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

Δελτίο 158
15 Σεπτέμβρη 2009

Filtering Network Attacks With a 'Netflix' Method
Dark Reading (08/28/09), J. Higgins

University of California, Irvine (UC Irvine) researchers have developed a new method for blacklisting spam, distributed denial-of-service attacks, worms, and other network attacks. The predictive blacklisting method, which was inspired by Netflix's moving ratings-recommendation system, uses a combination of factors to improve blacklisting, including trends in the times of attacks, geographical locations and IP address blocks, and any connections between the attacker and the victim, such as if an attacker has previously challenged the victim's network. UC Irvine professor A. Markopoulou says the predictive blacklisting method "formalizes the blacklisting problem" in regards to predicting the sources of attacks. The researchers found that their method improves predictive blacklisting, accurately predicting up to 70% of attacks. "The hit-count of our combined method improves the hit-count of the state of the art for every single day," Markopoulou says. She says the method could be applied to security logs gathered by firewalls, for example, helping an enterprise better defend itself against attacks. The researchers tested their algorithms using hundreds of millions of logs from hundreds of networks, gathered over a one-month period. Markopoulou says the next step is to improve the prediction rate and to understand how attackers could evade the prediction method.

Still Trying to Crack Nazi Enigma Messages
Network World (08/31/09), B. Brown

Enigma@home is attempting to break one of three original messages generated by the Enigma machine, which was intercepted in 1942. The Enigma M4 machine is believed to have been used by Germany to encipher the signals during the war. German-born violinist and encryption enthusiast S. Krah spearheaded the launch of the M4 Project in January 2006, and the first two messages were broken in a couple of months. Krah worked on the challenge messages of S. Singh's Cipher Challenge after the actual challenge was over and improved the algorithm so that real world messages could be broken. The algorithm was refined further with the help of a publication by G. Sullivan and F. Weierud. The M4 Project is relying on computer users to donate their spare PC processing power for the cause. "The three messages that are the target of the M4 Project were interesting for three main reasons: They were unbroken, published in a serious journal, and encrypted by the M4 Enigma model," says Krah. "This model has the largest key space of all and breaking these messages pretty much requires a distributed computing project."

Privacy Plug-In Fakes Out Facebook
Technology Review (09/09/09), R. Lemos

University of Waterloo, Ontario researchers have developed FaceCloak, a browser plug-in that shields social network users' private data from both malicious users and social network providers. Waterloo professor U. Hengartner says the plug-in replaces sensitive information in a user's profile with news feeds and meaningless text that can only be unscrambled by trusted friends and contacts. Carnegie Mellon University (CMU) professor A. Acquisti says most users are unaware of the privacy implications of posting personal information on social networking sites such as Facebook and MySpace. In 2005, Acquisti and fellow CMU researcher R. Gross found that almost 80% of Facebook users revealed their birthday and the majority provided public access to their real-world address, which could provide enough information to commit identity theft. Acquisti says users have recently started changing their access options to protect their information more carefully, but social network providers have not been good at protecting user privacy because monetizing personal information could result in millions of dollars in revenue. FaceCloak allows users to designate what information should be encrypted and made available only to friends. The user receives a secret access key and sends two other keys to friends. The keys are used to access the real information, which is stored on a separate server. Similar tools are being developed by other academic teams, including a Cornell University plug-in called None of Your Business that encrypts profile information so it can be read only by a small group of friends.

