

ESO - Security Trends Report

12/09

McAfee warns about '12 Scams of Christmas'

November 21, 2009 ([cnet](#))

Retailers aren't the only ones gearing up for the holiday season. Criminals are also out in force.

To highlight the increased crime during the holidays, security company McAfee has come up with the "12 Scams of Christmas" ranging from bogus electronic greeting cards that deliver malware instead of cheer to fake charities that steal your money and your identity.

It's especially important to be extra careful this time of year, says McAfee's David Marcus. "The bad guys know people are spending more time online, they're paying more bills online so [the criminals] stand a chance of being a bit more successful this time of year.

In a podcast interview (scroll down to listen), Marcus counted down the 12 scams of Christmas starting with:

1. Charitable phishing scams: Marcus warns consumers to be wary of e-mails that appear to be from legitimate charities. Not only will they take your money and deprive charities of needed funds, but they will also steal your credit card information and identity.

2. Fake invoices from delivery services: During this period, scammers will send out fake invoices and delivery notifications appearing to come from Federal Express, UPS, the U.S. Postal Service or even the U.S. Customs Service saying that they were unable to deliver a package to your address. They ask you to confirm your address and give them credit card information to pay for delivery.

3. Social networking friend requests: Bad guys take advantage of this social time of year by sending out authentic looking friend requests via e-mail. Marcus recommends that you not click on those links but sign into Facebook and other services and look for friend requests from the site itself. Clicking on a link could install malware on your computer or trick you into revealing your password.

4. Holiday e-cards: Be careful before clicking on a holiday e-card, especially if it's from a site you haven't heard of. This is a way to deliver malware, pop-ups, and other forms of unwanted advertising. Some fake e-cards will look like they come from Hallmark or other legitimate companies, so pay close attention and make sure it's from someone you know. If you're going to send an e-card, be sure you're dealing with a reputable service lest you risk infecting yourself and your friends.

5. Fake "luxury" jewelry: If you see an offer for luxury gifts from companies like Cartier, Gucci, and Tag Heuer at a price that's too good to be true, it probably isn't true. These links could lead you to malware and take your money or merchandise that will probably never arrive (or be fake if it does). Some of these sites, according to McAfee, even display the logos of the Better Business Bureau.

6. Practice safe holiday shopping. Make sure your wireless network is secure and be sure you're shopping on sites that are secure. Though it isn't an iron clad guarantee, you should look for the lock icon in the lower right corner of your browser and make sure the Web page starts with https. The "s" stands for "secure."

7. Christmas carol lyrics can be dangerous: Bad guys know that people are searching for holiday related sites for music, holiday graphics, and other festive media. During this time, they create fraudulent holiday related sites.

8. Job search related scams: With the unemployment rate at 10.2 percent, there are plenty of job seekers looking for work. Beware of online offers for high paying jobs or at-home money making schemes. Some of

these sites ask for money up front, which is a good way for criminals not only to steal your "set up fee" but misuse your credit card too. Marcus said that some "get rich quick" sites are all about money laundering, asking you to accept an inbound financial transfer and pay them.

9. Auction site fraud: McAfee has observed a rise in fake auction sites during the holidays. Make sure you're actually going to eBay or whatever site you plan to deal with.

10. Password stealing scams: Criminals use low-cost tools to uncover passwords, in some cases planting key logger software to record keystrokes. Once they get your passwords, they gain access to bank accounts and credit card accounts and send spam from your e-mail accounts.

11. E-mail banking scams: A common type of phishing scam is sending out official looking e-mails that appear to come from your bank. Don't click on any links but type in your bank's Web address manually if you need to access your account.

12. Files for ransom: Hackers use malware to gain control of your computer and lock your data files. To access your own data you have to pay them ransom.

Bottom line--Don't let the egg nog and holiday cheer keep you from using your critical thinking skills when you go online during the holiday season. And, of course, make sure your operating system is updated and that you're using up-to-date security software.

Study finds 64 percent of websites contain serious flaws

[Greg Masters](#)

November 12, 2009

While a number of trusted sources continually decry the vulnerabilities present in web applications, this vector remains the primary avenue of attack for cybercriminals, according to a WhiteHat Website Security Statistics Report released on Thursday.

Despite metrics that substantiate the claims and any number of security best practices recommendations, many organizations, particularly those building custom web applications, are at risk, says the report, which measured data collected from Jan. 1, 2006 to Oct. 1, 2009, across more than 1,300 websites.

The problem is exacerbated because it is not possible to patch against custom web application software, such as that used by big e-commerce sites, Jeremiah Grossman, founder and CTO of WhiteHat, told SCMagazineUS.com. And that, he said, includes the vast majority of sites.

The amount of time it takes to repair a vulnerability once discovered is also an issue for those charged with maintaining network security. According to the WhiteHat report: "The time to fix should be as short as possible because an open vulnerability represents an opportunity for hackers to exploit the website, but no remedy is instantaneous."

Resolution could take the form of a software update, configuration change, or web application firewall rule, the report said.

But, the good news is that more organizations are repairing the technical issues associated with these threats.

"We have the answers and know how to fix these vulnerabilities," Grossman said. "The task is to motivate the business to do so. It's a matter of resource allocation."

As there are at least 24 different classes of web exploits, enterprises are under a lot of pressure to ensure their sites receive security checkups, said Grossman.

[Cross-site scripting](#) and [SQL](#) injection remain the top method of attack, while social networking and education sites are the top two verticals with the most vulnerabilities, according to the report.

"Taking application security seriously is more than just spending more – it is being strategic," the report said.

Among the sites examined by WhiteHat, only 36 percent were found to be free of any serious vulnerabilities. While they appear similar to those with vulnerabilities, these companies chose to fix any issues they've had, reducing the potential for attack, said Grossman.

Thirty years ago, criminals robbed brick-and-mortar banks, said Grossman. Today, every bank and company is equidistant to a cybercriminal.

"You can rob banks no matter where you are," he said.

Smartphones on Wi-Fi vulnerable to security attack

By John Cox

November 17, 2009 05:32 PM ET

Network World - A new report from a [mobile security](#) vendor details how the most popular [smartphones](#), including the iPhone, are vulnerable to man-in-the-middle attacks, carried out via public Wi-Fi connections.

According to the report by [SMobile Systems](#), smartphone users connecting to unencrypted Wi-Fi hotspots can be easily compromised by knowledgeable attackers using an array of existing tools. The authors of the study used those tools to intercept username/password combinations sent from several different smartphones

The tests used a laptop with software tools to intercept communications between smartphones connecting to a Wi-Fi access point, and then to bypass SSL. That information was then used to access a variety of e-mail accounts. The same information could be used to access an online banking account or other information.

