Colleagues, as the first quarter of the year ends I want to thank you for all the support you are providing to the chapter. For those who were not able to make the Spring Conference at the University of Colorado in Colorado Springs (UCCS), we had over 210 attendees, seven (7) paying sponsors, and some really good briefings and demonstrations. I think most attendees would say the event was a success...at least I hope the attendees think that. Please let the board hear your feedback on what you liked and what you would like to see changed.

While we were successful getting sponsors for the conference, we’re not having that same success for monthly meetings so the April meetings will cost each member $10 and the chapter will pick up the rest. We are reaching out to dozens of companies asking them to sponsor our meetings but that hasn’t been an easy sell thus far and while several are saying they are interested, their companies are not putting forth the funding yet. In the meantime, we have a lot of very smart people in this chapter who are more than willing to share some of their knowledge with the membership at large so we’re going to be calling on those members to do this as needed. Whether we have a sponsor or not, the board will work diligently to ensure learning is taking place at every meeting we hold so in addition to members, we will also reach out to other individuals and organizations to come speak to us on relevant and interesting topics.

Let me talk about another success area for the chapter and that is Membership. Kudos to Dave Reed (Membership Chair) and Cindy Thornburg (Chapter Vice President) for their efforts to reach new people and retain current members. As I am writing this we have had 19 new members’ sign up in March bringing our membership total to 370 people. That’s really good news and we want to ensure we continue to reach out to the community at large and recruit members. We also want to ensure we are providing a service that our members covet so current members will remain with us and also decide they want to play a more active role. While larger numbers of people are great, in order to reach our goal of providing outstanding training and education to our members we need more help. We have many roles in this

(Continued on page 3)
"In the future, people won’t be confined to their meatspace bodies."

**20 Crucial Terms Every 21st Century Futurist Should Know**

By George Dvorsky, io9, March 17, 2014

The National Security Agency has built a surveillance system capable of recording “100 percent” of a foreign country’s telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place, according to people with direct knowledge of the effort and documents supplied by former contractor Edward Snowden.

We live in an era of accelerating change, when scientific and technological advancements are arriving rapidly. As a result, we are developing a new language to describe our civilization as it evolves. Here are 20 terms and concepts that you’ll need to navigate our future.

Back in 2007 I put together a list of terms every self-respecting futurist should be familiar with. But now, some seven years later, it’s time for an update. I reached out to several futurists, asking them which terms or phrases have emerged or gained relevance since that time. These forward-looking thinkers provided me with some fascinating and provocative suggestions — some familiar to me, others completely new, and some a refinement of earlier conceptions. Here are their submissions, including a few of my own.

1. **Co-veillance**

Futurist and scifi novelist David Brin suggested this one. It’s kind of a mash-up between Steve Mann’s sousveillance and Jamais Cascio’s Participatory Panopticon, and a furtherance of his own Transparent Society concept. Brin describes it as: "reciprocal vision and supervision, combining surveillance with aggressively effective sousveillance." He says it’s "scrutiny from below." As Brin told io9:

Folks are rightfully worried about surveillance powers that expand every day. Cameras grow quicker, better, smaller, more numerous and mobile at a rate much faster than Moore’s Law (i.e. Brin’s corollary). Liberals foresee Big Brother arising from an oligarchy and faceless corporations, while conservatives fret that Orwellian masters will take over from academia and faceless bureaucrats. Which fear has some validity? All of the above. While millions take Orwell’s warning seriously, the normal reflex is to whine: “Stop looking at us!” It cannot work. But what if, instead of whining, we all looked back? Countering surveillance with aggressively effective sousveillance — or scrutiny from below? Say by having citizen-access cameras in the camera control rooms, letting us watch the watchers?

Brin says that reciprocal vision and supervision will be hard to enact and establish, but that it has one advantage over "don’t look at us" laws, namely that it actually has a chance of working.

2. **Multiplex Parenting**

This particular meme — suggested to me by the Institute for the Future’s Distinguished Fellow Jamais Cascio — has only recently hit the radar. "It's in-vitro fertilization," he says, "but with a germline-genetic mod twist." Recently sanctioned by the UK, this is the biotechnological advance where a baby can have three genetic parents via sperm, egg, and (separately) mitochondria. It’s meant as a way to flush out debilitating genetic diseases. But it could also be used for the practice of human trait selection, or so-called "designer babies". The procedure is currently being reviewed for use in the United States. The era of multiplex parents has all but arrived.

3. **Technological Unemployment**

Futurist and scifi novelist Ramez Naam says we should be aware of the potential for "technological unemployment." He describes it as unemployment created by the deployment of technology that can replace human labor. As he told io9,

Read the rest here:
We’ve added 19 new members in March including 8 at the Cyber Focus Day at UCCS. Please continue talking to your colleagues and friends about becoming a member of our chapter. Word of mouth is always our best advertising and it does seem to be working as most of our new members had referral entries.

Next, I’d like to welcome those new members on behalf of the Chapter! When you’re participating in Chapter activities, please take a moment to introduce yourself to members of the board, me, and other members. Don’t forget to identify yourself as a new member and feel free to ask for help or information. I did get to meet several of our new members at the Cyber Focus Day, too.

Since I’ve had quite a few positive responses from people, I will continue to send a reminder email to folks whose membership expires during the current month. That’s a separate project from the multiple reminders that folks get from ISSA International. This is another area where members can help by engaging their colleagues who are members but perhaps not as active as they could be. Increasing participation and increasing energy in chapter activities can only help motivate people to remain members of the chapter.

Bring your check book or credit card to the April chapter meeting. We need to fund some student members! After the chapter announced at the FBC-ISSA Cyber Focus Day that we were sponsoring three new UCCS students as ISSA members, several individuals indicated an interest in personally sponsoring additional student memberships. Pat asked me to pick up the lead on coordinating this effort so if you have any interest in personally sponsoring one or more students send me an email with how many memberships you’d like to sponsor. Each membership costs $55 per year including chapter dues. I’ll be happy to work with you if you have special requests such as male/female, veteran, etc. You will be able to pay the fee via check to the chapter either in person or mail to me, Melody Wilson will get it deposited, and then the chapter will sort out the payment process with ISSA International. Assuming Melody has her credit card reader available, we can also handle credit card payments at our meetings. As I identify sponsorships, I’ll coordinate with UCCS to identify appropriate students to become members. Also, if you know a specific student at any of the local universities you’d like to sponsor, I can work with you on that too.

Thanks for all your efforts and support.

David Reed
Membership Committee Chairman
dreed54321@att.net

<table>
<thead>
<tr>
<th>New Members: March</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jessica Rheinschmidt</td>
</tr>
<tr>
<td>John Urban</td>
</tr>
<tr>
<td>Brad Stokes</td>
</tr>
<tr>
<td>Sean Reese</td>
</tr>
<tr>
<td>Kirstie Hodges</td>
</tr>
<tr>
<td>Leticia James</td>
</tr>
<tr>
<td>Jayme Paul Smith</td>
</tr>
<tr>
<td>Sonny Cordova</td>
</tr>
<tr>
<td>Frank Gatta</td>
</tr>
<tr>
<td>Brian Soderquist</td>
</tr>
<tr>
<td>Laura Francis</td>
</tr>
<tr>
<td>Frederick Engle</td>
</tr>
<tr>
<td>Kurt Reich</td>
</tr>
<tr>
<td>Jennifer Di Santo</td>
</tr>
<tr>
<td>Valentin Rojas</td>
</tr>
<tr>
<td>Aaron Perkins</td>
</tr>
<tr>
<td>Patrick Leedom</td>
</tr>
<tr>
<td>Samuel Smith</td>
</tr>
<tr>
<td>Mark Jenson</td>
</tr>
</tbody>
</table>

A Note From Our President

(Continued from page 1)

chapter that only require a couple hours every couple months so please see one of the board members if you can spare that time...we could use your help!