Researchers Find a New Way to Attack the Cloud
IDG News Service (09/03/09), R. McMillan

Researchers at the University of California, San Diego (UCSD) and the Massachusetts Institute of Technology (MIT) have found security holes in Amazon's EC2 cloud-computing service. The researchers were able to execute basic versions of side-channel attacks, in which a hacker looks at indirect information related to the computer to determine what is taking place on the machine. The researchers succeeded in pinpointing the physical servers used by programs running on the EC2 cloud, and then extracted small amounts of data from those programs. Previous research has demonstrated the vulnerability of side-channel attacks. In 2001, University of California, Berkeley researchers were able to extract password information from an encrypted SSH data stream by performing a statistical analysis of how keystrokes generated traffic on the network. By looking at the computer's memory cache, the UCSD and MIT researchers were able to obtain basic information about when other users on the same machine were using a keyboard to perform tasks such as accessing the computer using an SSH terminal. The researchers say that measuring the time between keystrokes enables them to determine what is being typed on the machine. To perform this attack, the researchers had to determine which EC2 machine was running the program they wanted to target, a difficult challenge as cloud computing is supposed to hide this information. However, by performing an analysis of DNS traffic and using a network-monitoring tool, the researchers developed a technique that could provide a 40% chance of placing their attack code on the same server as their target. Security experts say that side-channel techniques could lead to more serious problems for cloud computing.

ACM Statement Regarding British Prime Minister Gordon Brown's Apology on the Treatment of Alan Turing, ACM (09/11/09), W. Hall

ACM applauds Prime Minister Brown's statement on the treatment of Alan Turing, writes Dame Professor W. Hall, ACM President. ACM has long celebrated the fundamental contributions of Alan Turing not only for his instrumental role in British code-breaking efforts that hastened the end of World War II, but for his insights to the mathematical underpinnings of computing and computer science, which continue to drive innovation and produce unimaginable advances in science and technology that have made the world a better place. As a consequence, the most prestigious award in computing and computer science, the A.M. Turing

Award, was established by ACM in 1966, and named after Alan Turing. ACM looks forward to joining with other organizations to celebrate the centenary of Turing's birth in 2012.

A Turing Test for Computer Game Bots
Technology Review (09/10/09), D. Kushner

The BotPrize is a three-month contest in which programmers are challenged to develop a software bot to control a game character that can pass for human, with the goal of devising better artificial intelligence (AI) for games as well as non-game applications. "The BotPrize [is] important for AI in general because it highlights a central question in AI: How is human intelligence related to computer intelligence?" says Edith Cowan University's P. Hingston. The second annual BotPrize competition placed bots in Unreal Tournament 2004, a first-person-shooter game in which the winner is the one that scores the most virtual kills. The humanness of the bots was judged solely on the basis of their physical behavior, and a bot had to fool at least 80% of the judges in order to win the $6,000 prize. Epic Games programmer S. Polge says developers often prefer creating AIs "that can make unexpected plans and present emergent and surprising challenges to the player"--not only because it can improve games, but also because AIs that mimic humans too closely can be as irritating and obnoxious as human opponents. Simulation game creator Will Wright is hoping that the BotPrize fosters an interest among AI researchers to create programs that emulate emotions. "Machine interactions are becoming a ubiquitous part of our environment, but they're not necessarily the most satisfying, so acknowledging our emotional dimension is an interesting task to go for in AI," he says.

Stimulus Funds to Further Cyber Security Research
Penn State Live (09/08/09), J. Spinelle

The American Recovery and Reinvestment Act of 2009 will fund a project designed to protect the privacy and security of business information systems and data centers from cyberattacks. More than $1 million will be awarded over three years to Pennsylvania State University researcher P. Liu, George Mason University researcher S. Jajodia, and Western Illinois University researcher M. Yu. The researchers hope to accelerate customer and supplier services and to ensure secure business information. They will attempt to combine four areas of data security--redundancy, detection and analysis of microscopic intrusion, automatic response, and diversity-driven protection. The researchers say the project could lead to stronger security measures in the business world, increased efficiency in customer and supplier service, and improved data protection in the wake of cyberattacks. "This grant will enable us to take a big stride forward towards building self-protecting and trustworthy information systems and data sets," Liu says. "This project will 'stand on the shoulders' of our recent research achievements in trusted recovery, self-healing information systems, and intrusion-tolerant computing."