Smobile tested the Nokia N95, HTC Tilt running Windows Mobile, HTC G1 running Android, and the iPhone 3GS with the latest firmware. In each case, the user would have had no idea that their information had been compromised.

Examples of the tools used are Arpspoof, which redirects packets from a target host on the LAN to the intended host on the same LAN, by forging Address Resolution Protocol replies to the target host; SSLStrip, to hijack HTTP traffic; Ettercap, a utility for sniffing, intercepting and logging; or Wireshark, a network protocol analyzer used as a packet sniffer. Another tool, webspay, lets the attacker sniff out and open any Web pages accessed by the victim.

"Utilizing this method, the attacker has effectively told the victim device to route all traffic through the attacker's machine [laptop], and the attacker machine then forwards the requests to the Wi-Fi hotspot." The attack computer captures all the traffic and can modify or kill active connections. With SSL bypassed, as soon as the victim accesses an e-mail or other account, the login credentials will appear in plain text on the attack computer.

The authors of the study warn smartphone users to "seek out and identify applications that provide adequate encryption technologies to protect confidential or private information." Applications for doing so exist, but are still rare, the authors note. The goal should be end-to-end encryption between the client application and the target server. Lacking that, users need to be aware that their information can be visible to a snooper.

For enterprises, the key issue is to treat smartphones with Wi-Fi as if they were corporate laptops with Wi-Fi. That means client security software, for firewall and antivirus.

Are nations paying criminals for botnet attacks?

By Ellen Messmer

November 17, 2009 01:03 AM ET

Network World - Nations that want to disrupt their enemies' banking, media and government resources don't need their own technical skills; they can simply order botnet attack services from cybercriminals.

That's a point made in McAfee's new report "Virtually Here: The Age of Cyber Warfare," which draws from the opinions of about 20 experts, including William Crowell, former deputy director of the U.S. National Security Agency.

There have been several larger denial-of-service attacks over the past few years that raised suspicions about whether they were initiated by nations in conflict against their adversaries. Such incidents include cyberattacks that hit Estonia and Georgia, which some viewed as traceable to Russia. More recently, many were tempted to blame North Korea for this year's July 4th [cyberattacks on South Korea](#) and [U.S. resources](#) (though others disagreed).

The McAfee report, prepared by Paul B. Kurtz, an analyst at Good Harbor Consulting, presents the opinions of diplomats, researchers and others about the nature of cyberattacks that seem concentrated on a specific country but where it's hard, if not impossible, to determine whether or not another nation-state initiated the attack.

One reason it may be hard to tell is simply because a nation state may go to the criminal underground to secretly pay for a massive botnet attack against its enemy. In this case, it's conceivable that the criminals themselves would not fully understand what they're being asked to do since the request and payment of botnet attack services are typically carried out as anonymously as possible, says Dmitri Alperovitch, vice president of threat research at McAfee.

"There is an overlap between cyberwar and cybercrime," Crowell points out in the report. "For instance, anyone can go to a criminal group and rent a botnet. We've reached a point where you only need money to cause disruption, not know-how, and this is something that needs to be addressed." The hacking skills of a criminal group may make them natural allies for nation states looking for a way to deny involvement in cyberattacks, it's noted.

The cyber warfare report points out that this year's July 4th cyberattacks against South Korea and the United States., in which North Korea was the suspected aggressor, showed that high-profile cyber events can have significant political repercussions. The report notes that by the end of that week, Rep. Peter Hoekstra (R-Mich.) "was stating publicly that the U.S. should conduct 'a show of force or strength' against North Korea for its alleged role in the attacks." The congressman expressed concern that unless the United States and allies "stood up to North Korea" there could be a next time when "they will go in and shut down a banking system or they will manipulate financial data" or that people could even get killed.

McAfee's Alperovitch says there is "no absolute proof" that North Korea had anything to do with the cyberattacks, but notes it was odd that the botnet was entirely concentrated in South Korea, something of a technical feat. Another unusual aspect of the situation with North Korea is that it gets its Internet link from China, Alperovitch points out, because North Korea never took ownership of the top-level domains assigned to it by ICANN.

Though no one seems to know for sure, the report concludes that if the attacks did originate with North Korea, one motivation could have been to test the impact of flooding South Korean networks and the transcontinental communications between the U.S. government and South Korea to disrupt military communications.

Meanwhile, some nations are known to be developing their own cyber defense and offense capabilities. According to the report, the nations that have the most sophisticated cyberwar capabilities are the United States, France, Israel, Russia and China. If a cyber conflict of real consequence heats up, businesses and individuals can be expected to be caught in the middle of it -- which suggests there should be much more open and public discussion about the issues around the world.

Cloud Security: Danger (and Opportunity) Ahead

In the first in his series of "Clearing the Cloud" columns, security expert Ariel Silverstone explores the dangers of cloud computing and outlines security best practices to make it work.

By Ariel Silverstone, CISSP

May 19, 2009 — [CSO](#) —

The dramatic change in the rate of adoption and the amount of discussion taking place regarding cloud computing demands that this technology, or rather a set of related technologies, continue to evolve utilizing a security-sensitive design.

We approach quickly the point in which the amount of data and of processing in the cloud will be not only unmanageable but also pose a security and related privacy risk to the users of the data, and to people who the data concerns.

In this series of articles, I do not intend to solve the problem of security in the cloud. My intent is to define the problem and propose several salient ways to address it. As always, comments are welcome.

Terminology

While the term "cloud computing" may be new, the idea certainly is not. Just look at the greatly varying definitions I found while researching this article. These include all of the following technologies:

- 1. The grid
- 2. VMWare and Xen-type virtual machines
- 3. IBM-type mainframes
- 4. Amazon-type flexible storage
- 5. Intel VTX-type hypervisors
- 6. Page files
- And many, many others

Instead of focusing on a specific technology, I propose we define the salient characteristics of cloud computing. For the purposes of this article series, I will define cloud computing as the technology having the characteristics of:

"Service-based data processing and storage capability which is flexible, extensible and virtual"

Some may add the following:

"and available via the Internet"

I will treat the second part of the definition as optional, for the purpose of discussing security. I find that the connectivity method here is secondary to the basic tenets of security, and thus am able to include locally virtualized machines in the discussion.

Generally, the purpose of cloud computing is to avoid the expense involved in building or acquiring the infrastructure. Similarly, when deploying virtual machines, one does not buy multiple servers or separate processors. I find the computing slice concept -- which includes storage, processing power, etc. -- to be a compelling one. In the near future, I predict that we will not even CARE whether the computing slice resides locally or across the world. As long as the computing service is provided in a timely and efficient manner, we will be satisfied.