What can you expect from your chapter over the next six (6) months? Continued lunch and dinner meetings to ensure we can reach as many members as possible, CISSP and Security + training events, an August 2-day conference, web site improvements, continued interaction with other professional organizations leading to opportunities for us to present at their meeting/conferences, continued mentoring of college and K-12 students, and a host of other professional opportunities allowing our members to excel.

If you have ideas, questions, or concerns please reach out to me at plavery1961@gmail.com.

Thanks again for your support.

Pat
Upcoming Open House

L-3 NSS will be hosting an Open House on April 16th from 1:00 pm – 6:00 pm in Colorado Springs, CO at the L-3 Building off Tech Center Drive! We are seeking professionals with various levels of IT experience to support the Air Force Satellite Control Network (AFSCN) communities for the Consolidated AFSCN Modification, Maintenance, & Operations (CAMMO) opportunity.

Description
L-3 NSS will be hosting a Recruiting Event on Wednesday, April 16, 2014 from 1:00 pm to 6:00 pm
L-3 Building: 5575 Tech Center Drive, Suite 118, Colorado Springs, CO 80919

PLEASE BRING A RESUME FOR REVIEW

The L-3 CAMMO Team: Combining the Leader in Sustainment with the Trusted Partner in O&M

Clearance required: Secret

Positions contingent upon Contract Award:
CM/DM Analysts, Designers, Electronic Specialists, Engineering Technicians, Hardware Engineers, IT, Logistics Programmers, Project Managers, QA, Software Engineers, Systems Engineers

Due to the nature of our work these positions require the ability to obtain and maintain a Department of Defense security clearance.

Link to Apply:
https://l3com.taleo.net/careersection/l3_ext_us/jobdetail.ftl?lang=en&src=L3NSSCAMMO&job=055271

DoDI 8500.01 Cybersecurity &
DoDI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) Instruction
Risk Management Framework (RMF) for DoD Information Technology (IT)

DoDI 8500.01 reissues and renames DoD Directive (DoDD) 8500.01E (Reference (a)) as a DoD Instruction (DoDI) pursuant to the authority in DoDD 5144.02 (Reference (b)) to establish a DoD cybersecurity program to protect and defend DoD information and information technology (IT).

Web site address:

DoDI 8510.01 Reissues and renames DoD Instruction (DoDI) 8510.01 in accordance with the authority in DoD Directive (DoDD) 5144.02. It establishes the Risk Management Framework for DoD IT (referred to in this instruction as “the RMF”), establishing associated cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. The RMF replaces the DoD Information Assurance Certification and Accreditation Process (DIACAP) and manages the life-cycle cybersecurity risk to DoD IT.

Web site address:
The Colorado Springs Chapter of ISSA is hosting a 40-Hour CISSP Examination Preparation Seminar.

**Location:**
Colorado Technical University (CTU)
4435 N. Chestnut St., Colorado Springs, CO  80907

**Dates:**
Apr 5 & 19 // May 3 & 17 2014

**Dates:**
Check in between 8:00 AM and 8:15 AM on Mar 22
Class starts on the dates provided and runs from 8:15 AM to 4:45 PM each day (30 min lunch)

**Cost:**
- Non ISSA and Trial Members - **$500**
- Current ISSA Members (not ISSA-COS) - **$210**
- Current CTU CSS 200 students - **$175**
- Current ISSA-COS members - **$125**
- Current ISSA-COS members who are also Current CSS 200 Students $100

ISSA members, who have already taken the class but would like to attend as a refresher, please contact Colleen Murphy for tuition rates.

**Registration & Volunteer Instructors Contact:**
Volunteers for instructors and support staff may contact Colleen Murphy at: crmurphy.cs@hotmail.com or Russ Weeks at: scoutguy@gmail.com.

To register for class provide your name, contact info, ISSA member number and student status to Colleen Murphy or Russ Weeks. Questions; please call Colleen at: 719-651-0415.

**Updated Course Content and In-Chapter Instructors**

- Updated and expanded material - CISSP Test Objectives & Exam Tips
- Each block of instruction covers the exam objectives

*All Instructors are CISSP Certified*

**Topics covered include**

- Access Control
- Telecommunications and Network Security
- Information Security Governance and Risk Mgt
- Software Development Security
- Cryptography
- Security Architecture and Design
- Operations Security
- Business Continuity and Disaster Recovery Planning
- Legal, Regulations, Investigations and Compliance
- Physical (Environmental) Security

**To Become a Member of ISSA visit:** [www.issa.org](http://www.issa.org) / Join ISSA. Specify the Colorado Springs Chapter.
Pat and the Board presenting a $1000 check to Dr. Dan Dandapani, Dean of the UCCS College of Engineering and Applied Science, and Ms. Margo Hatton, UCCS Director of Development.

Presenting student memberships to three UCCS students.

New Senior Members Dan Hans and John Schutt.

Door Prize Winners
Survey Winners
Chuck Forth (1st),
Steve Shepherd
(100th), Carl Spray
(Random)

Aaron Perkins, UCCS Student and new ISSA members presenting a briefing titled "Training the Next Generation"

Brian Kirouac, ISSA Board Member presenting a demonstration titled "Web Hacking"

Outstanding support from vendors

Attendees 210
If You Are Going to be in Orlando, Florida
Check this out!

One of our Chapter members, Wally Magda, is on his way to becoming a SANS Instructor! As part of this effort he is hosting a lunch on Orlando. If you can support him, please do! Details follow:

**Topic:** ICS Cybersecurity in an Interconnected World

**Tuesday, April 8th, 12:30pm - 1:15pm**

This event is **free**, but space is limited and allocated on a first-registered basis. **Lunch will be provided.** Please go to the link below to register.

http://www.sans.org/event/sans-2014/bonus-sessions/4645

Wally Magda is an internationally recognized cyber security expert for Industrial Control Systems (ICS) with over 20 years of experience. His deep security experience spans military nuclear missile command and control systems, intelligence agencies, enterprise cyber security and industrial control systems. He volunteers as an instructor teaching CISSP prep courses at a local technical university. Wally earned a Bachelor of Science degree in Management Information Systems (MIS) and holds a number of professional certifications including ISA Certified Automation Professional (CAP), SANS GIAC Global Industrial Cyber Security Professional (GICSP), ASIS Physical Security Professional (PSP), and ISC2 Certified Information Systems Security Professional (CISSP).

Mentorship—A Note From Our VP

A mentor is a person with experience and knowledge that guides and directs a person who has less experience. A person can be a mentor and may not even realize it. Mentors give advice and guidance to others. The information the mentor is providing is unbiased and may or may not be taken.

Within the chapter we have several individuals that are mentors. They are willing to advise and give direction to those asking for guidance. The experience levels of the chapter members are huge. There are several individuals who were on a different career path before they became a computer security person and there are several others that have always been in this field.

One of the chapter's priorities is to inspire younger members to be involved. During the Cyber Focus conference at UCCS, the student speaker Aaron spoke of his mentor. The new generation is looking for mentors and we have the members to fill that capability. The next generation is not the only ones seeking mentors, there are some mature individuals wanting out of their current career path and would like to get into this field. They too need someone to guide them along.

