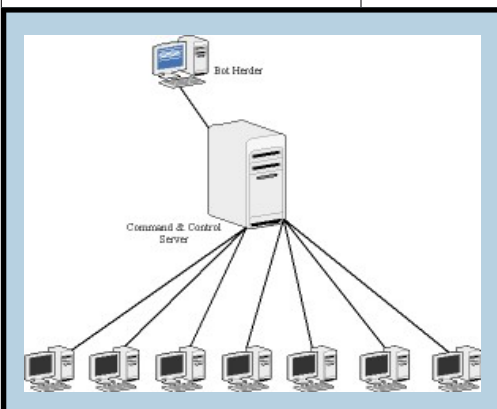


JJS I.T. NEWS

INSIDE THIS ISSUE:

Unique Excel Entries	2
Pythonology	2
Multifactor Auth	2
TPM	3
Leadership	3
Cartoon	4
Website Safety	4

Information Technology is a tool for productivity. Our overarching goal in I.T. is to *proactively contribute to the company's success.*



OUR NEW WEB PORTAL IS HERE!

The new Sheeran Web Portal went into production on October 6th! What makes it a Web Portal, instead of a regular Web Site? According to Wikipedia, web portals “present information from diverse sources in a unified way”. This is a little more dynamic than a typical web site that just serves up web pages.

On our web portal, we include an ecommerce module for web ordering, a reporting module for inventory control, an email support module, online documentation, and upload/download functionality. It is modular, so that new features can be added without a ton of web development. Our next module will include graphical reporting with FusionCharts!

One of the most important challenges of creating the web portal is balancing simplicity of design with flexibility for future needs. Our IT department worked hard to ensure that the overall design was simple enough to manage internally, while making it robust enough to meet our future needs. “Future needs” in this way means the ability to easily meet the needs of most clients – both

current and future. This sounds much easier than it actually is!

What all can a web portal do? Here is a list of just some of the features we hope to implement in the future:

- Online payments
- Online price quotes
- Submit mailing & printing jobs
- Project tracking & status
- Newsletter & mailing sign-ups



Have an idea for the web portal? You can submit ANY ideas through the bugzilla system by selecting IDEAS after clicking ‘New’ bug!

ARE BOTS TAKING OVER THE NET?

I’ve seen two stories in the past few months about botnets, which prompted me to include the topic here. The good news is: botnets are being infiltrated by the good guys. The bad news: there are too many bots out there.

If you’ve sat in on any of my training seminars, you already know a little about botnets. Here’s a quick summary:

A botnet is a collection of bots (robots) that can be controlled remotely. They are installed via worms, Trojans, or backdoors and can be used to send spam, click-through fraud, adware/spyware, and for distributed denial-of-service

(DDoS) attacks.

It is estimated that one quarter of all personal computers connected to the Internet are part of a botnet.

Dutch police found a 1.5 million node botnet, but most botnets are estimated at 20,000 nodes. At this time, many botnets are scaling back in size in order to prevent detection.

The Kracken botnet is the worlds 2nd-largest (as of April 2008) and is believed to have infected at least 50 of the Fortune 500 companies.

Preventative measures? Everything you already know – don’t click on unknown links, don’t visit questionable web sites, use web filtering software, keep systems patched, don’t user your computer when logged in as administrator – in a nutshell, practice safe Internet usage :)

DE-DUPE ENTRIES IN EXCEL COLUMN

To generate a list of unique entries from a column in Excel, use Data | Filter | Advanced Filter. Here are the steps:

- First, highlight the column you wish to extract the unique entries from.
- Click 'Data', 'Filter', 'Advanced Filter' and select the 'Copy to Another Location' option. Type the new location column in the "Copy To" field (ie: D1).
- Check the "Unique Records Only" checkbox
- Click OK

Excel will copy the unique entries from the source column to the new location, sorted alphabetically.



Just Wing It

People often spend too much time up front trying to solve problems they don't even have yet.

Don't.

Don't sweat stuff until you actually must.