When dealing with cloud-based delivery, the problem with security grows. Instead of having direct control over our concept of "defense in depth," we now have marginal control at best. Many times, such as with Amazon's EC2 service we have virtually no control, no pun intended. We sometimes do not have even the basic notification of something about to go wrong or something that has.

Both for Amazon's service and for our basic hypervisors, we no longer control ingress to the machine processing space. In the case of Amazon, it is Amazon's routers (and presumably firewalls). In the case of our virtual machine managers, we relegated the inter-memory systems and processes to the handling of a "black box," one that we seldom, if ever, have any control over. These are security problems and I also believe that these are legal problems. Allow me to explain.

What happens if and when data that we store or process on a virtualized machine gets compromised? Will we know? If WE do not know, how will we notify our constituents, especially when data breach notification laws are in place? How will we know to improve our security?

These are not idle words. If you look at the Amazon contract (and this is an example only, I do not wish to "pick on" Amazon, which I appreciate and respect), you will see the following sentences:

"4.3: We are not responsible for any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of, Your Content (as defined in Section 10.2), your Applications, or other data which you submit or use in connection with your account or the Services."

"7.2: We will have no liability to you for any unauthorized access or use, corruption, deletion, destruction or loss of any of Your Content or Applications."

What you do not see is that the provider accepts any responsibility or duty to inform the data owner, you, of any breach, notify you of any attempt, nor responds to any incident. The agreements are worded such that the customers' of Cloud computing bear all responsibility for such risks. It therefore appears that any law requiring breach notification, and any regulation or requirement, such as PCI, cannot be complied with.

Since the concern above is present, and understanding the incredible potential of cloud computing to improve the performance of IT foundation and infrastructure, we must find a solution, or a set of solutions, to standardize and address security concerns communicating to the cloud, within the cloud, and to data elements which reside therein.

In the next article, I will discuss the requirements for such solutions, and will include the excellent proposals brought forth from the Jericho Group and from the [Cloud Security Alliance](#). I will also issue a "call to action" for these and other organizations to address the issue of cloud security before the

technology become either unmanageable or, conversely, be seen as too risk-laden for corporations to use.

Clear Metrics for Cloud Security? Yes, Seriously

In the second installment of his series on "Clearing the Cloud," security expert Ariel Silverstone proposes some clearer definitions and metrics to improve cloud security.

By Ariel Silverstone, CISSP

November 17, 2009 — [CSO](#) —

Since publication of my first article -- [Cloud Security: Danger \(and Opportunity\) Ahead](#) -- it seemed new informations and cloud solutions were appearing daily. I'm gratified, for example, to see NIST, the National Institute of Science and Technology, has published its [15th draft on cloud computing](#), and with it, agreed with much of the definition I proposed in the previous article: "Service-based data processing and storage capability which is flexible, extensible and virtual."

NIST suggested cloud computing has the following salient characteristics: "On-demand self-service, based upon ubiquitous network access, using location-independent resource pooling; feature rapid elasticity and provide a measured service."

It's interesting to note that NIST specifically called out the piece about the service having to be measured. I wholeheartedly agree and take this to be a step in the maturity of cloud computing.

Security Models

[The Jericho Forum](#) proposed an interesting approach to cloud computing security. Starting with a description of cloud layers, it allows us to envision the problem. Here, the forum proposed that security (and identity management) are elements that cross all layers and in effect provide a design they call Collaboration Oriented Architecture (COA).

Once this foundation has been laid, they defined cloud security as a cube-shaped model that highlights various possibilities of architecture. The one addressed here is, of course, the outsourced/external/de-parameterized option. At about the same time, the Cloud Security Alliance, of which I am a member, designed a not-too-different view. The CSA broke down cloud computing into three delivery types:

- 1. Infrastructure as a Service (IaaS)
- 2. Platform as a Service (PaaS)
- 3. Software as a Service (SaaS)

And then proceeded to define the cloud consumption models:

- 1. Private
- 2. Public
- 3. Managed

- 4. Hybrid

The CSA's model of service delivery stacks, however, is very complicated. While I do not disagree with their reference model, I find it to be exceedingly complex. So allow me here to define the problem statement a bit differently. Let's expand the basic three tenets of security:

- 1. Confidentiality
- 2. Availability
- 3. Integrity

Clearly, in the case of cloud computing, and especially in the public/external case, we no longer have any control. Once the bits "leave our network," control passes elsewhere. Losing one control typically mandates an increase in the other controls. Here, we have another set of problems. Let us explore the remaining controls:

Confidentiality

Typically, we handle confidentiality through the use of technologies such as encryption and access control. We can still encrypt, but imagine what happens to a large data set. It has to be sent, or assembled, in the cloud, remain there in an encrypted form, and be transferred to us, for processing.

Once the data is at our location, we have to decrypt it, perform the operations needed, then re-encrypt and resend to the cloud. Doable yes. But the performance tax here is huge. While today's routers and servers no longer have their performance brought down to 1/6th by encryption, we still pay a heavy price.

One other element within confidentiality is the ability to destroy data. In a cloud that we do not own, and on storage media that we do not control, there is high probability that the same media be used for other purposes. These storage buckets are dynamic and the service/platform/application provider might allocate them to other users.

This sharing, and in many cases, repeated sharing, of storage media leads to the need for assured destruction. We must follow a strict regime that states how long is data to be kept, when and by whom destroyed, and how such destruction is verified. Since degaussing tapes and shredding CDs is out of the question, we must employ more agile software (or, dare we say hardware?) based methods to assure that destruction.

This question becomes infinitely more complicated when we consider that data at rest does not necessarily "rest" on a certain part of a certain hard drive. The data can, and usually does, move between storage locations on the drives. The onus is still on us to assure confidentiality, but we don't manage the drives. The only practical solution here is to demand regular scouring of storage media from the service providers. Do we think that such a requirement is feasible?

Finally, lest someone think I am only talking about the storage aspect of cloud computing, the above discussion is easily applicable to processing in a cloud as well.

Availability

When dealing with a cloud-computing resource, we are at the mercy of the network, the remote server, and whatever controls are applicable along the way, be they host- or network-related.

Yes, we always were at the mercy of such risks, but we owned them before. At what point does the enterprise take notice? As we can see from recent, published outages at Google and elsewhere, users are very sensitive to the information they require, and rightly so.

Even when taking steps to "assure" access, which in reality translates into reducing exposure to this particular risk, we have typically resulted to building redundancy into the system.

