. Some manufacturers learned from these attacks and began designing much more secure hardware that could not be easily bumped, picked, impressioned, shimmed, or rapped open.

The real problem is that the production of secure locks costs money and requires an understanding of security in the context of laptops. Many vendors are only interested in selling something that looks good, and is cheap to produce but that is really not secure because it means higher profit margins. Often the consumer does not know the difference and ends up spending money for an inferior product which offers a false sense of security.

There is a vast difference in quality among laptop lock designs. If a consumer pays forty dollars for a lock from a company like HP, it would not seem unrealistic to believe that he should have a reasonable expectation of a certain minimum measure of quality and security. After all, the reputation of Hewlett Packard for engineering excellence cannot be questioned in many areas including

Tubular locks, unless specially designed, are inherently less secure than other forms of locking... [+]

computers, printers and test equipment, so nobody would question their competence in the design of laptop locks.

It has been more than six years since I looked at laptop locks and their security in depth. Because of increased corporate and government reliance upon these devices, my original disclosures about their insecurity received a great deal of media attention including the **New York Times.** As a result the industry, at least some of it, radically changed their designs and attention to critical components that could make the difference between a few seconds of protection and significant deterrence.

I thought it was time to survey the industry again, especially since I have been involved in laptop lock designs and received a **patent** to remedy one of the original problems: the ability to open many of these locks with a plastic pen.

So a few months ago I began obtaining samples from many manufacturers in the U.S., Asia, and Europe to test and to examine the current state-of-the-art. Given a number of recent **high-profile thefts** of computers and the resultant serious compromise of millions of individual identities, I thought this was a highly relevant topic, especially for those that travel with their laptops. What I found were many companies that are still peddling the same inferior and insecure products. Some of these locks are imported but branded by the manufactured as their own. I suspect this is what HP has done, although when I spoke with their tech support personnel in two different centers they stated that the locks were indeed manufactured by HP.

I called Hewlett Packard several weeks ago to ask about their model **BV411AA** and BV411UT locks that **sell for about $40** and are recommended by the company to protect a laptop. The individuals I spoke with at HP were quite insistent when I repeatedly asked them about the security of these locks. They told me that they could not be removed from a laptop without difficulty and that the computer would be destroyed in the

process. When I pushed the point with one of the extremely helpful technicians, he offered to send one of the locks for me to evaluate. This was after he told me that several different supervisors had concurred in what he was reporting: *there was no security problem with these locks*.

The lock arrived the next day and I was able to open it in seconds with a common screwdriver.

I attempted to contact HP by calling their corporate-level escalation unit in order to advise them that their locks were defective in design. That is when I ran into the HP bureaucracy machine. I was politely told that the company does not talk to the public and that "if you have something to tell us, then you will have to do it in writing." So I sent them an email. That was three weeks ago. Of course I have never received a response.

The tech that sent me a sample called the following week to ask if I would be placing an order. I told him that the locks had a serious security defect, could be opened in a few seconds, and that someone should call me. He said that he would route this to a product specialist who surely would follow-up. Nope. I guess the HP rule is still in place: they don't talk to customers the likes of me about such things! And incredibly, the technician I spoke with never asked me how I could open the lock he had sent to me and told me was so secure!

So, here is the problem: HP is selling a lock to protect your computer that can be opened in about fifteen seconds with a common 3" screwdriver with a plastic handle. Watch the video that my associate, Tobias Bluzmanis and I produced that demonstrates just how simple this is.

needed to move the pin to an unlocked state is a counter-force, just like Newton described.

It is the same theory that every pool player understands when a series of balls are on the table and touching each other in a straight line. If you strike the left-most ball, the one at the right will move. Only this time it is your computer that gets stolen, not the movement of pool balls. The net result: just about anyone can figure out how to remove one of these locks in seconds without a trace and, notwithstanding what I was told by HP, with absolutely no damage to your computer.

So you are the judge: is fifteen seconds of delay worth the $40 cost of this lock? More importantly, if you had purchased this product would you believe it was secure enough to protect your computer and everything in it? Of course you would because it “looked” good enough, and was sold by a respected company.

The problem is that designing locks is not one of HP's core businesses or within their expertise. I would imagine that someone in accounting decided they could save money by buying these cheap locks from offshore for a

The lock is struck at a certain angle with the head of the screwdriver and it opens. How is this possible?

Evidently the engineers at HP never heard of **Sir Isaac Newton**, the famous English Physicist, and his T**hird Law of Motion** which states that "for every action, there is an equal and opposite reaction." This is a really simple premise that every security engineer understands. The law is directly applicable to the design of the HP lock and explains why it can be opened.

In order to attach this cable lock to a laptop, the center portion of the locking cylinder is depressed which causes the extension of the scissor-locking system to engage with the Kensington security slot. This is simple, neat, and easy for the consumer. Unlike most other locks there is no need to use a key for locking (only for unlocking); just push, and the center of the lock moves inward against the computer until it clicks into a locked position. That "click" (and the way it is accomplished) is precisely the problem.

What the geniuses at HP failed to recognize or understand is that the real security of this design rested upon a spring-loaded pin that locked into place when the center of the mechanism was depressed by the user. All that is

couple of dollars and sell them for five times that amount. Unfortunately, the consumer may be left without a laptop because I can only assume that HP never bothered to do a security analysis on this product before offering it for sale.

There are many different lock designs, both key and combination, that are available in the marketplace. Corporate risk managers need to understand the differences, how these locks work, and which are vulnerable. In my next article I will explore specific designs and show how to defeat lots of them. It is incumbent upon anyone that relies upon these locks, especially in the commercial and government sectors, to understand how to evaluate them and to make sure that what you are buying is indeed secure. In the case of the HP models BV411AA and similar designs, they are not.

Marc Weber Tobias

Follow

I wear two hats in my world: I am both an investigative attorney and physical security/communications expert. For the past forty years, I have worked investigations, ... **Read More**