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

Δελτίο 138
30 Δεκέμβρη 2008

Profs Stand Up to Secure Laptops
Pittsburgh Tribune-Review (12/01/08), M. Cronin

Wireless Internet connections are more difficult to secure than cable connections because users send out information on radio waves that travel in every direction. Hackers can find ways to identify individual wireless users, pinpoint their location, intercept information from those users, and even piggyback on their paid Internet sessions for free. University of Pittsburgh professor J. Brustoloni says it is possible to read emails and attachments sent over wireless connections at hotspots using programs available for free on the Internet. Carnegie Mellon University (CMU) professor S. Seshan says he is willing to give up some privacy in exchange for useful services, but right now he has no idea what information he is disclosing or who can see that information when using a wireless connection. Seshan and CMU computer science doctoral student J. Pang are working with Intel on two wireless security projects. Pang is the lead student on an effort to hide a wireless user's unique address and encrypt any emails, attachments, or other forms of information. Seshan is working to build virtual fences around Wi-Fi hotspots using electronic "steerable" antennas to create areas in which only authorized users can send and receive messages. Meanwhile, CMU professor P. Narasimhan is studying how small devices such as pacemakers and handheld devices can be embedded with enhanced security features.

Estonia to Use Mobile Phones to Simplify E-Voting
IDG News Service (12/15/08), M. Ricknas

Estonia is expanding the authentication of voters to mobile phones. The Estonian Parliament recently voted in favor of the move as a way to make it easier for Estonians living abroad to participate in elections. "In some places, because of internal security policies, it's not possible to use an ID card, so mobile ID is just giving them another option," says S. Meikar, a member of the Estonian Parliament and a proponent of e-voting. Estonia has used a national ID card for authenticating voters since 2005 and will add the mobile phone as an option in 2011. Authentication must occur via a digital certificate stored on Subscriber Identity Module cards. "You still need a computer and the Internet, but now you will have a choice of using your ID card plus card reader or a mobile ID to authenticate yourself," Meikar says. He says it will take about six months to make Internet voting systems technically ready to accommodate mobile-phone authentication.

Plugging a Password Leak
Technology Review (12/19/08), R. Kremen

Researchers from Harvard University's Center for Research on Computation and Society, the University of California, Berkeley, and Stanford University have improved the security of browser-based automatic log-in procedures. The researchers focused on password managers created with browser bookmarklets that use JavaScript to automatically log in a user to a Web site. The researchers identified a major flaw in bookmarklets in which an attack could trick bookmarklets into revealing all of a user's passwords. Bookmarklet-based password managers generally store passwords on a central server, and when a user visits one of those sites the user is automatically logged in. However, the researchers found that bookmarklets could not be trusted to know what Web site the user was actually visiting, meaning a few lines of code would be enough to trick the system into logging into a malicious site. The researchers found a solution that checks the referrer header instead of checking a browser window's location. The improved bookmarklet uses the secure socket layer (SSL) data transfer protocol to prevent the header from being easily forged. The researchers say that in the future a new browser feature called postMessage will enable browser windows to securely transfer information back and forth, providing even better security than the SSL solution.

US Not Ready for Cyber Attack
Reuters (12/19/08), R. Mikkelsen

The results of a two-day cyberwar simulation involving 230 representatives from US government defense and security agencies, private companies, and civil groups found that the United States is not prepared to defend itself against a major hostile attack against its computer networks. The war game simulated a surge in computer attacks during a time of economic vulnerability, and challenged participants to find a way to mitigate the attacks using real-life knowledge of tactics and procedures. The exercise took place almost a year after President Bush launched a cybersecurity initiative aimed at improving US computer defenses. "There isn't a response or a game plan," says M. Gerencser from Booz Allen Hamilton, which ran the simulation. "There isn't really anybody in charge." US Rep. J. Langevin (D-R.I.) says that a successful attack could cause the US's banking or national electrical systems to fail. Both the government and industry need to invest billions of dollars to improve security, says US Rep. D. Ruppersberger (D-Md.). Homeland Security secretary M. Chertoff told participants that cyberattacks will become a routine warfare tactic to damage command systems in preparation for a traditional attack, and that international law and military doctrines need to be updated to address cyberattacks.

'Smart' Surveillance System May Tag Suspicious or Lost People
Ohio State University Research News (12/16/08), P. F. Gorder

Ohio State University (OSU) researchers are developing a computerized surveillance system that incorporates video cameras, large video screens, and geo-referencing software to detect when someone is acting suspicious or appears to be lost. OSU professor J. Davis and doctoral student K. Sankaranarayanan say they have completed the first three phases of the project, including a software algorithm that creates a wide-angle panoramic view of a street scene, another that maps the panorama into a high-resolution aerial image, and a method for actively tracking a target. The final goal is a network of smart video cameras that will enable surveillance officers to quickly and efficiently observe a wide area, with computers managing much of the work. "In my lab, we've always tried to develop technologies that would improve officers' situational awareness, and now we want to give that same kind of awareness to computers," Davis says. The system is designed to analyze and model the behavior patterns of people and vehicles moving in an area. "We are trying to automatically learn what typical activity patterns exist in the monitored area, and then have the system look for typical patterns that may signal a person of interest--perhaps someone engaging in nefarious behavior or a person in need of help," Davis says. The system takes a series of snapshots from numerous directions to create a 360-degree, high-resolution view of the camera's entire viewing area. The researchers are exploring adding touch-screen capabilities to the system.