The board realizes the need for mentors. Currently the person seeking advice is hoping to find someone with common ground to direct them. If you are seeking a mentor or be a mentor please contact Mark Spencer, mark.l.spencer@comcast.net, Lora Woodworth, woodworth74@gmail.com or myself at thorbuc@aol.com.

Cindy
Vice-President, ISSA-COS
NSA surveillance program reaches ‘into the past’ to retrieve, replay phone calls

By Barton Gellman and Ashkan Soltani, Washington Post, March 18, 2014

The National Security Agency has built a surveillance system capable of recording “100 percent” of a foreign country’s telephone calls, enabling the agency to rewind and review conversations as long as a month after they take place, according to people with direct knowledge of the effort and documents supplied by former contractor Edward Snowden.

A senior manager for the program compares it to a time machine — one that can replay the voices from any call without requiring that a person be identified in advance for surveillance.

The voice interception program, called MYSTIC, began in 2009. Its RETRO tool, short for “retrospective retrieval,” and related projects reached full capacity against the first target nation in 2011. Planning documents two years later anticipated similar operations elsewhere.

In the initial deployment, collection systems are recording “every single” conversation nationwide, storing billions of them in a 30-day rolling buffer that clears the oldest calls as new ones arrive, according to a classified summary.

The call buffer opens a door “into the past,” the summary says, enabling users to “retrieve audio of interest that was not tasked at the time of the original call.” Analysts listen to only a fraction of 1 percent of the calls, but the absolute numbers are high. Each month, they send millions of voice clippings, or “cuts,” for processing and long-term storage.

At the request of U.S. officials, The Washington Post is withholding details that could be used to identify the country where the system is being employed or other countries where its use was envisioned.

No other NSA program disclosed to date has swallowed a nation’s telephone network whole. Outside experts have sometimes described that prospect as disquieting but remote, with notable implications for a growing debate over the NSA’s practice of “bulk collection” abroad.

Bulk methods capture massive data flows “without the use of discriminants,” as President Obama put it in January. By design, they vacuum up all the data they touch — meaning that most of the conversations collected by RETRO would be irrelevant to U.S. national security interests.

In the view of U.S. officials, however, the capability is highly valuable.

In a statement, Caitlin Hayden, spokeswoman for the National Security Council, declined to comment on “specific alleged intelligence activities.” Speaking generally, she said “new or emerging threats” are “often hidden within the large and complex system of modern global communications, and the United States must consequently collect signals intelligence in bulk in certain circumstances in order to identify these threats.”

NSA spokeswoman Vanee Vines, in an e-mailed statement, said that “continuous and selective reporting of specific techniques and tools used for legitimate U.S. foreign intelligence activities is highly detrimental to the national security of the United States and of our allies, and places at risk those we are sworn to protect.”

Some of the documents provided by Snowden suggest that high-volume eavesdropping may soon be extended to other countries, if it has not been already. The RETRO tool was built three years ago as a “unique one-off capability,” but last year’s secret intelligence budget named five more countries for which the MYSTIC program provides “comprehensive metadata access and content,” with a sixth expected to be in place by last October.

The budget did not say whether the NSA now records calls in quantity in those countries, or expects to do so. A separate document placed high priority on planning for MYSTIC accesses against projected new mission requirements, including “voice.”

Ubiquitous voice surveillance, even overseas, pulls in a great deal of content from Americans who telephone, visit and work in the target country. It may also be seen as inconsistent with Obama’s Jan. 17 pledge “that the United States is not spying on ordinary people who don’t threaten our national security,” regardless of nationality, “and that we take their privacy concerns into account.”

Read the rest here:
The ISSA Colorado Springs Chapter is looking for volunteers for the following positions:

1. **Security+ Review Seminar Coordinator**

**Duties:**
Recruit and schedule instructors. Coordinate review of course content and accompanying PowerPoint slides. Coordinate printing of PowerPoint slides and provide to students at each session. Proctor review sessions. Coordinate with ISSA Training Team registrar and refreshments coordinator to communicate class size for planning/preparation purposes. Help set up class room for instructors. Respond to registering student queries as needed.

We currently hold three Security+ review seminars each calendar year; the first Saturday of March, June, and September. If the first Saturday happens to be a holiday, we divert to the second Saturday. Your duties will include coordinating the June 7, 2014, Security+ session.

2. **Security+ Instructor**

**Duties:**
We need instructors for the **7 Jun 2014** Security+ Review Seminar for the following topics:

- **Network Security**
- **Compliance and Operational Security**
- **Threats and Vulnerabilities**
- **Application, Data, and Host Security**
- **Access Control and Identity Management**
- **Cryptography**

We provide you our baseline slides for instruction, but you may modify as you see fit as long as your changes remain within official CompTIA content. During the review seminar, each topic consist of no more than 1.25 hours of instruction. Scheduling of time slots is completed through the Security+ Review Seminar Coordinator. We have a policy that instructors be Security+ Certified, but can work with individuals on a case by case basis if needed.

If you are interested in either the coordinator or an instructor position, please contact:

Jim Stephens (jstephens22@comcast.net) or Colleen Murphy (crmurphy.cs@hotmail.com).
Wow, it is hard to believe we have already burned-up three months of 2014! Yet, here we are in April so I wanted to communicate to you what your Chapter Training Team has done so far this year.

In March we held our first of three Security+ Review Seminars. We had 19 people register for the review, one of the highest numbers we have had in the last couple of years. We will repeat the Security+ review on 7 June and 6 September of this year. We followed this with the kickoff of our 2014 CISSP Review Seminar with 13 students. The CISSP Review Seminar is a five-Saturday event, so we have four more to go and it is not too late to join. The next meeting is 5 April. If you would like to join or if you already have your CISSP and would like to attend to earn CPEs, please contact Colleen Murphy (crmurphy.cs@hotmail.com) or Russ Weeks (scoutguy@gmail.com) for more details.

Thanks to some forward thinking on the part of Jeff Pettorino and Russ Weeks, we recently started using Eventbrite (www.Eventbrite.com) to advertise our review seminars and other training sessions. Eventbrite also provides us the means to allow students to pre-pay for the event with a credit card. Each time we distribute a flyer for an upcoming event, we will include the specific Eventbrite URL for your convenience.

As you may know, we use an all-volunteer force to conduct review seminars and it takes a great deal of effort in the form of logistics, scheduling, advertising, banking and content development to the end point of actually executing the review. Many thanks to the review coordinators, registrar, logisticians, treasurer, content reviewers and instructors for putting this all together! Also big thanks to Colorado Technical University for allowing us to use their facilities!

The Training Team is also participating in a Colorado Springs Chapter initiative to reach out to local schools and military bases to further professional education and spark interest in potential new members. To this end, we have started providing vouchers to attend our review seminars for free and have distributed them to Colorado Technical University, the University of Colorado at Colorado Springs, the Air Force Academy (base, not the school), Ft Carson, and Peterson AFB. My apologies to the folks at Schriever AFB; we did not get a voucher to you on our last go around, but will do so from this point forward.

We use a couple of different methods to distribute the vouchers. For the schools it is less complicated as we can provide the voucher to their faculty and they in-turn distribute them to their deserving students. The military bases are not that simple as there are many different entities on each base. Until we come up with a more formalized method, I challenge personnel from each base to contact me (jstephens22@comcast.net) with nominees for vouchers for the next two Security+ Review Seminars. Please be aware there are a limited number of vouchers available. Nominees can be military, civilian, or contractor. Nomination cutoff date is one week prior to the scheduled class date.

