PURSUIT OF ZΩH — THE WEEKLY

This Week in

Computer Science

NO. 007 • 15 NOVEMBER 2026 • NEWS OF 8 NOV – 15 NOV 2026 • 4 STORIES

THIS WEEK

Sleepy clicks, quiet alarms and a hard game of stones

The spring clock change made university staff likelier to click a phishing link, a language model quietly silences a code scanner's warnings, a chip naps on nanowatts, and generalized Kalah turns out to be PSPACE-complete.

IN THIS ISSUE

01 HUMAN FACTORS IN SECURITY
One lost hour of sleep, more clicks on a phishing link

02 SOFTWARE SECURITY
Small rewrites hide real bugs from a code scanner

03 COMPUTER ARCHITECTURE
A programmable chip that sleeps on 24.9 nanowatts

04 COMPLEXITY OF GAMES
Kalah, the stone-sowing game, is PSPACE-complete

01

HUMAN FACTORS IN SECURITY

One lost hour of sleep, more clicks on a phishing link

Phishing defenses usually target filters and training, but the person reading the email has off days too.[1] A University of California, Irvine study sent a simulated phishing email to 11,218 employees, randomly assigned to receive it on the Monday right after the spring 2026 switch to daylight saving time or one week earlier.[1,2] After the clock change, the chance of clicking the suspicious link rose by about 13%.[1] The click rate was 17.76%, against 15.56% the week before.[2] Opening the email and reporting it as spam did not change.[1]

WHY IT MATTERS

A single lost hour is about as mundane as sleep loss gets, yet it showed up in real security behavior; the author urges extra vigilance around clock changes and other sleepy stretches such as holidays.[1,2]

CAVEAT *One institution and one clock change; the transition stands in for lost sleep, which was not measured in each person.*[1]

~13%

rise in the chance of clicking a phishing link on the Monday after the spring clock change

SOURCE 1

[1] doi:10.1073/pnas.2622467123 · [2] eurekalert.org

ON THE ROAD?

Listen to this issue

6-minute episode, read aloud: the same four stories, written for the ear. Stream it, or download the MP3, from the Computer Science page.

pursuit-of-zoe.com/pages/computer-science#zoh-weekly

02

SOFTWARE SECURITY

Small rewrites hide real bugs from a code scanner

When a security scanner's warning vanishes after a code change, developers tend to assume the bug left with it.[3] A team tested that habit against CodeQL's taint tracking for JavaScript, which follows untrusted data through a program.[3] A large language model, shown only the alert, rewrote one function as a routine-looking maintenance edit that kept the flaw.[3] Across 172 flows from real npm vulnerabilities, three rewrites per flow silenced 26.2% of them, at about USD 0.51 per silenced flow.[3] Asked merely to refactor, the same model silenced none.[3]

26.2%

of 172 CodeQL-detected flows silenced by three flaw-preserving rewrites each

SOURCE 3

WHY IT MATTERS

A disappearing alert is weak evidence of a fix: 74% of the silencing rewrites also slipped past a separately built taint analyzer.[3] The misses trace to seven specific gaps, giving tool builders concrete targets.[3]

CAVEAT *Preprint, not yet peer reviewed; tested on JavaScript taint tracking only.*[3]

[3] arxiv.org

03

COMPUTER ARCHITECTURE

A programmable chip that sleeps on 24.9 nanowatts

Sensors spread over a flexible pad spend most of their time waiting for something to press on them, and a general-purpose microcontroller wastes power holding on to its state.[4] A Jiangnan University team built Pico-X, an eight-bit programmable processor designed to keep as little state as possible.[4] Made in a 28-nanometer fully depleted silicon-on-insulator process, it draws 24.9 nanowatts in a deep sleep that retains its state and 728.2 nanowatts when active at 25 kilohertz.[4] On a 4 × 4 pad demonstrator it recorded 12,842 events.[4]

24.9 nW

power in state-retentive deep sleep, without body bias (Pico-X, 28 nm FD-SOI)

SOURCE 4

WHY IT MATTERS

Hardwired controllers save power by giving up programmability; this design aims to keep both for sensors that must lie dormant yet react quickly.[4]

CAVEAT *A demonstrator that ran stably for more than 72 hours, with recall of 92.1% to 96.3% across three event classes; not a field deployment.*[4]

[4] doi:10.1038/s41467-026-79332-9

04

COMPLEXITY OF GAMES

Kalah, the stone-sowing game, is PSPACE-complete

Kalah is a two-player mancala game in which players sow stones from pit to pit, capturing some and banking them in a store.[5] Computers have solved several standard starting positions, but how hard the game gets on ever larger boards was open.[5] In a preprint, Ethan Dickey and Ethan Mader show that deciding whether a player can force a win from a given position, with the number of pits part of the input, is PSPACE-complete.[5] It holds under both common capture rules, with or without the free extra turn.[5]

MECHANISM

Start from a quantified Boolean formula

↓

Line Kalah: save target pits from capture

↓

Timer piles force one choice per variable

↓

A final capture tests one clause

↓

Embed the line in Kalah, stores empty

WHY IT MATTERS

It settles the difficulty of a classic sowing game on growing boards, placing it among the hardest problems that can be solved with polynomial memory.[5]

CAVEAT *Preprint, not yet peer reviewed; the hard cases are arbitrary positions on large boards with stone counts written in unary, not the usual opening.*[5]

[5] arxiv.org

WORDS THIS WEEK

Phishing
A fake message, usually email, built to trick someone into clicking a link, opening a file or handing over a password.

Silicon-on-insulator
A chipmaking process that builds transistors on a thin silicon layer over an insulating one, which helps cut leakage current and power.

Static analysis
Inspecting source code for bugs or security flaws without running it. Security teams often run such tools on every code change.

Recall
Of all the real events of one kind, the share a detector correctly catches.

Taint tracking
Following data from an untrusted source, such as user input, through a program to see whether it can reach a dangerous operation unchecked.

PSPACE-complete
Among the hardest problems that can be solved using an amount of memory that grows only polynomially with the input size.

SOURCES

1. PAPER E. Schechtman, “Modest loss of sleep increases susceptibility to cybersecurity threats,” Proceedings of the National Academy of Sciences (11 Nov 2026). doi:10.1073/pnas.2622467123
2. RELEASE University of California, Irvine, “Modest loss of sleep raises email phishing risk,” news release via EurekAlert (9 Nov 2026). https://www.eurekalert.org/news-releases/1150614
3. PREPRINT Z. Cao et al., “Preserve the Vulnerability, Break the Alert: Testing the Robustness of CodeQL Taint Tracking with Natural Rewrites,” arXiv:2611.17123 preprint (12 Nov 2026). https://arxiv.org/abs/2611.17123
4. PAPER Y. Xiong et al., “Pico-X: a 24.9 nanowatt microcontroller for long-duration autonomous operation in flexible landing-pad sensor networks,” Nature Communications (10 Nov 2026). doi:10.1038/s41467-026-79332-9
5. PREPRINT E. Dickey & E. Mader, “Sowing the Seeds of Intractability: Kalah is PSPACE-complete,” arXiv:2611.17252 preprint (12 Nov 2026). https://arxiv.org/abs/2611.17252

How this is made. Each story comes from the past seven days of journal, agency and society releases and is written fresh for curious minds, with a source for every claim. Superscripts refer to the list above. Spotted an error? Tell us through the contact page; corrections run in the next issue.

Choose what we feature next. Signed-in customers vote every other week at pursuit-of-zoe.com/pages/vote.