Here, that would presumably add lines, servers, networking equipment and personnel. Doable, but at what cost? What does the complexity of redundancy mean to an organization? What is the true cost of operations?

Let's look at an example: We have a volume of data which stretches at times by a factor of 10, so cloud computing seems like the perfect solution. So here is what may happen:

- 1. We ask the cloud service provider for an availability in data storage bursting. We will estimate this payment at 10 percent of our regular Cloud computing cost.
- 2. We ask our network services provider to create another redundant and highly-available path to the Cloud service provider. We will estimate that cost at 25 percent of our regular data communications cost.
- 3. And now we must consider what we are to do if such data-burst occurs when we have no availability to send it to the cloud. Are we going to dispose of it? Cease operations? No and no. So here we must plan for (at least) the storage of such data regardless whether we use cloud computing services.

Integrity

We can detect changes after they were made. From hashing to redundancy checks, from digital signatures to trip-wiring we are able to ascertain that a change occurred. But we can no longer prevent changes.

The bastion of defense-in-depth has crumbled when we talk about cloud computing. We do not own the moats, the walls, or the doors. Accepting data without verification should be unthinkable, verifying all inbound data will be complex and costly, adding yet another layer to the mix of technologies and methodologies that we must rustle.

Indeed, the cloud unchecked could lead to a wave of new attacks aimed directly at data whose guardians (by virtue of possession) are not incentivized to protect it from change, only mostly to be able to speed it on its way.

Cloud computing could be a goldrush to people designing man-in-the-middle attacks, too. While most hosting companies will boast of their monitoring and security, few, if any, can assure you that they have never been compromised. In fact, a provision of cloud data, with its already built-in doorway (or tunnel) to you, makes their life easier.

They can now both alter the data AND assure that it, and associated payloads, make their way to the intended destination.

So even if we are the best of meaning CIOs and the furthest thing from our mind is flouting the law, we are faced with a few obstacles in our way. Let's state some, in no particular order:

- 1. How do we comply with breach notification laws?
- 2. What happens if we have data regarding an EU national?
- 3. What must we do when we disclose risk information to Auditors? To the SEC?
- 4. How do we comply with rules relating to CALEA? E-Discovery? Data Forensics?

Lastly, we do remember that data has a lifecycle. Such DPLC mandates, ultimately, that the data be disposed off in a secure manner. Remember those Cloud-buckets? Well, these must be certifiably-erased when we are done with their utility. How do we do that in a Cloud?

If we remember the example we used above, authenticity of data is a problem that must be addressed.

Sometimes seen as a combination of non-repudiation, integrity and accountability, authenticity is a super-set that defines the reliability we assign and the trust we place in our data.

Should data in/from a cloud be seen as less-trusted data? If so, is there any worth to it? Would cloud end up being used only for data we could care less about?

Only time will tell.

Gov't executives cite unstructured data as top concern

[Angela Moscaritolo](#)

November 18, 2009

More than cloud computing, mobile devices and Web 2.0 applications, unstructured data is the cyberthreat federal government IT executives are most worried about, according to a survey released Wednesday by the Ponemon Institute and IT management software and solutions vendor CA.

In the [survey](#) of 217 senior IT executives from U.S. federal organizations, 79 percent said unstructured data – information not contained in databases – increases their organization's security risk. Unstructured data includes email and Word documents.

The common use of collaboration tools, such as SharePoint, also has caused an increase in the amount of stored unstructured data, which may contain confidential or sensitive information that is not always adequately safeguarded, Tim Brown, vice president and chief architect for security management at CA, told SCMagazineUS.com on Wednesday.

“They are worried that more data is being produced, more data is being shared and that data is not under the same control mechanisms they have had in the past,” he said.

Besides unstructured data, more than half of respondents were concerned about threats such as cyberterrorism, mobile devices, and Web 2.0 applications, the survey found. Seventy-one percent said the threat of cyberterrorism, defined as attacks intended to disrupt or harm a country or region, is on the rise.

In addition, 63 percent of respondents said mobile devices are a significant risk, and 52 percent said Web 2.0 applications contribute to the leakage of confidential or sensitive information and make an organization more susceptible to malware.

Cloud computing, on the other hand, garnered concern from 39 percent of respondents, the survey found. Brown said that as more agencies begin to implement on-demand technologies, he would expect cloud computing to worry more federal government IT executives.

FIVE GUIDELINES FOR SECURE CUSTOMER COMMUNICATION

DATE: NOVEMBER 24TH, 2009

AUTHOR: CHAD PERRIN

MAKE SURE YOUR COMMUNICATIONS WITH CUSTOMERS AND CLIENTS ARE SECURE. CHAD PERRIN OUTLINES FIVE GUIDELINES TO SECURE THE SENSITIVE DATA OF YOUR CUSTOMERS.

A ROCKY MOUNTAIN BANK EMPLOYEE ACCIDENTALLY SENT AN EMAIL CONTAINING SENSITIVE INFORMATION TO THE WRONG GMAIL ADDRESS. THIS VERY NEARLY RESULTED IN DISCLOSURE OF A CUSTOMER'S PRIVATE DATA TO THE WRONG PERSON. LUCKILY FOR THEM, PERHAPS, A COURT ORDER WAS ISSUED INSTRUCTING GOOGLE TO SHUT DOWN THE RECIPIENT'S ACCOUNT AND DELETE THE MIS-SENT EMAIL, PREVENTING THE INFORMATION FROM EVER BEING READ BY THE WRONG PERSON. UNFORTUNATELY, AN ENTIRELY INNOCENT THIRD PARTY — THE PERSON WHOSE EMAIL ADDRESS WAS SHUT DOWN — WAS SUBJECT TO SOME SERIOUS INCONVENIENCE FOR THE SAKE OF CLEANING UP THE BANK'S MESS.

NONE OF THIS HAD TO HAPPEN. THE WYOMING-BASED BANK'S DATA SECURITY POLICIES COULD HAVE PREVENTED THE PROBLEM, IF NOT FOR THE FACT THAT THOSE POLICIES ARE ABOUT AS INEFFECTIVE AS EVERY OTHER BANK'S POLICIES. THE QUESTION THAT NATURALLY ARISES IS: **WHY IS BANK SECURITY SO FAR BEHIND THE CURVE?**

WHY DO BANKS, UTILITY COMPANIES, AND OTHER ORGANIZATIONS THAT OFFER ONLINE SERVICES THAT DEAL IN SENSITIVE DATA NOT HAVE ADEQUATE SECURITY POLICIES IN PLACE TO GUARD AGAINST THESE PROBLEMS? WHY DO THEY NOT *AT LEAST* ALLOW USERS TO OPT-IN FOR SECURE MESSAGING VIA STANDARDIZED PRIVACY TECHNOLOGIES? WHY DOES THE CHASE ONLINE SITE FOR JP MORGAN CHASE BANK NOT ALLOW ITS CUSTOMERS TO LIMIT COMMUNICATIONS CONTAINING SENSITIVE INFORMATION SO THAT THEY WILL ONLY OCCUR OVER SECURE CHANNELS?