— excerpt from "Getting Real" (The smarter, faster, easier way to build a successful web application)
by 37signals.com

PYTHONOLOGY

This month marks the anniversary of Monty Python's Flying Circus. On Oct. 5, 1969, the first episode aired on BBC One. The six Brits from the original series have highly-educated backgrounds. In fact, Graham Chapman qualified as a medical doctor, but never entered practice. The others have degrees from Oxford or Cambridge.

Of course, there is no actual Monty Python person. However, the name has become a part of the English lexicon and until recently, was associated with either the python snake or the comedy of Monty Python.

To a computer geek like me, python represents a programming language and pythonology is the use of the python programming language to produce better, faster

software (really, I'm not making this up). Check it out for your self at: pythonology.org.

My first use of python was earlier this year in my CompSci programming class at Albright. Since then, I've written quick little python programs to solve some complicated work problems, including the expanding of variable kit components into the proper number of unique kit combinations (using recursive factorials!).

Python is one of the programming languages used within the Google search engine and is used throughout the web to drive complex web applications.

MULTIFACTOR AUTHENTICATION

Computer authentication refers to the process of proving that you are who you say you are. For example, I can say I'm Lori Homsher, but how does the computer know the real me from someone who is using my logon name?

In the security world, there are various *factors* of authentication that we can use to attempt to prove an identity. The more factors used, the more confidence we have in the results. Here are the most common factors:

- Something you know - this is the typical username/password combination, or PIN.
- Something you have—can include a security token, cell phone, ID card, etc.

- Something you are—this is biometrics: fingerprint/retinal/facial scan, voice recognition, etc.

There may be other factors as well, such as "someplace you are" and challenge/response factors. When two or more factors are combined for security, it is called 'multifactor authentication'.

Something you know (username/password) is the most common, but is considered fairly insecure in today's environments. It's even worse when the username is based on public information, such as name or email. Most banks and other online industries are moving to 2-factor authentication (or higher).

TRUSTED PLATFORM MODULE

TPM is a hardware component built into PCs and laptops for enhanced security. It offers good security against common attacks, but hasn't had widespread use.

Encryption keys are stored on the TPM chip, which can be used for disk encryption, or for user/machine identification. The most common use at this time is full-disk encryption (BitLocker can use TPM), but identification may be what brings TPM into common use.

TPM can support multifac-

tor authentication (see related article, page 2), combining identification with a PIN or biometric scan. The result is that TPM is able to provide secure authentication for web and business applications.

Web applications are a little tricky, since they're accessible from any PC. However, using a temporary password sent to a user's cell phone may authenticate the user, while the TPM process establishes the trusted connection between the PC being used and the web application. In

this way, a web application can establish a trust relationship with the PC, even if the PC is not the user's normal machine.

TPM includes Digital Rights Management (DRM) technology and has been criticized by privacy groups and people concerned with fair-use rights for copying and sharing digital content (music & videos). At this time, TPM is seeing only lukewarm acceptance among security folks, while privacy groups are openly criticizing it.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."

— Bruce Schneier

Who is Bruce Schneier?

He is an encryption expert who is "the closest the security industry has to a rock star", according to his latest book. Here are some Bruce Schneier facts, Chuck Norris style:

Bruce Schneier's secure handshake is so strong, you won't be able to exchange keys with anyone for days.

Bruce Schneier doesn't need steganography to hide data in innocent-looking files. He just pounds it in with his fist.

If Bruce Schneier wants your plaintext, he'll just squeeze it out of the ciphertext using his barehands.

Bruce Schneier eats 0s and 1s for breakfast. And snacks on pi.

Bruce Schneier's discrete logarithms are uncountable and continuous.

Check out his blog at: www.schneier.com/blog

LEADERSHIP FROM THE PEANUT GALLERY

From "Lead Now, Get Promoted Later", myleaderscompass.com

How can you act like a leader now, even when you're working in the peanut gallery? Most of us are not in leadership positions, but that shouldn't stop us from acting like leaders. It's easy to be critical of leaders — in any given newspaper you can find people complaining about our government leadership. But leadership is harder than it looks. The good news is, it can be practiced by anyone, regardless of your current position.