I am sad to report that Roy Harrell, who has been a very active member of the Training Team for numerous years, is departing the Colorado Springs area for a new job in San Antonio, Texas. Roy has been involved in many training areas, but most visible was his role as the sole coordinator and instructor for our Security+ Review Seminar. I am sure I speak for the entire chapter in thanking Roy for all his contributions and wish him the best of luck in his new job and community!

Lastly, with Roy’s departure I am looking for a new Security+ Review Seminar coordinator and instructors (see the previous page.) If you are interested and want more information please contact me via my email address (jstephens22@comcast.net). We have about two months before our next review and I would like someone in place as soon as possible to start coordination.

Jim Stephens
Vice President, Education and Training
ISSA-Colorado Springs
By Ayesha Rascoe, Reuters, February 28, 2014

U.S. utilities would benefit from an independent group to set industry-wide guidelines on combating cyber threats, according to a think-tank report released on Friday that was co-authored by a former director of the Central Intelligence Agency.

The report, from the Bipartisan Policy Center (http://bipartisanpolicy.org/news/press-releases/2014/02/friday-bpc-releases-new-recommendations-protecting-electric-grid), said a new independent organization could bring together the disparate interests in the sector to help manage cybersecurity for the nation’s electric grid, and help to deal with threats such as new malware that could be targeted at plants’ information technology systems.

“We don’t have one group looking at this holistically to see what the answers are,” said Curt Hebert, a co-author of the report who is a former chairman of the Federal Energy Regulatory Commission, the agency which oversees aspects of the nation’s electric grid.

The other authors of the report were Michael Hayden, director of the CIA under President George W. Bush, and Susan Tierney, former assistant secretary at the Energy Department under President Bill Clinton.

The report suggested that a new entity be modeled after the nuclear industry’s Institute of Nuclear Power Operations, INPO was established by nuclear companies in 1979 following the recommendations of a presidential commission after the Three Mile Island nuclear plant accident.

The industry-funded institute conducts regular evaluations of nuclear plants, establishes performance objectives and helps train nuclear plant employees.

In addition to identifying best practices regarding cybersecurity, the industry body proposed by the report would also analyze cyber incidents as they happen and offer technical assistance.

The proposal faces some push back from the Edison Electric Institute, a trade group representing investor-owned electric companies. The group raised concerns about whether the industry needs another organization weighing in on security matters.

Scott Aaronson, senior director of national security policy at EEI, said the functions described in the report could be carried out by existing organizations.

Read the rest here:
http://www.reuters.com/article/2014/02/28/us-usa-cybersecurity-utilities-idUSBREA1R21620140228

Spring Cleaning: Who Has Access to Your Data?

By Nick Bilton, New York Times March 14, 2014

It’s almost that time of year again. Wash off the car. Take the cover off the grill. And figure out who has access to your social accounts.

Whether you realize it or not, dozens — if not hundreds — of apps and services have access to your social accounts and can see everything you’re doing online. Tweets, Likes, your location, are all there for the taking. What’s worse, there’s a pretty good chance you unwittingly gave them permission.

On Thursday, this happened to me. I looked at Twitter and noticed that a start-up was tweeting from my account. I immediately deleted the Twitter message and revoked access to the service. But in doing so I noticed that hundreds of old apps have access to my Twitter, Facebook, Google and LinkedIn accounts.

It was time to do a little cleanup.

Just like the spring cleaning rule that says, “If you haven’t worn it in six months, throw it out,” you should use the same edict with your online data: “If you haven’t logged in to an app or site in six months, revoke its access.”

Here are some tips to clean up who has access to all your personal data:

Twitter

If you venture over to Twitter’s “Applications” page you will be able to see a long list of all the apps and services that currently have access to your Twitter profile. If you’re like me, you’ve probably forgotten about many of these apps — or, as I discovered, some of these companies have since been acquired by other companies. While many of these services use this access only to know who you are on another site, many are also collecting data about you.

To be safe hit the “Revoke Access” button for any apps that you haven’t visited in the last few months. Or any that look a little sketchy.

You will want to be especially careful of applications that have the ability to tweet on your behalf. These apps will have a line of text below their logo that say “Permissions: read and write.” My advice: Limit these to only sites you absolutely trust.

Read the rest here:
http://bitsblogs.nytimes.com/2014/03/14/spring-cleaning-who-has-access-to-your-data/?_php=true&_type=blogs&_r=0
Forget USBs - these ‘post-it notes’ transfer files just by sticking them on to a computer

By Victoria Woollaston, Daily Mail, March 11, 2014

Transferring data onto your computer could soon be as simple as using a post-it note.

Scientists have invented data storage devices that look like the sticky labels, and transfer files simply by being stuck onto the front of a computer, or other device.

The tiny, paper-thin drives called Datastickies are stacked one on top of another, like real post-it notes, and are then peeled off as and when they're needed.

The user then sticks them to the front of their computer, TV, smartphone or tablet to transfer data via a special adhesive.

Datastickies are made from graphene - a super-strong, conductive material made of a single layer of carbon atoms - and will be sold in a range of different sizes up to 32GB.

The technology is still being developed, but its hoped they will one day replace popular USB drives.

Datastickies' design was the brainchild of designer Aditi Singh and university professor Parag Anand, both from New Delhi, India.

Singh said: 'Datastickies are a design concept for graphene-based flash drives that may replace USB data drives in the future.

'USB-based drives can be inconvenient to use as the positioning and insertion of the drive in the USB slot needs to be done precisely.

'When the slots are at the rear of a device, as is the case for many desktop computers, this task becomes even more troublesome.

'Datastickies are envisaged to solve this problem by carrying data like a stack of sticky-back notes.'

The special adhesive used to stick the devices together, and onto electronic devices, is conductive.

It is a 'special low-tack, pressure-sensitive adhesive' capable of being reused without leaving marks like a repositional note, explained the designers.

Datastickies will be sold in a variety of colours and patterns based on type and size. They can also be stacked and used together for increased capacity.

The top surface can be written on, and if a file needs to be given to someone, a single sticky can be handed out rather than an entire pen drive.

'Datastickies are not easily lost because they can be stuck down on any object', continued the designers.

Read the rest here:
http://www.dailymail.co.uk/sciencetech/article-2578243/Forget-USBs-post-notes-transfer-files-just-sticking-computer.html

Facebook's security chief talks encryption plan

By Rachel King, ZDNet, March 18, 2014

Facebook has built its business upon the sharing of content between people worldwide, but protecting that data is a gargantuan responsibility -- one that demands an increasing amount of transparency.

Facebook’s chief security officer Joe Sullivan sat down for a whiteboard session at the social network’s Silicon Valley headquarters on Tuesday morning, providing a deep dive about the company’s security strategy.

That strategy, Sullivan explained, starts with the security knowledge and culture within Facebook offices.

"You can't expect security to be perfect," Sullivan asserted, arguing that security is in a constant state of improvement.

A decade ago, Sullivan observed positively that security has changed from something people don’t really want to do to something people are excited about -- starting with internal hacks and dummy phishing emails used as learning lessons within the Menlo Park, Calif.-based company itself.

One simple requirement for Facebook employees that could go a long way is the requirement for every Facebook employee to have Login Approval settings turned on, adding an extra layer of security authentication to keep others from logging into their accounts.

These days, Sullivan observed positively that security has changed from something people don't really want to do to something people are excited about -- starting with internal hacks and dummy phishing emails used as learning lessons within the Menlo Park, Calif.-based company itself.