WHEN SPECIFYING YOUR OWN DATA PRIVACY POLICIES, PARTICULARLY AS THEY APPLY TO COMMUNICATING WITH CUSTOMERS AND CLIENTS OUTSIDE YOUR ORGANIZATION, THE IDEAL POLICY SHOULD INCLUDE THE FOLLOWING CHARACTERISTICS:

1. USE CRYPTOGRAPHIC DIGITAL SIGNATURES FOR ALL COMMUNICATIONS SO THEY CAN BE VERIFIED, EVEN IF THEY DO NOT CONTAIN SENSITIVE DATA. PUBLIC KEY ENCRYPTION PROTOCOLS SUCH AS OPENPGP ARE PERFECT FOR THIS.

IN THE CASE OF A MAJOR BANK, THIS ENSURES THAT EMAILS RECEIVED BY CUSTOMERS AND CLIENTS WITH THE ABILITY TO VERIFY DIGITAL SIGNATURES WILL KNOW THE DIFFERENCE BETWEEN A LEGITIMATE EMAIL AND A PHISHING EMAIL.
2. USE OPEN STANDARD ENCRYPTION PROTOCOLS TO ENCRYPT ALL COMMUNICATIONS THAT CONTAIN SENSITIVE DATA. AGAIN, PUBLIC KEY ENCRYPTION PROTOCOLS SUCH AS OPENPGP ARE PERFECT FOR THIS.

ENCRYPTED EMAILS WILL PROTECT CUSTOMERS AND CLIENTS FROM BOTH EAVESDROPPING, SUCH AS MAN-IN-THE-MIDDLE ATTACKS, AND PACKET SNIFFING ON LOCAL NETWORKS AND ACCIDENTAL LEAKS, SUCH AS THE ROCKY MOUNTAIN BANK EMPLOYEE'S MISSENT EMAIL — BECAUSE, EVEN IF THE EMAIL IS SENT TO THE WRONG PLACE, THE UNINTENDED RECIPIENT WON'T BE ABLE TO READ THE EMAIL.
3. REQUIRE CUSTOMERS OR CLIENTS TO USE DIGITAL SIGNATURES AND ENCRYPTION AS ABOVE, WHEN POSSIBLE, AND OUT-OF-BAND VERIFICATION OTHERWISE, BEFORE AUTHORIZING ANY CONTROL OVER THEIR ACCOUNTS.

A SECOND AUTHENTICATION FACTOR — OUT-OF-BAND COMMUNICATIONS — SUCH AS A TELEPHONE CALL OR A CRYPTOGRAPHIC DIGITAL SIGNATURE WILL SERVE TO IMPROVE VERIFIABILITY OF THE IDENTITY OF A CUSTOMER OR CLIENT SENDING ANY INFORMATION OR INSTRUCTIONS. WHERE DIGITAL SIGNATURES AND ENCRYPTION IN EMAIL ARE NOT PRACTICAL, DO NOT SEND EMAIL.

4. USE ALTERNATE SECURE CHANNELS, SUCH AS TLS-ENCRYPTED WEB SITES, INSTEAD. SNAILMAIL DOES NOT QUALIFY AS A SECURE CHANNEL.

UNFORTUNATELY, THE ANSWER TO ELINOR MILLS' QUESTION, "WHAT RECOURSE WOULD THE BANK HAVE IF THE DATA HAD BEEN SENT VIA REGULAR MAIL TO THE WRONG ADDRESS?" IS THE SAME AS IT EVER WAS. THE BANK'S RECOURSE FOR MISDELIVERED BANK STATEMENTS, CREDIT AND DEBIT CARDS, AND OTHER SENSITIVE COMMUNICATIONS WHEN THEY ARE SENT VIA THE U.S. POSTAL SERVICE HAS ALWAYS BEEN TO PRETEND THERE IS NOT A PROBLEM. YOU HAVE PROBABLY RECEIVED OTHERS' BANK AND UTILITY BILL MAILINGS IN THE PAST, IN FACT, AND KNOWN THAT NOTHING WOULD BE DONE ABOUT IT IF YOU DID NOT SEND THE MAIL BACK TO THE SOURCE.

5. WHERE A CUSTOMER OR CLIENT ABSOLUTELY DEMANDS THAT SECURITY FEATURES BE TURNED OFF OR AVOIDED FOR THE SAKE OF "CONVENIENCE", MAKE SECURITY THE DEFAULT, AND ONLY ALLOW AN OPT-OUT OPTION FOR DOWNGRADING SECURITY.

IT IS OF COURSE TRUE THAT MANY CUSTOMERS AND CLIENTS OF MANY ORGANIZATIONS WOULD NEVER STAND FOR THE SORT OF "INCONVENIENCE" REPRESENTED BY THE NEED TO EMPLOY SECURE COMMUNICATIONS TECHNOLOGIES. LET THEM OPT OUT. MAKE IT EASY, IN FACT, BUT MAKE IT A CONSCIOUS DECISION ON THAT PERSON'S PART, WITH A DISCLAIMER ATTACHED DETAILING IN BROAD STROKES THE KINDS OF SECURITY PROBLEMS THAT COULD RESULT. THEN, LET THEM LIVE WITH THEIR CHOICE. LET THE REST OF US, WHO ARE WILLING AND ABLE TO MAKE USE OF THE SECURITY TECHNOLOGIES CURRENTLY AVAILABLE, REAP THE BENEFITS.

GIVEN ENOUGH TIME, WITH ENOUGH ORGANIZATIONS TAKING THAT APPROACH, I THINK THE DEFAULT WILL BEGIN TO SWING THE OTHER WAY. EASE-OF-USE IMPROVEMENTS FOR PRIVACY TECHNOLOGIES, AND EASE OF ACCESS, WILL BOTH IMPROVE AS MORE AND MORE PEOPLE USE THEM — BECAUSE MORE AND MORE ORGANIZATIONS MAKE IT POSSIBLE TO USE THEM WHEN DEALING WITH THOSE ORGANIZATIONS. OF COURSE, THIS RELIES ON THE POSSIBILITY OF ORGANIZATIONS ACTUALLY CARING ENOUGH ABOUT THE PRIVACY AND SECURITY OF THEIR CUSTOMERS AND CLIENTS TO DO SOMETHING ABOUT IT.

