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

Δελτίο 127
31 Αυγούστου 2008

Risk Assessment Planned for Voting Systems
Government Computer News (08/19/08), W. Jackson

The Election Assistance Commission (EAC) wants to conduct a formal risk assessment of voting systems to identify an acceptable level of risk, as well as appropriate security controls, for all types of voting systems used in federal elections. The assessment will apply principles established in the Federal Information Security Management Act (FISMA), as well as procedures and guidelines for FISMA compliance created by the National Institute of Standards and Technology. Although the EAC does not have authority over state and local jurisdictions, the commission provides a set of voluntary guidelines for certifying voting systems used in many states. The EAC has released a request for proposals for a contractor to conduct a "scientifically founded voting system risk assessment." The commission is looking for a multidisciplinary team of academic researchers, security and software engineers, security professionals, and election administration professionals to conduct the work. The first phase will produce reference models for election processes to define the operational context in which voting systems are used, and models for each generic type of voting system, such as paper ballot, optical scan, or Direct Recording Electronic machines. The second phase will analyze risks associated with each technology and perform assessments of potential harm from those risks. The third phase will identify an acceptable level of impact for voting systems.

Simple and Secure Networked Home
ICT Results (08/18/08)

The European Union-funded ESTIA project has demonstrated software that enables a person to control audiovisual equipment and other products in the home through a single, remote interface. Networked devices are automatically recognized by the system, and the network can be administered using a variety of home electronics, including TV, cordless phones, PDA, or a PC. An increasing number of home-based electronics are being manufactured with networking and remote-control capabilities, even washing machines, dryers, and ovens, but few people are using these features. ESTIA lead researcher L. Dittmann says this is because people perceive the control of networked devices as too complicated, particularly because most networkable devices have their own proprietary control systems, and due to trust and control issues. The ESTIA researchers aimed to address these issues by creating an interface that gives users a personal identity with different access rights to different networked devices. For example, the interface enables people entering the house to type in a four-digit code on a pad by the door, allowing the house to monitor who is there. If an adult is in the house, the children would be allowed to use the oven or microwave, but if the children are home alone their access may be limited to the TV. The ESTIA home networking architecture selects and uses whatever networking technologies are available, from IP-based networks to KNX, a wire-based platform for building control systems.

Planning to E-Vote? Read This First
Scientific American (08/18/08), L. Greenemeier

With less than three months until the US presidential election, many states continue to struggle with electronic-voting technology. In an effort to avoid the problems that plagued the 2000 presidential election, and to meet the requirements of the 2002 Help America Vote Act, many states and counties rushed to obtain e-voting systems, but now those machines also are problematic. Faulty e-voting systems could allow voters and pool workers to place multiple votes, crash the system with a virus, create fake vote tallies, and cause miscounts through other errors, according to studies commissioned by California and Ohio within the past year. "Nothing we do now will affect the November election," says Stanford University professor and Verified Voting Foundation founder D. Dill. "We don't know how to make secure paperless voting." In Ohio, problems with e-voting technology have cost the state $112 million, including discrepancies during the primary election when the county board of elections determined that the Premier DRE system malfunctioned and failed to count votes from memory cards uploaded to the system's vote tabulation computer server. Ohio secretary of State J. Brunner commissioned Project EVEREST to study e-voting technology throughout Ohio. The team of academics and private researchers found exploitable weaknesses in all three e-voting vendors' systems. EVEREST researcher and Pennsylvania State University professor P. McDaniel says e-voting systems have to be completely redesigned with security in mind, which, in the short term, means adding more thorough vote-auditing capabilities so discrepancies can be investigated.

E-Voting Vendor: Programming Errors Caused Dropped Votes
IDG News Service (08/22/08), G Gross

Premier Election Solutions, formerly known as Diebold Election Systems, admitted that its machines have dropped votes, saying a programming error caused hundreds of votes to be dropped in Ohio's March primary elections. The votes were dropped as the machines' memory cards were uploaded to vote-counting servers. Premier originally blamed the error on antivirus software, but the company now admits that a logic error in the machines' GEMS source code caused the miscount. "We now have reason to believe that the logic error in the GEMS code can cause this event when no such antivirus program is installed on the server," wrote Premier president D. Byrd in a letter to Ohio Secretary of State J. Brunner. "We are indeed distressed that our previous analysis of this issue was in error." Premier's C. Riggall says the antivirus software could trigger the error, but it is not the underlying problem, and Premier's earlier analysis was incomplete. Premier also released a product advisory notice, warning users of its electronic-voting machines running some versions of the GEMS software and informing them on how to avoid vote loss. Riggall says Premier has developed a fix for the logic error, which is now being tested. Premier also has submitted a version of the GEMS software for federal certification, but the new software will not be certified before the US elections in November.