One simple requirement for Facebook employees that could go a long way is the requirement for every Facebook employee to have Login Approval settings turned on, adding an extra layer of security authentication to keep others from logging into their accounts.

When looking at some of the more recent high-profile cyber attacks, notably those conducted by the Syrian Electronic Army going after media outlets and corporations, Sullivan posited there has always been a personal and social component to the attacks.

Read the rest here:
IBM Sponsored a Major Hollywood Movie

About Computers in 1957

In the sixth chapter of his 2010 book The Computer Boys Take Over, Nathan L. Ensmenger looks back at the 1957 movie Desk Set within the context of 1950s computing and the fear that one day we’d all be replaced by machines:

What is less widely remembered about Desk Set is that it was sponsored in part by the IBM Corporation. The film opens with a wide-angle view of an IBM showroom, which then closes to a tight shot of a single machine bearing the IBM logo. The equipment on the set was provided by IBM, and the credits at the end of the film—in which an acknowledgment of IBM's involvement and assistance features prominently—appear as if printed on an IBM machine. IBM also supplied equipment operators and training.

The IBM Corporation’s involvement with Desk Set was more than an early example of opportunistic product placement. Underneath the trappings of a lighthearted comedy, Desk Set was the first film of its era to deal seriously with the organizational and professional implications of the electronic computer. In the midst of the general enthusiasm that characterized popular coverage of the computer in this period crept hints of unease about the possibility of electronic brains displacing humans in domains previously thought to have been free from the threat of mechanization.

You can read the rest of chapter 6 from the book here:
The Role of the Forensic Accountant

By Randall Jackson, Computerworld New Zealand, March 18, 2014

The Green Party recently called on the government to sign up to an accord that ensures financial transactions between the government and oil, gas and mineral companies are made public.

Green Party energy spokesman Gareth Hughes says there are "a number of mechanisms and instruments to promote openness and transparency in the energy sector", and "officials make publicly available information on all currently held".

"At the moment it's pretty hard to find that information if you're not a forensic accountant or tax expert."

This raises questions of what is the forensic accountant, what do they do, and how does that differ from computer forensic and the whole cyber crime specialist?

Wayne Kedzlie is a rare individual who covers both disciplines. He is a seasoned IT professional (programming, databases, BI, ERP) who has graduate and postgraduate qualifications in finance and accounting, and corporate and chartered accounting tenures on his CV.

"With the uttermost respect to the accounting profession, technical IT skills (databases, IT security, data mining, architecture, etc) are well outside the domain expertise of your classic accountant," he says. "And so for firms that offer forensic services, the forensic IT component is serviced by IT specialists, and the forensic accounting component by forensic accounting specialists. The required skills sets could not be more different."

Kedzlie says the computer forensic specialist is all about the preservation and cataloguing of IT assets in the interests of a fraud investigation. This will invariably canvas emails, files and documents, images, and databases storing financial, billing and intellectual assets. Where computer forensic is about data preservation, collection and assembly, forensic accounting is about analysis and reporting.

"I had a lawyer in Court ask me whether my forensic work 'would be described as basically straight copying the data onto hard drives'. Aside from trying not to laugh at the proposition, it indeed showed the knowledge gap between the lay-person and the sophisticated technologies and techniques that make up the arsenal available to the computer forensic specialist.

"The computer forensic specialist preserves the IT assets in a forensically sound way. This needs to occur as soon as fraud is suspected or, better still, as a planned programme of continuous testing for fraud through testing of physical and IT controls and the running of test investigations."

He says there are very few organisations he has come across that take a proactive approach to fraud prevention. "Invariably we adopt the ambulance at the bottom of the hill approach, and at that stage, while a culprit might be held to account, the damage is well and truly done.

"Spinning hard drives overwrite data. The sooner those drives are preserved, the more likely data can be recovered. Put simply, nothing on a hard drive is ever deleted: the process of preservation and then the use of specialised forensic tools to identify and catalogue key data or chains of data is the key responsibility of the computer forensic specialist.

"First, we boot evidential computers direct from a USB drive, or we remove the drive from the machine, as it is important that the preservation process itself does not disturb the evidence. We then image the drive using industry approved technologies which delivers a forensically sound evidence that will stand up to the rigours of investigation and the Court processes."

Read the rest here: http://www.computerworld.co.nz/article/540725/role_forensic_accountant/?fp=16&fpid=1
Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It

By Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack, Bloomberg BusinessWeek, March 13, 2014

The anger has spilled into Congress, where company officials, including Chief Financial Officer John Mulligan, were called to testify in February. The House Committee on Oversight and Government Reform, which this week received from Target documents related to what executives knew and when they knew it, will now seek additional material related to Bloomberg Businessweek’s reporting, said Frederick Hill, a spokesman for U.S. Representative Darrell Issa, the panel’s chairman. “The Oversight Committee has asked Target when it will be producing documents related to the November 30 incident,” Hill said. Major banks and store chains are pointing fingers at each other over years of delay in adopting a more secure technology that uses cards with embedded chips. Such cards, now common throughout Europe, are harder to counterfeit than those with magnetic strips. Target executives—Chief Information Officer Beth Jacob resigned on March 5—promise that their company will help lead that transition; they announced in February that they’ll spend $100 million for registers and other technology that read the new cards. Its stock is trading near $61, almost unchanged since the day it disclosed the hack. FireEye shares have more than doubled, to around $80.

Sometime in early March someone broke into Rescator.so and stole the logins, passwords, and payment information of carders, then posted the data online. Krebs says it’s unclear who was behind the hack, but it appears to be someone who wanted to shut the operation down, possibly vigilantes or competitors.

Target was striving to be different. Company officials say its information security staff now numbers more than 300 people—a tenfold increase since 2006, says one of the chain’s former information security managers. Less than a year before the Thanksgiving attack, Target brought in FireEye, a security software company in Milpitas, Calif., that was initially funded by the CIA and is used by intelligence agencies around the world.

The system works by creating a parallel computer network on virtual machines. Before data from the Internet reach Target, they pass through FireEye’s technology, where the hackers’ tools, fooled into thinking they’re in real computers, go to work. The technology spots the attack before it happens, then warns the customer. Unlike antivirus systems, which flag malware from past breaches, FireEye’s isn’t as easily tricked when hackers use novel tools or customize their attack, customers say. “It’s a very smart approach,” says Robert Bigman, the CIA’s former chief information security officer. “When we first started working with them several years ago, no one ever thought of doing it that way.”

On Nov. 30, according to a person who has consulted on Target’s investigation but is not authorized to speak on the record, the hackers deployed their custom-made code, triggering a FireEye alert that indicated unfamiliar malware: “malware.binary.” Details soon followed, including addresses for the servers where the hackers wanted their stolen data to be sent. As the hackers inserted more versions of the same malware (they may have used as many as five, security researchers say), the security system sent out more alerts, each the most urgent on FireEye’s graded scale, says the person who has consulted on Target’s probe.

“The malware utilized is absolutely unsophisticated and uninteresting,” says Jim Walter, director of threat intelligence operations at security technology company McAfee.

The breach could have been stopped there without human intervention. The system has an option to automatically delete malware as it’s detected. But according to two people who audited FireEye’s performance after the breach, Target’s security team turned that function off. Edward Kiledjian, chief information security officer for Bombardier Aerospace, an aircraft maker that has used FireEye for more than a year, says that’s not unusual. “Typically, as a security team, you want to have that last decision point of ‘what do I do,’” he says. But, he warns, that puts pressure on a team to quickly find and neutralize the infected computers.