EVEN IF *THEY* DON'T, *YOU* SHOULD. IF YOU ARE IN A POSITION TO OFFER YOUR CUSTOMERS AND CLIENTS A SECURE WAY TO COMMUNICATE, DO SO. IF THEY TURN YOU DOWN, SO BE IT, BUT IF THEY TAKE YOU UP ON THE OFFER YOU WILL HAVE HELPED TO MAKE MORE PEOPLE SAFE. MORE TO THE POINT, YOU MAY BECOME PART OF THE LONG-TERM SOLUTION TO THE UBIQUITY OF UNSECURE COMMUNICATION ON THE WEB. YOU KNOW WHAT THEY SAY ABOUT PEOPLE WHO AREN'T PART OF THE SOLUTION. . . .

Scammers get better tools for tapping social networks

Data could enable more targeted phishing, corporate surveillance

By Jaikumar Vijayan

November 30, 2009 09:18 PM ET

Computerworld - New tools capable of quickly finding, gathering and correlating information about individuals from social networking sites and other public sources are giving online scammers a powerful new weapon, say security researchers.

The tools allow potential attackers to build detailed profiles of individuals by finding and piecing together bits and pieces of information about them scattered on social sites and other public forums. The information can then be used in highly targeted, "spear-phishing" scams and other attacks against individuals and enterprises, they said.

Two companies providing such tools are Core Security Technologies Inc., with its Exomind application, and Paterva, with its Maltego product. Exomind is designed to find, combine and correlate information on individuals and groups of individuals from across multiple social networking sites. It can be used to build a concise portrait of an individual and to identify key relationships with others on social networks and in the real world, said Ariel Weissbein, head of CoreLabs, the R&D unit of Core Security.

Paterva describes Maltego as an open source intelligence and forensics application that can import and correlate data from almost any publicly available online source, including social networks, search engines and PGP key databases.

The application can be used to determine relationships and real-world connections between people, groups of people such as those in a social network, companies and Web sites. It can also be used to find links between domains, DNS names, IP addresses and even documents and files on the Internet.

For instance, the tools can be used to develop a list of Gmail users at the National Security Agency, find which NASA employees are using MySpace, or to attach e-mail addresses to phone numbers. A graphical user interface presents the information visually.

Paterva claims more than 5,000 users in the security, forensics and law enforcement industries. Maltego has typically been used in tasks such as mapping corporate and social networks and performing information footprints on corporations.

Exomind can also be used to profile the vocabulary that individuals use in their interactions with others on social networking sites, Weissbein said. The information can be used to impersonate a co-worker, business partner or customer -- right down to the particular vocabulary of that person.

"Exomind is a framework that allows us to do open-source intelligence over social networks," Weissbein said. It is a tool that can be used to understand, and then take advantage of, the trusted relationships that exist within a social networking site, he said. "It does not help anyone to compromise a system, but (it) provides you with tools to leverage trust relationships."

Exomind was developed to understand social networks' negative impacts on privacy, he said. "In general, by anticipating what bad guys can do and proposing counter-measures we help the larger Internet community."

Hugh Thompson, program committee chairman and a member of the RSA Conference Board, said that the intelligence that such tools can help gather from social and other sites poses an emerging risk for enterprises.

Employees can directly or indirectly disclose a lot of information about their companies on social sites that can compromise company information or security, he said.

For example, an employee suddenly changing social networking relationships, or new relationships between employees of two different companies could signal an impending partnership between the two companies. A Twitter message from Bentonville, Ark., about a meeting with a company headquartered there could signal a new or blossoming relationship with Wal-Mart, he said.

Similarly, a sudden increase in the number of job seekers from within a company could signal impending layoffs, Thompson said. "If you suddenly see people recommending a number of other people, it could mean they are hoping for some reciprocity, maybe because they are looking for a job," Thompson said.

"If you see this behavior from one person, that doesn't tell you much. But if you see it across five or 10 people who are all in the same group," that could be an indicator of a broader trend, he said.

The availability of such tools highlights the need for individuals to be especially careful about what they disclose on social networking sites.

The tools enable easier discovery -- and correlation of seemingly random bits of data -- to uncover previously undetected relationships and trends, he said. Even if users don't reveal sensitive data outright, they often reveal enough about themselves and their workplaces in different sites to enable a profile to be built, Thompson said.

"Nobody has really understood the risk of data being correlated" from across multiple sites in the manner enabled by tools like Maltego and Exomind, Thompson said. "People tend to put business-related things on LinkedIn but then have this weird mix of personal and business information [on sites such as Facebook.]"

Northrop Grumman launches cybersecurity research group

By Grant Gross

December 1, 2009 10:47 AM ET

IDG News Service - Government security contractor Northrop Grumman has joined with three leading cybersecurity research universities to launch a research consortium focused on fixing the most vexing problems in information security.

Northrop Grumman will distribute "millions" of dollars over more than five years to Carnegie Mellon University in Pennsylvania, Purdue University in Indiana and the Massachusetts Institute of Technology on projects to counter the most complex problems in cybersecurity, said Robert Brammer, chief technology officer of Northrop Grumman's information systems division.

The company created the Northrop Grumman Cybersecurity Research Consortium for two reasons, Brammer said at a press conference today in Washington. "First, the values of information services and systems have never been greater," he said. "Second, the cybersecurity threats also have never been greater."

Brammer called large-scale cyberattacks a "credible threat" in the coming years. "We require leap-ahead technology developments in order to improve the posture of our defenders," he added. "We need significant new technology developments, combined with improved security education, global standards, and understanding of security economics and psychology."

Northrop Grumman, which has worked on cybersecurity for 20 years, chose the three universities for their long-term, cutting-edge cybersecurity research, Brammer said. "No one organization has the capabilities necessary to address all cybersecurity threats," he added. "No matter how large and functional your organization is, it's certainly obviously true that most of the smart people in the world do not work for you."

The consortium will work on a number of projects, including dependable software analysis, secure computer design, next-generation secure networks, computer forensics and improved software, participants said.

Northrop Grumman plans to use the research to improve its own cybersecurity product offerings, which are tailored to government agencies. University researchers will be able to publish papers on their research and will own the intellectual property on projects solely developed at the universities. Northrop Grumman and the universities will share intellectual property developed jointly.

