DEPARTMENT: DEPARTMENTS

Celebrating 50 Years of the Turing Award

To celebrate the first 50 years of the A.M. Turing Award, ACM is sponsoring a yearlong series of programs, as highlighted on the Turing 50th website http://www.acm.org/turing-award-50.

Vicki L. Hanson

Page 5

Social and Ethical Behavior in the Internet of Things

"Denial-of-service" cyberattacks require us to up our technical game in Internet security and safety. They also expose the need to frame and enforce social and ethical behavior, privacy, and appropriate use in Internet environments …

Francine Berman, Vinton G. Cerf

Pages 6-7

DEPARTMENT: LETTERS TO THE EDITOR

Use the Scientific Method in Computer Science

Adi Livnat's and Christos Papadimitriou's critique of genetic algorithms in "Sex as an Algorithm" (Nov. 2016) stands in counterpoint to a voluminous empirical record of practical successes.

CACM Staff

Pages 8-9

DEPARTMENT: PANELS IN PRINT

Artificial Intelligence

To help celebrate 50 years of the ACM Turing Award and the visionaries who have received it, ACM has launched a campaign called "Panels in Print," which takes the form of a collection of responses from Turing laureates, ACM award …

CACM Staff

Pages 10-11

DEPARTMENT: BLOG@CACM

Liberal Arts Academia Wants YOU!

Janet Davis makes a plea to CS practitioners to consider even a short teaching stint.

Janet Davis

Pages 12-13

COLUMN: NEWS

Secure Quantum Communications

Data locking experiments provide stepping stones to a possible future in quantum cryptography.

Chris Edwards

Pages 15-17

Are Computer Chips the New Security Threat?

Security researchers have identified a technique for installing a backdoor on computer chips, a security flaw that could profoundly change the computing industry.

Samuel Greengard

Pages 18-19

It's Not the Algorithm, It's the Data

In risk assessment and predictive policing, biased data can yield biased results.

Keith Kirkpatrick

Pages 21-23

COLUMN: INSIDE RISKS

The Future of the Internet of Things

The IoT can become ubiquitous worldwide — if the pursuit of systemic trustworthiness can overcome the potential risks.

Ulf Lindqvist, Peter G. Neumann

Pages 26-30

COLUMN: EDUCATION

Fostering Creativity Through Computing

How creative thinking tools and computing can be used to support creative human endeavors.

Aman Yadav, Steve Cooper

Pages 31-33

COLUMN: KODE VICIOUS

The Unholy Trinity of Software Development

Tests, documentation, and code.

George V. Neville-Neil

Pages 34-36

COLUMN: PRIVACY AND SECURITY

User-Centric Distributed Solutions for Privacy-Preserving Analytics

How can cryptography empower users with sensitive data to access large-scale computing platforms in a privacy-preserving manner?

Azer Bestavros, Andrei Lapets, Mayank Varia

Pages 37-39

COLUMN: VIEWPOINT

Smart Machines Are Not a Threat to Humanity

Worrying about machines that are too smart distracts us from the real and present threat from machines that are too dumb.

Alan Bundy

Pages 40-42

AI Dangers: Imagined and Real

Arguing against the arguments for the concept of the singularity.

Devdatt Dubhashi, Shalom Lappin

Pages 43-45

SECTION: PRACTICE

Life Beyond Distributed Transactions

An apostate's opinion.

Pat Helland

Pages 46-54

Are You Load Balancing Wrong?

Anyone can use a load balancer. Using it properly is much more difficult.

Thomas A. Limoncelli

Pages 55-57

BBR: Congestion-Based Congestion Control

Measuring bottleneck bandwidth and round-trip propagation time.

Neal Cardwell, Yuchung Cheng, C. Stephen Gunn, Soheil Hassas Yeganeh, Van Jacobson

Pages 58-66

SECTION: CONTRIBUTED ARTICLES

Copyright Enforcement in the Digital Age: Empirical Evidence and Policy Implications

Government-sanctioned and market-based anti-piracy measures can both mitigate economic harm from piracy.

Brett Danaher, Michael D. Smith, Rahul Telang

Pages 68-75

Computing History Beyond the U.K. and U.S.: Selected Landmarks from Continental Europe

It is past time to acknowledge 400 years of European computational innovation from non-English-speaking scientists and engineers.

Herbert Bruderer

Pages 76-84

SECTION: REVIEW ARTICLES

Model Learning

Model learning emerges as an effective method for black-box state machine models of hardware and software components.

Frits Vaandrager

Pages 86-95

SECTION: RESEARCH HIGHLIGHTS

Technical Perspective: Cleaning Up Flaws in TLS Implementations

One unfortunate fact about protocols is that as they get older and applied to more scenarios — and TLS is used basically everywhere — they tend to gain weight. A truism of the security community is that "complexity is the enemy …

Eric Rescorla

Page 98

A Messy State of the Union: Taming the Composite State Machines of TLS

We systematically test popular TLS implementations and find unexpected transitions in many of their state machines that have stayed hidden for years. We show how some of these flaws lead to critical security vulnerabilities. …

Benjamin Beurdouche, Karthikeyan Bhargavan, Antoine Delignat-Lavaud, Cédric Fournet, Markulf Kohlweiss, Alfredo Pironti, Pierre-Yves Strub, Jean Karim Zinzindohoue

Pages 99-107

Authentication Using Pulse-Response Biometrics

We propose a new biometric based on the human body's response to an electric square pulse signal, called *pulse-response*.

Ivan Martinovic, Kasper Rasmussen, Marc Roeschlin, Gene Tsudik

Pages 108-115

COLUMN: LAST BYTE

Fatal Guidance

In a series of interactive murder mysteries, I might not have done it, but, then again, maybe I did

William Sims Bainbridge

Pages 120-ff