Ειδήσεις για την ΑΣΦΑΛΕΙΑ στις ΤΠΕ απ' όλο τον κόσμο...

Δελτίο 14
11 Μάρτη 2006

Online Amateurs Crack Nazi Codes
BBC News (03/02/06), A. Blenford

Software powered by grid computing has cracked one of the German ciphers from World War II that stumped both Allied code breakers during the war and cryptography enthusiasts since the publication of the ciphers in 1995. Encoded in 1942 by an updated German Enigma machine, encrypted German ciphers led to major Allied losses in the North Atlantic. S. Krah, a German violinist with a yen for open-source software and cryptography, began the renewed quest to crack the German codes out of "basic human curiosity," despite their relative lack of historical significance. Drawing on the years of work by veteran amateur cryptographers, Krah wrote a code-breaking program that he published on the Internet, drawing the interest of around 45 users who volunteered their machines for the project. The project now runs on 2,500 independent machines. It took just over a month to decode the first of the three ciphers, in which a German submarine reported that it was submerging and relayed the last recorded enemy position. The Enigma machine employed an array of rotors and electrical contents to uniquely encode messages, confounding the celebrated Allied cryptographers at Bletchley Park in the UK. The transmissions were scrambled further as plugboards swapped pairs of letters as the message was being encoded. Krah's software combines algorithms with raw computing power to reproduce the possibilities of the plugboard swaps, while systematically wading through the rotor setting combinations.

Tech Groups Urge Congress to Keep Net Neutrality
IDG News Service (03/02/06), G. Gross

Legislation banning discrimination by broadband providers against rival services transmitted over their networks should be considered by Congress, according to a letter various tech groups sent to the House Energy and Commerce committee on Wednesday. 64 tech companies, trade groups, and consumer proponents issued the letter in response to recent reports that the committee was about to strip a communications bill of so-called net neutrality provisions. The letter's signatories include Amazon.com, EarthLink, eBay, Match.com, Microsoft, Pulver.com, Tivo, Yahoo!, the Consumer Federation of America, Free Press, and Public Knowledge. "We...believe that unless Congress acts, the Internet is at risk of losing the openness that has made it an engine for phenomenal social and economic growth," reads the letter. "We are writing to urge that Congress take steps now to preserve this fundamental underpinning of the Internet and to assure the Internet remains a platform open to innovation and progress." According to the letter, consumers rather than network providers should determine what Web services and sites they use. Verizon, Comcast, AT&T, and other major broadband providers claim a net neutrality law is unnecessary, given a dearth of proof that a problem exists, and suggest that a net neutrality provision would be one of the first major Internet regulations. The communications bill the committee is considering includes a simplified plan for video franchising that would permit large telecom firms to enter the video market and rapidly get approval to roll out services designed to compete with cable TV.

China Splits From the Internet? Probably Not
Computer Business Review (03/01/06), K. Murphy

The Chinese Ministry of Information announced that on March 1, 2006, a number of new Chinese-language second-level domains would be added to the Internet so that "Internet users don't have to surf the Web via the servers under the management of the Internet Corporation for Assigned Names and Numbers of the United States." If this is true, then Internet experts' fears have come true about rival DNS roots servers causing worldwide incompatibility. The UN World Summit on the Information Society (WSIS) has been debating how to handle the DNS root server Pandora's Box for years, and in November 2005 issued a policy conclusion stating that reliance on the ICANN-run root should continue. However, because of translation difficulties in the Chinese announcement, and also China's PR interests in making anti-US news splashes, it is possible China has not set up a separate root. Since March 2005, China has routed some Chinese specialty domains behind the scenes through .cn, making it seem like a host of .cn-based domain names float independently from the ICANN-run root. In this case, ISPs resolve domains to .cn behind the scenes, and private company New.net used the same tactic to sell its non-approved domains such as .shop and .sport. "As far as I can tell, what they're doing is using DNS forwarders, much like ISPs do", says J. Klensin, former chief of the Internet Architecture Board. ICANN currently has no comment, but believes the news is not as bad as the announcement makes it seem.

TIA Lives On
National Journal (02/25/06) Vol. 38, No. 8, P. 66; S. Harris

Despite a congressional mandate putting an end to its activities, the Total Information Awareness (TIA) program, collectively a government anti-terrorism initiative that relied on extensive data mining of personal records and government databases, continued on under different names after having been transferred from the Pentagon to another organization. The Advanced Research and Development Agency (ARDA) has assumed two of the most critical elements of the TIA program, including the Information Awareness Prototype System, the architectural framework that links together numerous data mining tools. TIA owes its origins to Hicks & Associates' B. Sharkey and former National Security Advisor J. Poindexter, who pitched the idea to officials at the Defense Department in the wake of the Sept. 11 attacks. DARPA agreed to host the project, with Poindexter at the helm until protests over his role in the Iran-Contra scandal forced his resignation. It remains unclear if the program will continue under ARDA, though documents have revealed that it had full funding at least until September 2004. Another component of the original TIA program that lived on after it was halted by pressure from privacy groups, Genoa II, concentrated on creating technologies that policymakers and analysts could use to anticipate terrorist attacks. Although the link between the TIA initiatives and President Bush's domestic surveillance program remains unsubstantiated, the early-warning system that TIA was designed to create is the specific type that the NSA is using to eavesdrop on phone calls and emails.