Participants said they hoped the consortium would help raise awareness of cybersecurity problems, in addition to providing useful research.

Cybersecurity problems are not new, said Eugene Spafford, executive director of the Center for Education and Research in Information Assurance and Security at Purdue.

"It's one that many of us have been warning about for nearly three decades," he said. "The problems have been anticipated and seen in advance. Unfortunately, none of the warnings have been taken seriously, particularly by government."

Instead of addressing problems proactively, many government agencies and private companies have been fixing cybersecurity problems after they have happened, Spafford added.

In some cases, universities have competed against each other for limited cybersecurity research dollars, Spafford said. He called the new consortium a "wonderful" opportunity for cybersecurity researchers to work together.

Group Offers Alternative to Cyber Regulations

Internet Security Alliance Suggests 9 Incentives to Secure IT

December 3, 2009 - Eric Chabrow, Managing Editor

The Internet Security Alliance, an industry group affiliated with Carnegie Mellon's cybersecurity laboratory, issued a report Thursday that argues that giving businesses incentives and not regulating them will better safeguard the nation's IT systems.

Entitled [Implementing the Obama Cybersecurity Strategy Via the ISA Social Contract Model](#), the ISA contends the process of developing effective regulations is inherently time consuming and that any regulations specific enough to assure improved cybersecurity would become outdated soon after their enactment.

The ISA report says cybersecurity is an enterprise-wide risk management that must be understood as much for its economic perspective as for its technical issues.

"Government's primary role ought to be to encourage the investment required to implement the standards, practices and technologies that have already been shown to be effective in improving cybersecurity," the 74-page report says.

ISA proposed nine incentives it contends could alter economic perspective with respect to investment in cybersecurity procedures, encouraging private entities to improve their security posture in the broad national interest:

Enact a Cyber Safety Act, patterned after the Safety Act that spurred physical development after the 9/11 attacks, by providing marketing and insurance benefits for companies that design, develop and implement of cybersecurity technology, standards and practices.

Tie federal monies - grants, Small Business Administration loans and stimulus and bailout money - to adoption of designated effective cybersecurity standards and best practices.

Leverage purchasing power of the federal government. Government could increase the value of security in the contracts it awards to the private sector, thereby encouraging broader inclusion of the level of security provided to government, which in turn could facilitate broad improvement of the cybersecurity posture among the owners and operators of the national critical IT infrastructure.

Streamline regulations and reduce complexity. Regulatory and legislative mandates and compliance frameworks that address information security, such as Sarbanes-Oxley, Gramm-Leach-Bliley, the Health Insurance Portability and Accountability Act, along with state regimes, could be analyzed to create a unified compliance mode for similar actions and to eliminate any wasteful overlaps.

Tax incentives for the development of and compliance with cybersecurity standards practices and use of technology. Tax credits can be made contingent upon compliance with established and pre-identified cybersecurity practices. Such incentives could encourage small and midsize businesses to implement cyber protections.

Provide grants and/or direct funding of cybersecurity research and development to companies that are developing and implementing cybersecurity technologies or best practices. Alternatively, R&D could be run through one or more of the federally funded R&D centers.

Limit liability for good actors. The government could create limited liability protections for certified products and processes or those certified against recognized industry best practices.

Create a national award for excellence in cybersecurity, akin to the Commerce Department's Malcolm Baldrige Award. Organizations may strive to receive the award as a means of differentiating themselves in marketing, particularly in a marketplace in which security concerns continue to increase.

Promote cyber insurance. Cyber insurance, if more broadly employed, could provide a set of uniform and constantly improving standards for corporations to adopt and to be measured against, all while simultaneously transferring a portion of risk that the federal government might face in the case of a major cyber event.

Besides incentives, the report also suggests ways to craft a new, practical model for information sharing; create an enterprise education program to properly structure industry; address the technical and legal disconnect created by digital systems; manage the global IT supply chain; and address the international nature of cybersecurity issues.

Security worries continue to dog cloud vendors

December 3, 2009 ([V3](#))

Half of all companies concerned about data leaks, say analysts.

Worries over security are severely hampering the adoption of cloud computing services, according a recent analyst report.

Research firm Forrester said that a recent survey revealed that roughly half of all companies, from small businesses to large enterprises, cited security worries as the primary reason for not adopting cloud services. Advertisement

Security concerns have long been one of the biggest issues with cloud services. The enterprise and government sectors have both expressed concerns about putting corporate data in the hands of third parties and remotely-accessed systems, while security experts have made cloud security a hot topic.

The cloud security sector itself has also grown as vendors seek to offer services and best practice guidelines to help improve data security on cloud platforms.

The Forrester study was performed as part of the firm's larger report on the state of emerging business hardware.

Analysts noted that, while cloud adoption is being hampered, technologies such as virtualisation and energy

management are seeing healthy growth and giving hope for an economic rebound in the IT space as a whole in the coming year.

"Despite the hesitancy about cloud computing, virtualisation remains a top priority for hardware technology decision-makers, driven by their objectives of improving IT infrastructure manageability, total cost of ownership, business continuity and, to a lesser extent, their increased focus on energy efficiency," said Forrester senior analyst Tim Harmon.

Cisco, Juniper gear vulnerable to hacking: U.S. govt

December 2, 2009 ([Reuters](#))

The U.S. government has identified flaws in equipment from four companies, including Cisco Systems Inc (CSCO.O), that hackers can exploit to break into corporate computer networks.

Technology

The Department of Homeland Security's U.S. Computer Emergency Readiness Team, US-CERT, said on its website on Wednesday that the warning applies to certain networking products from Cisco, Juniper Networks Inc (JNPR.K), SonicWall Inc (SNWL.O) and SafeNet Inc.

The flaw applies to equipment with technology known as SSL VPN that companies use to set up secure communications systems for safely accessing internal computer systems over the Internet.

It affects VPN systems run directly through a Web browser, rather than through software installed on a user's PC, which is more widely used.

Hackers who exploit the vulnerability could gain broad access to corporate networks, then steal confidential data, install malicious software or turn PCs into spam servers.

US-CERT's posting said the manufacturers have yet to develop a remedy for the problem, which government officials brought to their attention on September 24.

In the meantime, US-CERT researchers have developed three "workarounds" that they said minimize, but do not eliminate, the risk of an attack.

Barry Greene, head of Juniper's security response team, said his company has known of the vulnerability for several years and has urged customers to run the systems with workarounds in place.

"Our customers who follow the best common practice significantly reduce the risk -- to the point where they don't need to worry about it," he said.

SafeNet spokeswoman Donna St. Germain said her company had already devised a way to completely eliminate the risk and advised customers how to configure their equipment to do so.