Target had done a months-long test of FireEye that ended in May and was rolling out the technology throughout the company’s massive IT system. It’s possible that FireEye was still viewed with some skepticism by its minders at the time of the hack, say two people familiar with Target’s security operations. And the SOC manager, Brian Bobo, departed the company in October, according to his LinkedIn page, leaving a crucial post vacant. (Bobo declined to comment.) Yet it was clear Target was getting warnings of a serious compromise. Even the company’s antivirus system, Symantec Endpoint Protection (SYM), identified suspicious behavior over several days around Thanksgiving—pointing to the same server identified by the FireEye alerts. “The malware utilized is absolutely unsophisticated and uninteresting,” says Jim Walter, director of threat intelligence operations at security technology company McAfee. If Target had had a firm grasp on its network security environment, he adds, “they absolutely would have observed this behavior occurring on its network.”

Read the rest here:
Online attacks hit Russian state and media in wake of independent media crackdown

A local Anonymous branch is DDoSing Russian media outlets, while a similar attack also took out the websites of the Kremlin and the Russian Central Bank. This follows the state blockading of several Putin-unfriendly outlets.

By David Meyer, Gigaom, March 14, 2014

Russian state and media websites have been hit by a wave of denial-of-service attacks. The attacks followed the blockage of several major Russian media outlets at the order of the Kremlin.

One of the attacks, on the presidential website of the Kremlin itself, is the most powerful ever to have hit that facility, according to Putin organ RT. However, the Kremlin also claimed this attack was entirely unrelated to the standoff in Ukraine.

Russia’s Central Bank also saw its website knocked offline on Friday morning, though it is partially back. Meanwhile, on Thursday, a local branch of Anonymous claimed responsibility for taking out the TV station Channel One:

That’s interesting because the first reaction of the affected station was to claim that the distributed denial-of-service (DDoS) attack emanated from Kiev, the Ukrainian capital. Anonymous Caucasus was explicit in a subsequent tweet that the DDoS had nothing to do with Ukraine.

Such attacks use scores of computers — often surreptitiously hijacked to form a “botnet” — to bombard the target with more data than its systems can handle, until those systems temporarily collapse.

Ukrainian state and media organizations have reported many online attacks in recent weeks that may or may not have been orchestrated by the Kremlin.

“Violation of the established order”

Other Russian media outlets were also attacked on Thursday, and earlier in the week Anonymous Caucasus claimed responsibility for an attack on “lapdogs of the FSB” LifeNews (the FSB is the Russian security agency, the successor to the KGB).

The latest attacks, however, may be connected with the blocking on Thursday of several major news sites by Russian ISPs. This was on the Kremlin’s orders, under a 2012 law that was ostensibly designed to protect children from child pornography and material relating to drug use and suicide.

Read the rest here:

The New Kind of DDoS That Could Cripple the Internet

By Eric Limer, Gizmodo, March 14, 2014

If you’re a regular on the internet, you probably know how a DDoS can choke your favorite site with garbage traffic. Well get used to it because they’re not going away; they’re actually getting worse.

Just this year, a new kind of amplified DDoS attack called a NTP DDoS has started to pop up in the darker corners of the web, leveraging old, poorly-written protocols to rally digital armies more mammoth than anything we’ve seen before, and the folks over at Computerphile have a great—if slightly long—explanation of exactly how it works. (You can jump to 3:20 if you want to skip a history lesson and cut to the chase.)

In short, cyber ne'er-do-wells have figured out how to abuse old servers that will send a list of 600 responses if they're asked the right question, making it trivial to drown targets in data even if you only have a few zombie machines at your disposal. This kind of attack has been known about for a while in theory, but now it's rearing its ugly head. And it's probably not attack of this kind out there.

Read the rest here:
Ethical hacker backer hacked, warns of email ransack

Switches registrars, tightens security after 'upsetting' incident

By John Leyden, The Register, March 13, 2014

The IT security certification body that runs the Certified Ethical Hacker programme has itself been hacked.

The EC-Council said the same hackers who ran the DNS poisoning attack that resulted in the defacement of its website in late February had also managed to access the control panel for its website after breaking into the systems of a third-party registrar. This compromised access allowed the miscreants to circumvent security controls and get into the security organisation’s email system, as a breach notice from the EC-Council to its members explains.

EC-Council uses a cloud service provider for enterprise email. Once the domain privilege was attained, the hacker then issued a password reset request to the email service provider. This circumvented EC-Council’s best practices of using complex passwords and 2-factor authentication. We have informed the service provider of this password reset policy vulnerability and are hopeful that they have already rectified it for the benefit of the IT community in general.

With administrative access to the email service provider, the hacker was able to compromise a small number of email accounts before the EC-Council security team was able to respond to the breach. This resulted in unauthorized access to messages in those specific email boxes for a short duration of time.

The investigation into the breach is still ongoing and it's unclear which member data, if any, has been exposed. Credit card transactions are run through a different system that wasn’t exposed by the attack but any private information sent by email might have been compromised, although this is uncertain.

“As a precautionary measure, we are writing to notify members that have sent any personally identifiable information to EC-Council via email that there is a possibility that these may have been exposed through email,” the breach notification from the EC-Council explains. "No credit card data was compromised."

Read the rest here:
http://www.theregister.co.uk/2014/03/13/ethical_hacker_cert_org_pwned/

BAE System Publishes White Paper on “Snake” Cyber Espionage Campaign

By Eduard Kovaks, Softpedia, March 8, 2014

BAE Systems has published a white paper detailing “Snake,” a complex cyber espionage campaign that has been in development since at least 2005. The report details the sophisticated tools and techniques used by the attackers.

Last week, German security company G Data published a report on Uroboros, an espionage rootkit allegedly created and utilized by a Russian intelligence agency. BAE says Uroboros is only one component of a major project.

The 2008 attacks against US networks, the ones that involved a piece of malware dubbed Agent.BTZ, are said to be part of this campaign. The latest variants of Agent.BTZ are much more complex, but they still share many similarities with the original threat.

Last year, the malware was spotted 8 times in Ukraine, 9 times in Lithuania, 4 times in the UK, 2 times in the US and once in Romania.

Two of the samples analyzed by researchers were compiled in late January, which suggests that the campaign is still active. In fact, a large number of infections (14) were observed this year in Ukraine.

The malware authors have used various names to identify different components of the project. In addition to “snake” and “uroboros,” experts have also seen “snark” and “sengoku.”

While this latest research paper doesn’t mention anything about a Russian intelligence agency being behind the cyber espionage operation, experts do note the fact that the malware developers work just like any other professional, from Monday to Friday, from around 9 AM to 6 PM.

What this research once more demonstrates, is how organised and well-funded adversaries are using highly sophisticated tools and techniques to target legitimate organisations on a massive scale,” said Martin Sutherland, managing director at BAE Systems Applied Intelligence.

Read the rest here:
What if all the lights go out?

The U.S. is at risk of a nationwide blackout — and policymakers and industry have known this for years.

By The Times Editorial Board, Los Angeles Times, March 16, 2014

Californians may be inured to rolling blackouts that cut off their power for hours at a time, but imagine an outage that darkens the entire country — for more than a year. That nightmare scenario could happen if just a handful of crucial, heavy-duty electrical transformers are taken down, according to a confidential federal report disclosed last week by the Wall Street Journal. Federal regulators and the utilities’ trade association were outraged that the report was leaked, but the real outrage is that this vulnerability persists even though policymakers and industry executives have known about it for years.