Here are a few leadership tips from MyLeadersCompass.com:

- Offer solutions: True leaders don't stand around waiting for problems to fix themselves. See a glitch, propose a solution.
- Demonstrate integrity: When things get tough, people want to work for and alongside people they trust. Do what you say you're going to do. Align your words and your actions.
- Make your peers better: One of the responsibilities of a leader is to make the organization better. Find ways to help your peers succeed and you're already accomplishing a leader's mission. Share what you learn and invite others to do the same.

- Sharpen your communication skills: Leaders spend a lot of time communicating with other people. Practice being an excellent communicator. Don't shy away from difficult conversations. Practice writing clearly. Most people fear public speaking. If you're not good yet, find a course, or ask someone who is good to help you.
- Act like a leader: Stop whining. Look out for your own development and seek opportunities. Take on a challenge or do something scary. Stepping outside your comfort zone is the best way to increase the size of your comfort zone.
- Catch people succeeding: Every employee wants to succeed. A leader's job is to catch people succeeding. When you see someone doing a good job, point it out. Success is contagious!

Ruggero, Ed (2008, April 29). Lead now, get promoted later. Retrieved May 22, 2008, Web site: <http://myleaderscompass.com/?p=24>



Sheeran Direct Marketing
71 Southgate Blvd
New Castle, DE 19720
Phone: 302.324.0200
Fax: 302.324.0213
www.jjsheeran.com

Editor: Lori Homsher
Email:
lhomsher@jjsheeran.com

"NOT SAFE"

REMEMBER THAT A LOCK IMAGE INSIDE THE PAGE DOES NOT MEAN SECURITY!

LESSON:

1. LOOK FOR AN SSL LOCK IN THE BROWSER FRAME.
2. ALWAYS LOOK CAREFULLY AT THE WEB ADDRESS.

Copyright 2008. Srikanth & Jakobsson. SecurityCartoon.Com

THIS IS THE NAME OF THE COMPANY (ALSO CALLED THE "DOMAIN"). IT IS NOT BARNES & NOBLE.

A LOCK INSIDE THE CONTENT OF A PAGE IS JUST A PICTURE!

THIS IS JUST A PICTURE... DOES NOT MEAN A SECURE CONNECTION.

Reproduced with permission. Please visit www.SecurityCartoon.com for more material.

WEBSITE SAFETY

Calvin: You can't just turn on creativity like a faucet. You have to be in the right mood.

Hobbes: What mood is that?

Calvin: Last-minute panic.

We've all received email that asks us to update our accounts. If you receive an email from Paypal or eBay, but are not a customer of those companies, it is easy to recognize these as phishing attempts. However, what if you visit a web page and are asked to update your profile information? Is there a way to identify whether the page is legitimate and not the result of a pharming attack, web hijack, or DNS poisoning? Actually, there are several details you can look for to help you analyze the legitimacy of a web page:

- First, look at the URL in the address field. The domain name should match the company in some way. In the cartoon example above, the domain is password-update.com, which has nothing to do with Barnes and Noble.
- Also in the address line, look for the protocol of https. This indicates the site is using SSL, which includes a certificate issued to the company and SSL encryption of all data sent to their server.

Extended Validation) is now available that will cause the URL (address link) to be color-coded in green (green = good) . If you see the green address bar, it means the site is not fraudulent.

- The "secure sign" lock must be in the bottom right corner of your browser FRAME, not on the web page itself. Anyone can put a picture of a lock in a web page. However, only SSL-signed sites get the lock in the lower right corner of the browser frame.
- Site Seals—there are several site confirmation seals out there – including SiteSafe and WatchDog. We added WatchDog to our web portal as an automated, proactive way to scan the site for performance and vulnerability problems.

The best rule for web site use is this: if you have any doubt about the validity of a web site, don't risk it!

- A new form of SSL certificate (EV–