The government agency said that SSL VPN products from other companies could potentially be at risk, though it has not tested them.

A spokesperson for Cisco said he could not immediately comment on the matter. SonicWall did not respond to a request for comment.

Many More Government Records Compromised in 2009 than Year Ago, Report Claims

Dec 2, 2009, By [Hilton Collins](#)

If you're bummed about the data in your department that just got breached, you have some cold comfort. Although the combined number of reported data breaches in the government and the military has dropped in 2009 compared to last year, many more records were compromised in those breaches, according to recent figures compiled by a California nonprofit.

As of Tuesday, Dec. 1., the Identity Theft Resource Center (ITRC) reported 82 breaches in U.S. government and military organizations. Although the year isn't over, that's fewer than the 110 that occurred in 2008.

But here's the catch: The breaches so far in 2009 have compromised more than 79 million records, whereas fewer than 3 million were hacked in 2008. A sobering upswing, to say the least.

The ITRC publishes data breach information on its [Web site](#), with updates coming most Tuesdays. The center publishes quarterly and annual reports on breaches in government and the military, and four other areas -- business, finance, health care and education. Breaches in government and military organizations are combined in the ITRC's tally.

Linda Foley, the center's founder and chairwoman, says the reported numbers show that government and military organizations need to be more vigilant about securing data when it's mobile.

"It's the same problem. Records are being exposed, so they're being hacked into; they're being lost; they're being put into laptops and carried around. Again, it comes back to, 'Why are they carrying information with them that they didn't need?'" she said.

The ITRC collects its data by mining breach reports that have been reported by reputable sources in news, television, radio and other media. Breaches are stratified into different categories; one breach can belong to more than one kind. They include accidental breaches, breaches caused by subcontractors, breaches caused by hackers, breaches caused by insider theft and breaches that occur when data is in the field. The report also records how many electronic records are compromised versus paper documents.

"I think what everybody needs to be doing across-the-board, No. 1 - encryption, or using a system that is not easily understood by someone who doesn't have a similar system," Foley advises.

She also recommends that government and military agencies centralize their information so it can be tracked and secured more easily.

The overall number of breaches across all sectors in the Dec. 1 data is 461 cases and about 222 million compromised records. The total number of breaches for 2008 numbered 656 and more than 35 million compromised records.

Social network and banking scams are on the rise, says Cisco

By **Robert McMillan**

December 8, 2009 04:17 AM ET

IDG News Service - What do phishing, instant messaging malware, DDoS attacks and 419 scams have in common? According to Cisco Systems, they're all has-been cybercrimes that were supplanted by slicker, more menacing forms of cybercrime over the past year.

In its [2009 Annual Security Report](#), due to be released Tuesday, Cisco says that the smart cyber-criminals are moving on.

"Social media and the data-theft Trojans are the things that are really in their ascent," said Patrick Peterson, a Cisco researcher. "You can see them replacing a lot of the old-school things."

Peterson is talking about attacks such as the Koobface worm, which spreads via Facebook and Twitter. Koobface asks victims to look at a fake YouTube video, which ultimately leads to a malicious download. Cisco estimates that Koobface has now infected more than 3 million computers, and security vendors such as Symantec expect social network attacks to be a major problem in 2010.

Another sneaky attack: the Zeus password-stealing Trojan. According to Cisco, Zeus variants infected almost 4 million computers in 2009. Eastern European gangs use Zeus to hack into bank accounts. They then use their networks of money mules to wire stolen funds out of the U.S. They have been linked to about \$100 million in bank losses, some of which have been recovered, the U.S. Federal Bureau of Investigation [said last month](#).

With that kind of success, older types of attacks such as instant messaging worms and phishing are now on the decline, Peterson said.

Traditional phishing is becoming harder as consumers become wary of suspicious banking sites and the banks themselves are now adept at getting these sites taken off the Internet.

Those factors make password stealing Trojans like Zeus even more popular, Peterson said. "They're focusing on other ways to basically accomplish the same thing."

One scourge that's not slowing down, however, is spam. Cisco expects spam volume to rise between 30 and 40 percent next year, even though countries such as the U.S. have knocked some spammers offline. In fact, U.S. spam dropped 20 percent in 2009, and the U.S. lost its traditional position as the world's number-one source of spam. More spam now comes from Brazil, Cisco says.

New cloud-based service steals Wi-Fi passwords

By Robert McMillan

December 7, 2009 05:02 PM ET

IDG News Service - For \$34, a new cloud-based hacking service can crack a WPA (Wi-Fi Protected Access) network password in just 20 minutes, its creator says.

Launched today, the [WPA Cracker](#) service bills itself as a useful tool for security auditors and penetration testers who want to know if they could break into certain types of WPA networks. It works because of a known vulnerability in Pre-shared Key (PSK) networks, which are used by some home and small-business users.

To use the service, the tester submits a small "handshake" file that contains an initial back-and-forth communication between the WPA router and a PC. Based on that information, WPA Cracker can tell whether the network seems vulnerable to this type of attack.

The service was launched by a well-known security researcher who goes by the name of Moxie Marlinspike. In an interview, he said that he got the idea for WPA Cracker after talking to other security experts about how to speed up WPA network auditing. "It's kind of a drag if it takes five days or two weeks to get your results," he said.

Hackers have known for some time that these WPA-PSK networks are vulnerable to what's called a dictionary attack, where the hacker guesses the password by trying out thousands of commonly used passwords until one finally works. But because of the way WPA is designed, it takes a particularly long time to pull off a dictionary attack against a WPA network.

Because each WPA password must be hashed thousands of times, a typical computer can guess perhaps just 300 passwords per second, while other password crackers can process hundreds of thousands of words per second. That means that the 20-minute WPA Cracker job, which runs 135 million possible options, would take about five days on a dual-core PC, Marlinspike said. "That has really stymied efforts of WPA cracking," he said.

WPA Cracker customers get access to a 400-node computing cluster that employs a custom dictionary, designed specifically for guessing WPA passwords. If they find the \$34 price tag too steep, they can use half the cluster and pay \$17, for what could be a 40-minute job. Marlinspike declined to say who operates his compute cluster.

The attack will work if the network's password is in Marlinspike's 135 million-phrase dictionary, but if it's a strong, randomly generated password it probably won't be cracked.

The service could save security auditors a lot of time, but it will probably make it easier for senior management to understand the risks they're facing, said Robert Graham, CEO of penetration testing company Errata Security. "When I show this to management and say it would cost \$34 to crack your WPA password, it's something they can understand," he said. "That helps me a lot."