

If You Cannot Prevent It, Detect It: Why Defense In Depth Works

As audit season is finally over, (over 65% of all our assessments and audits happen in Q4) we finally have a chance to grab a cup of coffee and look back at a couple trends in 2011 that we think separate the best security teams from the worst.

First, we need to discuss how we measure the quality of a security team. At Savid, it is pretty simple. Since we perform ethical hacking to assess security programs at organizations, if we got access to something we shouldn't have, it counts as an intrusion in our books.

Most reviews of security controls look at what went wrong because it's harder to learn from the successes. So let's get the major failures of 2011 out of the way and then let's talk about what our best clients did to prevent us from breaking in. Overall, most of the security programs we assessed had application security issues. However, 2011 was the worst we have ever seen in terms of the depth and breadth of application security issues - even though the majority of the security programs we tested were in compliance with regulations such as HIPAA, PCI, and GLBA.

Ok, so with that out of the way, what did the best security teams do to prevent our ethical hackers from breaking in? One Thing: Defense In Depth.



2011 was the first year where we saw significant advancements in defense in depth deployments among our clients. For example, we saw a noticeable increase in proper system hardening (using standards such as CIS and NIST) and reduction of excessive permissions that stopped our attacks cold.

Properly deploying defense in depth can be the distinction between a data breach requiring notification or a simple documented incident. The difference between the two for some organizations could be millions of dollars. Oh, and it also has a side effect of making most malware non-functional by preventing the malware from creating temporary files, accessing DLLs, etc.

Continued on page 2

How To Securely Use The Cloud

Gartner, the largest IT research firm in the world, is predicting that 2012 will be the year that more than 50% of Global 1,000 companies store customer data in a public cloud – a 30% increase from 2011. Of course, these firms have compliance and regulatory concerns which should make you ask how are they putting potentially sensitive data into a public cloud? Sadly, the answer isn't some amazing new technology it's actually technology that was developed in Egypt circa 1900 BC – encryption.

Encryption As A Service (EaaS) or "cloud encryption" as it is commonly called is being used by more and more global firms to enable them to leverage large public cloud vendors such as Salesforce, Amazon, and even DropBox. Cloud encryption isn't really new, it hit the security industry scene in 2008 but more vendors, lower prices, and simpler implementation capabilities has put it into the list of "technology to learn about" for most CIOs and CSOs. Let's discuss how these cloud encryption services work.

First, there are multiple types of cloud encryption. Some vendors offer encryption for virtual machines that run at cloud providers such as Amazon's EC2 or Rackspace. Other cloud encryption vendors provide application level encryption by being an API proxy. For example, services such as Salesforce and Google Apps instead of storing a credit card number in plaintext in a field at Salesforce.com, the encryption proxy at your company's data center encrypts it first and Salesforce.com stores the encrypted value instead of the plaintext. Lastly, some cloud encryption vendors provide file based encryption where individual files are encrypted and the names encrypted instead of encrypting the actual storage.

Regardless of the cloud encryption approach, you might notice a trend. Cloud encryption technologies are really just "cloud" versions of the same technologies that have been in use at data centers worldwide such as Full-Disk Encryption, Database Encryption, and File Encryption. The difference is that these cloud encryption vendors solve one problem that plagues organizations – staying up to date with the data sources and destinations the encryption technology works with.

continued on page 2

Inside this Issue

If You Cannot Prevent It, Detect It: Why Defense In Depth Works	—1	Monthly Special	—2
How to Securely Use The Cloud	—1	The CEO Corner	—2
Stay Safe While Shopping Online	—3	<i>Michael Davis shares his thoughts</i>	
		Events	—3

Stay Safe While Shopping Online



As we all know, online shopping is nothing new but as its popularity continues to grow so does the malicious threats that can occur during your shopping experience. That is why we want to provide you with some reminders and tips on how to make you're online shopping a safer experience. We also encourage you to share these tips with your family who may make online purchases too.

There are a few simple precautions you can take to further secure yourself before you make your online purchases. First make sure you have a web filter in place that will warn you of suspicious websites. Keep your web browsers up to date too. Often times the site you are shopping on is legitimate but if your computer is infected with keyloggers and other malicious viruses you can run the risk of your credit card data being stolen.