Open-Source Bug Hunt Results Posted
Government Computer News (03/06/06), J. Jackson

Through a far-reaching analysis of open-source code sponsored by the Dept. of Homeland Security, Coverity has found that there is less than one-half of one bug embedded in every 1,000 lines of code, with even lower rates in popular applications such as the Linux kernel and the Apache Web server. The results are the first to appear from the three-year, $1.2 million grant awarded to Coverity, Stanford University, and Symantec. DHS is hopeful that calling attention to the bugs will prompt developers will fix them, shoring up the vulnerabilities that could be exploited by hackers to disrupt or take over a system. Coverity CTO Ben Chelf noted that while the automated scan cannot detect every bug, it discovered some that are overlooked by in-house reviews. The scan found that XMMS is the cleanest program, with only six bugs in 116,899 lines of code. The Advanced Maryland Automatic Network Disk Archiver (AMANDA) proportionally had the most bugs, with 108 discovered in its 88,950 lines of code. The bug density for all the programs was 0.43 per thousand lines of code, with the LAMP stack registering just 0.29 defects per thousand lines of code. Chelf notes the difficulty of making comparisons between open-source code and its commercial counterparts, given that Coverity has only tested a few commercial applications. Coverity has concluded from its study that the size of a program is a poor indicator of quality, as Linux has comparatively few bugs, while a smaller program such as AMANDA may contain many. The number of developers at work on a project, in proportion to its size, is a better predictor of overall quality.

UM Engineers Pioneer Digital Fingerprinting to Catch Cyber Thieves
Newswise (03/07/06)

University of Maryland researchers are developing new digital fingerprinting applications that could protect entertainment content and identify the sources of national security leaks without interfering with appropriate uses. K.J. Ray Liu and Min Wu, both professors of electrical and computer engineering at Maryland, are exploring new cyber forensics techniques to protect content and track the pirates who attempt to steal it through collusion attacks, where multiple attackers attempt to filch and distribute proprietary or classified materials, deleting or altering the original digital fingerprint in the process to avoid being traced. The new technology incorporates anti-collusion codes to safeguard content while still protecting legitimate uses. The technology could help Hollywood protect its copyrights as content passes over the Internet, and the researchers are also exploring techniques that could protect individual content items from inappropriate use without installing unwanted and potentially harmful products onto users' computers. The Maryland researchers' system embeds each item with a unique ID that can tell which users are involved in a piracy attack, and works with equal effectiveness for video, audio, and live multicasts, such as pay-per-view events. "The message our technology sends is: 'Don't bother to try anything, because we can catch you,'" said Liu. Anti-collusion codes could also help identify a person who leaks sensitive national security information embedded in a multimedia format.

Hey Neighbour, Stop Piggybacking on My Wireless
New York Times (03/05/06) P. 1; M. Marriott, A. Zarate, G. Ruethling

"Piggybacking," or the unauthorized use of someone else's wireless Internet connection, is increasingly becoming an issue for people who live in densely populated areas such as New York City or Chicago or in apartment buildings, makers of wireless routers say. One of the reasons why piggybacking is becoming increasingly common is because so many users do not bother to secure their networks with passwords or encryption programs--which allows anyone with a wireless-enabled computer within the 200-foot range of a wireless router to gain access to the network, says analyst Mike Wolf. That assessment is backed up by Humphrey Cheung, the editor of a technology Web site, tomshardware.com. In April 2004, Cheung and his colleagues measured how plentiful open wireless networks have become by flying two single-engine airplanes over metropolitan Los Angeles with two wireless laptops. The project logged more than 4,500 wireless networks, with only about 30% of them encrypted to lock out outsiders, Cheung said. For wireless Internet users who fail to protect their networks, the consequences can be much greater than slower Internet access. Symantec Security Response's David Cole says savvy users could piggyback into unprotected computers to gain access to files containing sensitive financial and personal information, release malicious viruses and worms that could do irreparable damage, or use the computer as a launching pad for identity theft or the uploading and downloading of child pornography.

Future Disruptive Technologies: The Perspectives of MIT & Stanford
Always On (02/01/06) Vol. 1, No. 4, P. 26; T. Byers

MIT vice president for research and associate provost A. Gast and Stanford University dean of engineering J. Plummer participated in a panel moderated by T. Byers at the recent AO 2005 Innovation Summit, where they discussed what disruptive technologies their schools are focusing on. Gast and Plummer agreed that universities, industry, and government have a shared responsibility to inspire the next generation of scientists and engineers, and key to this inspiration is the emphasis on disruptive technologies. Plummer said the fields generating the most excitement among engineers and scientists - biotechnology, energy, nanotechnology, and environment - can not only lead to new knowledge, but can also establish a platform for new entrepreneurism. He explained that his university is attempting "to seed the future by trying out all the wild and crazy ideas and seeing which ones actually have the possibility of being successful." Gast said two keys of Internet-related research at MIT are "the human computer interface and the distributed cell phone everywhere environment". She noted that MIT and Stanford are also concentrating on the grand challenge of energy and its connection to the Internet, and that the various issues associated with energy - consumption, production, storage, and portability - can lead to the development of many disruptive products. At the same time, she emphasized that technical advances "must proceed hand in hand" with tough policy decisions. Both Plummer and Gast said interdisciplinary collaboration - not just between researchers, but between researchers, social scientists, and economists - is critical. However, Plummer said that "while business and policy and technology must work together, their foundation is technology."