The transformers at issue raise the voltage of the power generated so it can be transmitted across long distances. The size of overfed dumpsters, they are custom fitted into arrays in utility substations, often industrial or remote areas. Last April, unidentified snipers shot holes in 17 transformers at a Pacific Gas & Electric substation near San Jose, forcing PG&E to scramble to reroute power. The utility averted a blackout, but the attack — which authorities have been investigating as vandalism, not terrorism — highlighted how susceptible substations could be.

Given that there are tens of thousands of substations on the national grid, PG&E’s experience may not seem so alarming. But according to the Federal Energy Regulatory Commission study disclosed by the Journal, a few dozen of the substations are so important to the flow of energy that knocking out just nine of them would cause a metastasizing blackout that stretched from coast to coast. And replacement transformers for these substations can take more than a year to build, deliver and install, in part because most are made overseas.

Industry officials downplayed the FERC study and said they’ve been preparing for attacks since Sept. 11, 2001, developing a system to share spare transformers. But that’s not very reassuring, considering that heavy-duty transformers aren’t interchangeable. Acting FERC Chairwoman Cheryl A. LaFleur also noted that the commission had just ordered the development of new mandates for keeping “critical” utility assets safe from physical attack.

Read the rest here:
http://www.latimes.com/opinion/editorials/la-ed-electricity-transformers-vulnerable-20140316,0,4805837.story#axzz2w4YkcK9S

Texting ATMs for Cash Shows Cybercriminals’ Increasing Sophistication

By Symantec, March 24, 2014

There is a growing chorus of voices calling for businesses and home users to upgrade existing Windows XP installations to newer versions of Windows, if not for the features, then at least for the improved security and support. ATMs are basically computers that control access to cash, and as it turns out, almost 95 percent of them run on versions of Windows XP. With the looming end-of-life for Windows XP slated for April 8, 2014, the banking industry is facing a serious risk of cyberattacks aimed at their ATM fleet. This risk is not hypothetical — it is already happening. Cybercriminals are targeting ATMs with increasingly sophisticated techniques.

In late 2013, we blogged about new ATM malware in Mexico, which could let attackers force ATMs to spew cash on demand using an external keyboard. That threat was named Backdoor.Ploutus. Some weeks later, we discovered a new variant which showed that the malware had evolved into a modular architecture. The new variant was also localized into the English language, suggesting that the malware author was expanding their franchise to other countries. The new variant was identified as Backdoor.Ploutus.B (referred to as Ploutus throughout this blog).

What was interesting about this variant of Ploutus was that it allowed cybercriminals to simply send an SMS to the compromised ATM, then walk up and collect the dispensed cash. It may seem incredible but this technique is being used in a number of places across the world at this time.

Read the rest here:
http://www.symantec.com/connect/blogs/texting-atms-cash-shows-cybercriminals-increasing-sophistication
New research forecasts the staggering cost of cybercrime

By David Finn, TechNet, March 18, 2014

A new study released Tuesday reaffirms what we in Microsoft’s Digital Crimes Unit have seen for some time now – cybercrime is a booming business for organized crime groups all over the world. The study, conducted by IDC and the National University of Singapore (NUS), reveals that businesses worldwide will spend nearly $500 billion in 2014 to deal with the problems caused by malware on pirated software. Individual consumers, meanwhile, are expected to spend $25 billion and waste 1.2 billion hours this year because of security threats and costly computer fixes.

As we announced in November, the Microsoft Digital Crimes Unit recently brought together 100 cybercrime experts from around the world – and across the areas of IP crimes, botnets, malware and technology-facilitated exploitation of children and the elderly – to form one global organization, so that when focus areas intersect, we can work better to build a safer Internet. The study released Tuesday, entitled “The Link Between Pirated Software and Cybersecurity Breaches: How Malware in Pirated Software is Costing the World Billions,” underscores how much these categories of crime overlap. NUS’s forensic analysis, for example, uncovered that of 203 computers purchased in 11 countries as “new” (but actually loaded with pirated software), 61 percent were infected with dangerous malware. Most of the infected computers had more than one malware threat on them, and any one threat could infect multiple files.

While these statistics are frightening, they shouldn’t be a surprise. After all, cybercriminals aim to profit from any security lapse they can find. And through pirated software, they’ve found another way to introduce malware into computer networks – breaking in so they can grab whatever they want: your identity, your passwords and your money. At the Microsoft Cybercrime Center, we’re focused on reducing malicious software crimes to keep personal and financial data safe and secure for everyone, reducing the financial incentive for criminals. Why? Because as the study uncovered, it’s a top concern for consumers, businesses and governments.

Sixty percent of consumers surveyed say their greatest fear from infected software is the loss of data, files or personal information, followed by unauthorized Internet transactions (51 percent) and hijacking of email, social networking and bank accounts (50 percent). But what really struck me is that, despite fearing such losses and attacks, 43 percent of these same consumers admitted they do not install security updates, making them sitting ducks for cybercriminals. Not protecting your computer these days is equivalent to leaving the doors and windows to your house unlocked. So when it comes to cybersecurity, we have a lot more work to do to persuade people to change their behavior.

The study also revealed that enterprises are particularly hard hit by malware introduced via pirated software. In 2014, businesses will spend $127 billion dealing with security issues and $364 billion dealing with data breaches, and almost two-thirds of these losses, or $315 billion, will be the result of organized crime – malware launched by financially motivated criminals. As for governments, they could lose more than $50 billion dealing with the costs associated with malware on pirated software in 2014. Government officials surveyed by IDC say their greatest concern from infected software is the loss of business trade secrets or competitive information (59 percent), followed by unauthorized access to confidential government information (55 percent) and the impact of cyberattacks on critical infrastructure (55 percent).

The IDC/NUS study was released as part of Microsoft’s “Play It Safe” campaign, a global initiative to create greater awareness of the connection between cybersecurity breaches, malware and piracy. The global study surveyed 1,700 consumers, IT workers, CIOs and government officials in 15 markets, in addition to conducting the forensic analysis on the 203 computers.

Read more here:
This Wearable Abacus Is Basically the World's Oldest Smart Ring

By Ashley Feinberg, Gizmodo, March 17, 2014

Smart rings may seem like something from an impossible (or at least highly unlikely) vision of the future, but surprisingly enough, tech you can wrap around your little finger isn't anything new. Just take this itty-bitty abacus from the 17th century as proof.

Coming to us from China's Qing Dynasty era, the ring features a 1.2 centimeter-long, 0.7 centimeter-wide abacus that, despite its small stature, is still a fully functional counting tool. But as ChinaCulture.org explains, the less-than-one-millimeter-long beads are far too small to be moved with your own stubby fingers:

Read the rest here:
http://gizmodo.com/this-wearable-abacus-is-basically-the-worlds-oldest-sm-1545627562

Upcoming Chapter Meetings

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>April 9</td>
<td>10:45 to 1:00</td>
<td>The Retired Enlisted Association</td>
</tr>
<tr>
<td></td>
<td></td>
<td>834 Emory Circle</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(719) 596-0927</td>
</tr>
<tr>
<td>April 17</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>May 14</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
<tr>
<td>May 22</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>June 11</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
<tr>
<td>June 19</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>July 9</td>
<td>10:45 to 1:00</td>
<td>TREA</td>
</tr>
<tr>
<td>July 17</td>
<td>5:45 to 8:00</td>
<td>TREA</td>
</tr>
<tr>
<td>August 5 &amp; 6</td>
<td>August Cyber Security Training Forum</td>
<td></td>
</tr>
</tbody>
</table>
March 4, Dark Reading – (International) Researchers create legal botnet abusing free cloud service offers. Researchers presenting at the RSA Conference the week of February 24 demonstrated how they were able to create a botnet by abusing trial accounts for several platform-as-a-service (PaaS) and infrastructure-as-a-service (IaaS) offers. The botnet was created by automating PaaS and IaaS trial sign-up processes and could be used to perform massive port scans, Bitcoin mining, and to manipulate sweepstakes, among other tasks. Source: http://www.darkreading.com/researchers-create-legal-botnet-abusing/240166428

