

Surviving Unemployment in the High-Tech Downturn

pp. 24-28

Stephen Blanchette Jr.

If your career has progressed relatively undisturbed until now, you probably haven't thought much about being unemployed. However, being prepared for unemployment could be as important as any other career management activity. The author offers tips that can be helpful for those who are newly unemployed—or are proactively considering the possibility. Although falling victim to downsizing or company failure will still be traumatic, knowing what to expect can help to prepare for treating the situation as an adventure, not a catastrophe.

Microsoft .NET Passport: A Security Analysis

pp. 29-35

Rolf Oppliger

Part of its .NET initiative, Microsoft's set of Web services includes .NET Passport, a password-based user authentication and single sign-in service. The system offers a simple and sufficiently secure alternative to privilege-management infrastructures and public-key infrastructure for many applications and services.

Released in 1999 and used in many Web-based applications and services, .NET Passport and its SSI service have been criticized for poor security and privacy. Its centralized nature makes it possible that other problems and security breaches will occur.

Protecting Intellectual Property in Digital Multimedia Networks

pp. 39-45

Ahmet M. Eskicioglu

Computer and communications network improvements offer intellectual-property owners new ways to reproduce, distribute, and market their IP. One problem with digital distribution and

storage technologies, however, is the formidable threat of piracy. Thus, understanding the opportunities provided by the ever-expanding information infrastructure and its impact on digital IP is essential.

Proponents and opponents of protecting IP with technical measures have presented strong arguments. Hopefully, these discussions will lead to a general consensus regarding protection technologies and a common interpretation of consumers' rights in the digital age.

Protecting Cryptographic Keys: The Trace-and-Revoke Approach

pp. 47-53

Dalit Naor and Moni Naor

Technology can offer options that apply any combination of content protection, hardware and software tamper resistance, or cryptographic keys to achieve content-ownership protection. The authors describe two methods for protecting content by creating a legitimate distribution channel. One method broadcasts encrypted data to a selected set of users and uses a tracing algorithm to uncover the compromised key's owner. The other method updates user keys to resecure a compromised network.

A Trusted Open Platform

pp. 55-62

Paul England, Butler Lampson, John Manferdelli, Marcus Peinado, and Bryan Willman

Although administrators can configure a system to restrict access to resources, in a mass-market setting they cannot be sure of the kernel's integrity. The commercial need for an open software and hardware architecture leads to huge and complex operating systems. A single programming error or intentional back door in this code base can open the way for an attack that renders the access-control system ineffective.

The authors describe Microsoft's next-generation secure computing base, a system that offers robust access control

through mechanisms for code authentication.

Preventing Piracy, Reverse Engineering, and Tampering

pp. 64-71

Gleb Naumovich and Nasir Memon

As computing becomes pervasive, concerns about data protection have taken on new urgency. What makes securing digital data so difficult is that it is rarely static—rather, data is manipulated by software, often in a networked environment.

Software is increasingly being distributed as mobile code in architecture-independent formats. Using reverse engineering, malicious parties can steal the intellectual property associated with such code with relative ease. Three promising techniques under development—tamper proofing, obfuscation, and watermarking—offer hope for providing more efficient and effective mechanisms for protecting software.

Technical Challenges of Protecting Digital Entertainment Content

pp. 72-78

C. Brendan S. Traw

The technology of a decade ago made digital copying and redistribution of entertainment content generally infeasible. Today, personal computers offer a platform that lets consumers easily alter a manufacturer's functionality—defeating measures to protect content brought into the PC's open, reprogrammable environment.

Thus, content-protection technology now plays an important role in creating an environment conducive to the long-term success of businesses based on digital information. While solutions based on a combination of technological and licensing mechanisms can effectively protect valuable entertainment assets from unauthorized copying and redistribution, they have limitations.