A New Breed of Hackers Tracks Online Acts of War
Washington Post (08/27/08) P. D1; K. Hart

Investigators at the University of Toronto's Citizen Lab are monitoring the use of cyber attacks in international warfare. While many of the investigators joined the Citizen Lab to help residents in countries that censor online content, the evolving demands of the Internet have shifted their focus to cyber attacks, how traffic is routed through countries, where Web sites are blocked, and how Internet traffic patterns form. The Citizen Lab started as a collaborative effort with Harvard Law School and Cambridge and Oxford universities to track patterns of Internet censorship in countries that use filters. Citizen Lab researchers developed a software

tool called Psiphon to help users bypass such Internet filters. However, over the past year the researchers have had to increase their efforts to gather evidence on Internet assaults, as online attacks are becoming increasingly important to military strategies and political struggles. Before Russia invaded Georgia in early August, the Citizen Lab noticed sporadic attacks aimed at several Georgian Web sites. Such attacks would be particularly effective against countries that rely on critical online activities such as online banking. After the ground war started, massive raids on Georgia's Internet infrastructure were deployed using techniques similar to those used by Russian criminal organizations, which was followed by attacks from individuals who found online instructions for launching their own attacks, crippling much of Georgia's communication systems. Weeks later, researchers are still trying to find the origin of the attacks.

Revealed: The Internet's Biggest Security Hole
Wired News (08/26/08), K. Zetter

Eavesdropping via Border Gateway Protocol (BGP) is no longer a theoretical vulnerability, as demonstrated by security researchers A. Kapela and A. Pilosov at the recent DefCon hacker conference. They unveiled a method that exploited the protocol so that they could silently monitor and intercept unencrypted Internet traffic bound for the conference network and reroute it to a system they controlled, and it is feared that this tactic could be used to commit corporate espionage, nation-state surveillance, and data mining by intelligence agencies without the need for ISP cooperation. Kapela said the security hole is not an actual software bug or protocol error, but rather a flaw that stems from "the level of interconnectivity that's needed to maintain this mess, to keep it all working." BGP's trust-based architecture makes the protocol vulnerable to claims from unfriendly routers that they are trustworthy, and Pilosov and Kapela have eliminated the outages such hijacks typically generate by forwarding the intercepted data surreptitiously to the actual destination. To prevent the data from boomeranging back to the attacker, the researchers employ Autonomous System (AS) path prepending that causes a chosen number of BGP routers to reject their deceptive advertisement, and then use these ASes to route the captured data to the appropriate recipients. Kapela noted that ISPs could prevent BGP eavesdropping by aggressively filtering to permit only authorized peers to draw traffic from their routers, and only for particular IP prefixes. The problem lies in the enormous amount of work this would entail, and the unaffordable cost of performing such filtering on a global scale. D. Maughan with the Dept. of Homeland Security's Science and Technology Directorate concluded that "the only thing that can force [ISPs to fix BGP] is if their customers ... start to demand security solutions."

Carnegie Mellon System Thwarts Internet Eavesdropping
Carnegie Mellon News (08/25/08), B. Spice

Carnegie Mellon University researchers have developed Perspectives, a Web security system that can prevent man-in-the-middle (MitM) Internet eavesdropping attacks. Perspectives also can protect against attacks that exploit the recently disclosed flaw in the Domain Name System. The researchers have incorporated Perspectives into a free Mozilla Firefox extension. Perspectives uses a set of friendly sites, or notaries, to authenticate Web sites for financial services, online retailers, and other transactions that require secure communications. By independently querying the desired target site, the notaries can check to see if each site is receiving the same authentication information, or digital certificate, in response. If one or more notaries report authentication information that is not the same as the information received by the browser of other notaries, a user would have reason to suspect that the connection has be-

en compromised. Although certificate authorities already help authenticate Web sites to reduce the risk of MitM attacks, Perspectives adds another layer of security and will be particularly useful when visiting sites that use self-signed certificates instead of certificate authorities. Perspectives also can detect if a certificate authority has been tricked into authenticating a fake Web site and warn the user that the site may be compromised.