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

Δελτίο 147
30 Απρίλη 2009

Hathaway Advocates for Direct White House Role on Cybersecurity
Computerworld (04/23/09), J. Vijayan

President B. Obama's acting senior director for cyberspace Melissa Hathaway, who recently completed a 60-day review of the US government's cybersecurity readiness, has called for the White House to take a more direct role in coordinating the nation's cybersecurity efforts. Hathaway says cybersecurity needs to be a shared effort between the private and public sector, but the task of leading that effort is "the fundamental responsibility of our government." She says the government's responsibility "transcends" the scope of individual departments and agencies, none of which have a broad enough view to match the wide variety of challenges. "Protecting cyberspace requires strong vision and leadership and will require changes in policy, technology, education, and perhaps law," she says. Hathaway is a former Bush administration aide who has been working as a cybercoordination executive for the US Office of the Director of National Intelligence. Hathaway's review found that the federal government is not "organized appropriately" to address threats in cyberspace, as responsibilities for cyberspace are scattered across too many departments, which have many overlapping missions and authorities. She also stressed the need for better collaboration between the government and the private sector on cybersecurity, since a large portion of the critical cyberinfrastructure is owned by private companies. "The public and private sector's interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend," she says. The US also needs to find a way of working with other countries to secure cyberspace, Hathaway says.

Carnegie Mellon Computer Scientists Develop Method for Verifying Safety of Computer-Controlled Devices, Carnegie Mellon News (04/20/09), B. Spice

Carnegie Mellon University professors E. Clarke and A. Platzer have developed a new method for identifying bugs in cyberphysical systems such as aircraft collision avoidance systems and high-speed train controls. The method has already discovered a bug in aircraft collision avoidance maneuvers that could have caused mid-air collisions, and has verified the soundness of the European Train Control System. "With systems becoming more and more complex, mere trial-and-error testing is unlikely to detect subtle problems in system design that can cause disastrous malfunctions," Clarke says. "Our method is the first that can prove these complex cyber-physical systems operate as intended, or else generate counterexamples of how they can fail using computer simulation." The method was used to analyze roundabout maneuvers in aircraft collisions, which are employed when two aircraft are on rapidly converging paths and involve both pilots turning right and then circling to the left until the two aircraft can safely turn right and continue on their original trajectories. The method found that when the aircraft approach at certain angles the roundabout maneuver actually creates a new collision course that the pilots may not be able to avoid. The method also could be used on other cyberphysical systems such as robotic surgery and nano-level manufacturing.

US Steps Up Effort on Digital Defenses

New York Times (04/27/09), D. Sanger; J. Markoff; T. Shanker

The US is engaged in an international race to develop both cyberweapons and cyberdefenses. Thousands of daily attacks on federal and private computer systems in the US, some malicious and some testing for weak points in the US's firewalls, have prompted the Obama administration to review the nation's strategy. Efforts include developing a highly classified replica of the Internet of the future to simulate what would be needed for the country's enemies to shut down power stations, telecommunications, and aviation systems. Obama is expected to propose a significantly larger cyberdefensive effort, including the expansion of a $17 billion, five-year program approved by Congress last year, as well as an end to the bureaucratic battle over who is responsible for defending the country's cyberinfrastructure. However, Obama is not expected to discuss the US's cyberoffensive capabilities, which has been a major investment area for the nation's intelligence agencies, as many of these cyberweapons remain classified. The White House declined to comment on whether Obama supports or opposes the use of US cyberweapons. Some exotic cyberweapons under consideration would enable a military programmer to enter a computer server in Russia or China and destroy a botnet, or activate malicious code that is secretly embedded on computer chips when manufactured, enabling the US to take control of an enemy's computer system.

Europe Funds Secure Operating System Research
IDG News Service (04/27/09), J. Kirk

Vrije Universiteit in the Netherlands has received a grant from the European Research Council that will enable it to continue its research into a more reliable operating system. Vrije professor A. Tanenbaum has developed Minix, which is based on Unix, has a small code base, and offers strong security controls. As part of Tanenbaum's microkernel concept, drivers for features such as sound and other peripheral components would operate like applications outside of the kernel. As a result, when something goes wrong, the computer would carry on. "Having to reboot your computer is just a pain," Tanenbaum says. "The question is 'Can you make a system that actually works very well?'" The approach would have other components function in tightly constrained modules that cannot interfere with one another if they crash, which would help improve security. Analysts say Minix has the potential to be more reliable and secure than Linux or Microsoft Windows.

Clandestine Defense Hub Prepares to Open at UM
Baltimore Sun (04/28/09), D. Wood

Some of the US's leading theoretical mathematicians, behavioral scientists, software engineers, and futurists will gather at a top-secret University of Maryland (UM) research center during the next few months to develop cutting-edge intelligence technology. The Intelligence Advanced Research Projects Activity (IARPA), currently under construction at UM's M-Square research park, will be dedicated to investigating new ideas for intelligence agencies. Challenges the center might tackle include a machine capable of quickly learning a new language so it can instantaneously translate intercepted communications, and software programs capable of using cultural and linguistic clues from interrogations to predict terrorist attacks. "The whole idea is to go beyond the threats of today, to anticipate the national security needs of tomorrow," says Sen. B. Mikulski (D-Md.). Funded by the US Office of the Director of National Intelligence, IARPA awards competitive grants for research into high-risk, high-payoff projects, with most of the research being highly technical and highly classified. A key area of research will explore modeling and other techniques to refine raw data, which officials say is overwhelming analysts, including new techniques, possibly including virtual

worlds that could help analysts sort through data more efficiently. One current research program is developing software capable of scanning eavesdropped conversations in foreign languages.