It is always best to shop at familiar websites but if you are looking at products or services from an unfamiliar sight do a little research before you begin; find out what other consumers have to say about the store or seller. Epinions.com and BizRate.com give customer evaluations that may help you determine the legitimacy of the company. It is also a good idea to review the website for the BBB and or TRUSTe approval icons. Be sure to

click those icons to ensure that they take you to those accredited sites and that you can find the companies name within their listings. Often times harmful sights will display the graphic with no link so be aware.

Remember, before entering your personal data and credit card information check the connection of the website out to make sure it is encrypted. The URL will start with (http"s") and also look for the padlock icon in the address bar or right corner of the window. Be aware of any warnings that your computer gives you regarding the security certificate of the site, when in doubt find somewhere else to shop.

Keep in mind when choosing a payment method it is always best to use PayPal if it is an option, that way your credit card and bank account information will not be shared with the merchants and sellers. PayPal will also protect you against fraudulent charges and if there are problems with your purchases. Once your purchases are made it's always a good idea to check your bank accounts and credit card statements to ensure the proper amount was charged; if the charges are wrong contact the website where your purchases were made immediately along with calling your Credit Card Company to inquire about a "charge back".

We hope that by keeping these tips in mind that you will continue to enjoy shopping online and are more secure in doing so.



Monthly Events

Jan. 19th, Data Connectors, Chicago

Attending Data Connectors this year? Stop by our booth and sign up to win fun gadgets and a chance to win big prizes. VIP Cocktail Hour following Conference at Bar Novo inside the Hotel featuring complimentary drinks & hors d'oeuvres with an exclusive raffle prize. Join us at the Renaissance Chicago Downtown Hotel at 1 West Wacker Drive, Chicago, IL

Feb. 23rd, Privileged Identity Management Webinar

Join us for this webinar and learn how to securely manage shared privileged accounts. To register for this event use this link: <http://www.savidtech.com/savid-events>

On-Demand Webinar: How To Managed And Secure Your Mobile Devices

Stop fighting between Apple, Google, and RIM! Learn how to manage and secure the growing number of mobile devices in your organization including iPhone, iPad, Android, Blackberrys, and more. Watch this anytime at the comfort of your own desk by using this link: <http://mcaf.ee/zewfk>

On-Demand Webinar: Virtualization Security in the Real World

This on-demand webinar discusses the current issues in securing virtualized environments, what to look out for, and what really works in reducing the risk of attacks within a virtualized environment. To watch, simply use this link: <http://mcaf.ee/dpqt6>





savidtechnologies

18470 Thompson Ct. Ste. 2B
Tinley Park, IL 60477

Comprehensive Knowledge. Delivered.

Take a Break!

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



"We don't need to worry about information security or message encryption. Most of our communications are impossible to understand in the first place."

Follow Us On

Get exclusive content, informational videos, and details on our upcoming events .



<http://www.facebook.com/savidtech>



<http://twitter.com/savidtech>



<http://www.savidtech.com/blog>

Monthly Trivia

Be the first to email us the correct answer and win a \$20 Starbucks Gift Card!

Find the one-word name of a well-known magazine hidden in each sentence

Example: Whenever I search the web on your computer it takes a long time.

Answer: EBONY (WEB ON Your)

Crash won the Oscar for Best Picture

Betamax immediately became obsolete when VHS arrived.

Katz's Delicatessen cemented its reputation long ago.

That's not what I meant!

Frank shared Booker T. Washington's views on economic matters.

Email your answer to: info@savidtech.com and look for the winner listed in next months newsletter
Congratulations to Jim Coons our last trivia winner.

Be our



Guest

**Data Connectors Chicago
Tech-Security Conference
& VIP Cocktail Hour**

**January 19th
8:15am-6:00pm**

**Renaissance Chicago
Downtown Hotel**

RSVP Here Today!
http://savidtech/vip_guest

Joke of the Month

"I needed a password eight characters long so I picked Snow White and the Seven Dwarves."

~ Nick Helm

Got a funny joke? Send it to us at info@savidtech.com and we may include it in an upcoming issue.