Safe embedded OS with multi-programming and compile-time isolation

Secure IPv6 mesh networking over low-power wireless via 6LoWPAN and 802.15.4
Finding and Preventing Bugs in JavaScript Bindings

81 bugs · Bountied security errors · Google Chrome & PDFium · DANGER!

We write static checkers to identify bugs at the boundary between JavaScript and C++ in runtime systems...

...and create an API to prevent these bugs by construction

Fraser Brown, Shravan Narayan, Riad S. Wahby, Dawson Engler, Ranjit Jhala, Deian Stefan
Bulletproofs

SHORT PROOFS FOR CONFIDENTIAL TRANSACTIONS AND MORE

Benedikt Bünz, Jonathan Bootle, Dan Boneh, Andrew Poelstra, Pieter Wuille, Greg Maxwell
Conserving Microcontroller Energy through Dynamic Clock Selection

- RCSYS
- RCFAST
- PLL
- DFLL
- RC80M
- OSC0

Main Clock
- RCSYS
- RCFAST
- DFLL

Clients
- CPU
- UART
- SPI
- CPU
- UART
- SPI
ObliDB: An Oblivious General-Purpose SQL Database for the Cloud

Saba Eskandarian and Matei Zaharia
Salsify: Low-Latency Network Video Through Tighter Integration Between Video Codec and Transport Protocol

• Salsify is a real-time video system with **3.9x lower delay** and **2.7 dB higher visual quality**, on average, compared to FaceTime, Hangouts, Skype, and WebRTC.

• Three major design improvements:
  • Video-Aware Transport Protocol
  • Functional Video Codec
  • Unified Control Loop

S. Fouladi, J. Emmons, E. Orbay, C. Wu, R. Whaby, K. Winstein
Fonduer: Knowledge Base Construction from Richly Formatted Data
Sen Wu, Luke Hsiao, Xiao Cheng, Braden Hancock, Theodoros Rekatsinas, Philip Levis, Christopher Ré

**Input:** Richly formatted documents (e.g. PDF/HTML/XML/etc.) → **Output:** Structured knowledge base

**Challenges:**
1. Prevalent document-level relations
2. Multimodal information
3. Data variety

**Used by:**

Blog: [hazyresearch.github.io/snorkel/blog/fonduer](https://hazyresearch.github.io/snorkel/blog/fonduer)
Code: [github.com/HazyResearch/snorkel/tree/fonduer](https://github.com/HazyResearch/snorkel/tree/fonduer)
CESEL

- IoT needs crypto acceleration + flexibility

- Our solution: CESEL
  - Wide SIMD + long word support
  - Special instructions (permute, bitslice)
  - No data-dependent control flow

- Significant energy savings compared to software
  - \(~5x\) for most ciphers
  - \(1.5x\) longer deployment time
Users often need to delegate their SSH credentials to remote partially-trusted hosts (e.g., to `git clone` from GitHub to AWS).

The popular `ssh-agent forwarding` offers minimal visibility—putting user’s credentials at risk.

**Guardian Agent** allows the user to verify and enforce security policies: who can do what to whom with the user’s credentials.
Finding low-magnitude earthquakes in years of continuous seismic data streams


Want to detect new earthquakes:
- Scale invariant
- Recurring
- Under low SNR
- Without relying on labeled events

New method based on waveform similarity

Challenge: How to scale up from 3 month at 1 station to 10 years at multiple stations
Verifiable universal two-factor (u2f) tokens

R.S. Wahby (Stanford), M. Howald (The Cooper Union), S. Garg (NYU), a. shelat (Northeastern), M. Walfish (NYU); R.S. Wahby, Y. Ji (NYU), A.J. Blumberg (UT Austin), a. shelat, J. Thaler (Georgetown), M. Walfish, T. Wies (NYU); R.S. Wahby, I. Tzialla (NYU), a. shelat, J. Thaler, M. Walfish; R.S. Wahby, Keith Winstein (Stanford), D. Mazières (Stanford)

U2F: hardware-backed authentication using public-key cryptography

What could go wrong?

e.g., kleptography: turning crypto against you

Our solution: make tokens verifiable with special- and general-purpose protocols