March 4, Help Net Security – (International) 300,000 routers compromised in DNS hijacking campaign. Researchers with Team Cymru found that around 300,000 small office/home office routers have been compromised and had their DNS settings changed to two IP addresses in the U.K. in order to allow them to perform man-in-the-middle (MitM) attacks. The researchers found that the attack dates to at least mid-December 2013 and has mostly affected routers in Europe and Asia. Source: http://www.net-security.org/secworld.php?id=16473

March 8, Softpedia – (International) BAE Systems publishes white paper on “Snake” cyber espionage campaign. Researchers at BAE Systems Applied Intelligence published a white paper on the Snake cyberespionage campaign, which they believe the Uroburos rootkit is a part of. The researchers stated that the campaign may have been in development since 2005, may still be active, and also contains components known as “snark” and “sengoku.” Source: http://news.softpedia.com/news/BAE-System-Publishes-White-Paper-on-Snake-Cyber-Espionage-Campaign-431214.shtml

March 16, The Register – (International) iOS 7 has weak random number generator. Researchers at Azimuth Security found that the random number generator used in the iOS 7 mobile operating system is weak to brute force attacks that could allow attackers to exploit vulnerabilities previously unable to be exploited. Source: http://www.theregister.co.uk/2014/03/16/ios_7_has_weak_random_number_generator/

March 17, Help Net Security – (International) US announces transition of oversight over Internet’s domain name system. The U.S. Department of Commerce’s National Telecommunications and Information Administration (NTIA) announced its intention to transition oversight of Internet domain name functions to global stakeholders. The NTIA requested that the Internet Corporation for Assigned Names and Numbers (ICANN) convene stakeholders and develop a transition proposal as a first step. Source: http://www.net-security.org/secworld.php?id=16530

March 20, Softpedia – (International) BlackOS: New malicious software used by cybercriminals to redirect traffic. Researchers at Trend Micro analyzed a piece of malware called BlackOS which automates the redirection of traffic from malicious or compromised Web sites. BlackOS started being advertised on underweb forums in February and is based on the “Tale of the North” software. Source: http://news.softpedia.com/news/BlackOS-New-Malicious-Software-Used-by-Cybercriminals-to-Redirect-Traffic-433325.shtml

March 27, U.S. Consumer Product Safety Commission – (International) Lenovo recalls battery packs for ThinkPad notebook computers due to fire hazard. Lenovo announced a recall March 27 of about 37,400 battery packs for ThinkPad notebooks in the U.S. and Canada due to an issue that can cause them to overheat, posing a fire hazard. Source: http://www.cpsc.gov/en/Recalls/2014/Lenovo-Recalls-Battery-Packs-for-ThinkPad-Notebook-Computers/
Article for the Newsletter?
If you would like to submit an article...

Are you a budding journalist? Do you have something that the Colorado Springs ISSA community should know about? Can you interview one of the “movers and shakers”? Tell us about it!

We are always looking for articles that may be of interest to the broader Colorado Springs security community.
Send your article ideas to Don Creamer at:
doncreamer-issa@q.com

Ensure that “Newsletter” is in the subject line.
Looking forward to seeing you in print!

Malicious apps can hose Android phones, erase data, researchers warn

By Dan Goodin, ArsTechnica March 24 2014

Security researchers said they have uncovered bugs in Google’s Android operating system that could allow malicious apps to send vulnerable devices into a spiral of endlessly looping crashes and possibly delete all data stored on them.

Apps that exploit the denial-of-service vulnerability work on Android versions 2.3, 4.2.2, 4.3, and possibly many other releases of the operating system, researcher Ibrahim Balic wrote in a blog post published last week. Attackers could exploit the underlying memory corruption bug by hiding attack code in an otherwise useful or legitimate app that is programmed to be triggered only after it is installed on a vulnerable handset. By filling the Android "apppname" field with an extremely long value exceeding 387,000 characters, the app can cause the device to go into an endless series of crashes.

"We believe that this vulnerability may be used by cybercriminals to do some substantial damage on Android smartphones and tablets, which include 'bricking' a device or rendering it unusable in any way," Veo Zhang, a mobile threats analyst at Trend Micro, wrote in a blog post published Sunday. "In this context, the device is 'bricked' as it is trapped in an endless reboot loop."

Zhang said the attack works by entering large amounts of data into the Activity label, which is the Android equivalent of the Window title in Microsoft Windows operating systems. As a result, attackers can create booby-trapped apps that have the potential to exploit the vulnerability. Zhang explained:

If a cybercriminal builds an app containing a hidden Activity with a large label, the user will have no idea whatsoever that this exploit is in fact taking place. Cybercriminals can further conceal the exploit by setting a timed trigger event that stops the current app activity and then opens the hidden Activity. When the timed event is triggered, the exploit runs, and the system server crashes as a result. This stops all functionality of the mobile device, and the system will be forced to reboot.

An even worse case is when the malware is written to start automatically upon device startup. Doing so will trap the device in a rebooting loop, rendering it useless. In this case, only a boot loader recovery fix will work, which means that all the information (contacts, photos, files, etc.) stored inside the device will be erased.

Read the rest here:
The Information Systems Security Association (ISSA®) is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications, and peer interaction opportunities that enhance the knowledge, skill, and professional growth of its members.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity, and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved. Members include practitioners at all levels of the security field in a broad range of industries such as communications, education, healthcare, manufacturing, financial, and government.

Position Chairs:
Lee Magginetti—Coins
David Willson—Sponsorship
Don Creamer—Newsletter

Chapter Financials
Overview

Status as of 31 January

<table>
<thead>
<tr>
<th>Account</th>
<th>Amount</th>
</tr>
</thead>
<tbody>
<tr>
<td>Savings</td>
<td>$63.33</td>
</tr>
<tr>
<td>Checking</td>
<td>$8,412.66</td>
</tr>
<tr>
<td>Membership checking</td>
<td>$1,434.87</td>
</tr>
<tr>
<td>Travel Support checking</td>
<td>$100.00</td>
</tr>
<tr>
<td>Training checking</td>
<td>$93.25</td>
</tr>
<tr>
<td>Cash (change/tips)</td>
<td>$10.00</td>
</tr>
<tr>
<td>PayPal Account</td>
<td>$985.23</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>$11,099.34</strong></td>
</tr>
</tbody>
</table>

This Is The Room Where The Internet Was Born

By Alissa Walker & Leonard Kleinrock, iO9, March 5, 2014

For something as ubiquitous as the internet today, it certainly isn't easy to find where it all started. I don't mean historically, I mean logistically: 3420 Boelter Hall is a tiny room in a basement hallway of a large nondescript building on the sprawling UCLA campus.

But from these inauspicious beginnings emerged the reason you're able to read this story, wherever and whenever you're choosing to do so. Although the internet itself has many authors—even, apocryphally, Al Gore—this is widely considered to be its birthplace. This room, with its glaring, lime green paint and scuffed linoleum flooring, is where the first ARPANET node was installed, where communications protocol was established, and where the first message was sent over the network to another node at Stanford University.

Read the rest here: