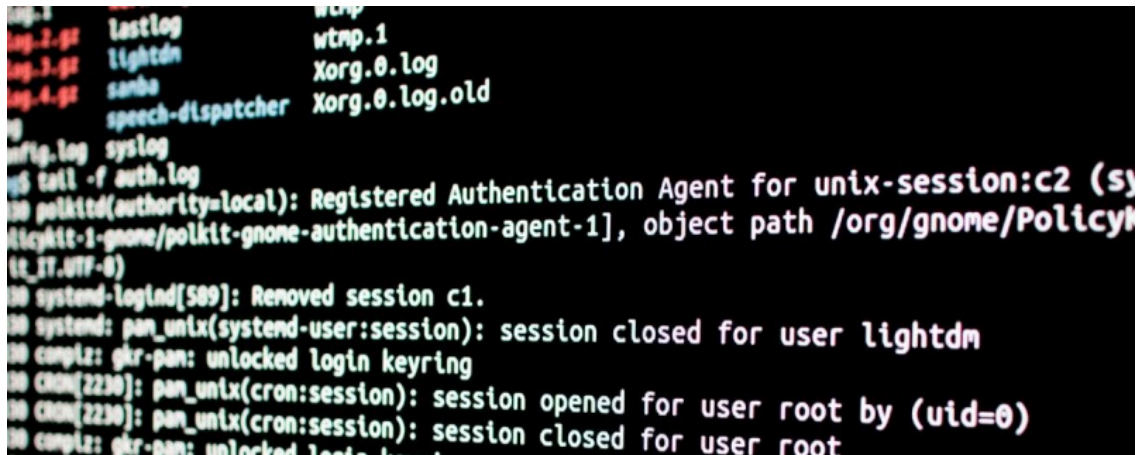


SEI Bulletin

Trouble reading this email? [View in browser.](#)



```
lastlog      wtmp.1
lightdm      Xorg.0.log
sanba        Xorg.0.log.old
speech-dispatcher
syslog
tail -f auth.log
polkitd(authority=local): Registered Authentication Agent for unix-session:c2 (sy
policykit-1-gnome/policykit-gnome-authentication-agent-1], object path /org/gnome/Policyk
(1_17.077-0)
systemd-logind[509]: Removed session c1.
system: pam_unix(systemd-user:session): session closed for user lightdm
complz: gkr-pan: unlocked login keyring
cron[2230]: pam_unix(cron:session): session opened for user root by (uid=0)
cron[2230]: pam_unix(cron:session): session closed for user root
complz: gkr-pan: unlocked login keyring
```

SEI Researchers Talk Large Language Models for Cybersecurity

August 14, 2024—Large language models (LLMs) have impacted many digital domains, but how do they apply to cybersecurity? In a recent SEI Podcast, Jeff Gennari and Sam Perl, researchers in the SEI’s CERT Division, discussed applications of LLMs and generative AI in cybersecurity, how to evaluate those applications, and the potential challenges.

“Every problem that we have in cybersecurity...can be impacted by large language models,” said Gennari in the podcast Evaluating Large Language Models for Cybersecurity Tasks: Challenges and Best Practices. “The space is also changing how we think about cybersecurity. The attack surface of our systems is changing when they have AI components.”

“Machine learning has been used in cybersecurity quite extensively,” said Perl. “We are talking about much more advanced sort of techniques in those areas and what will come next and how will it be used.”

[Listen to the podcast »](#)



[SEI Launches Course on Developing a National or Government Computer Security Incident Response Team](#)

The new course is intended to help nations develop robust cybersecurity capabilities.

[Ozkaya Explores Generative AI in Software Architecture During International Conference Keynote](#)

The IEEE International Conference on Software Architecture is the premier event for the field's researchers and practitioners.

[**See more news »**](#)



[Weaknesses and Vulnerabilities in Modern AI: AI Risk, Cyber Risk, and Planning for Test and Evaluation](#)

Bill Scherlis explores strategies for framing test and evaluation practices based on a holistic approach to AI risk.

[Weaknesses and Vulnerabilities in Modern AI: Integrity, Confidentiality, and Governance](#)

Bill Scherlis explores AI risk through the lens of confidentiality, governance, and integrity.

[Weaknesses and Vulnerabilities in Modern AI: Why Security and Safety Are so Challenging](#)

Bill Scherlis explores concepts of security and safety for neural-network-based AI, including ML and generative AI, as well as AI-specific challenges in developing safe and secure systems.

[**See more blogs »**](#)



Latest Podcasts

[Evaluating Large Language Models for Cybersecurity Tasks: Challenges and Best Practices](#)

Jeff Gennari and Sam Perl discuss applications for LLMs in cybersecurity, potential challenges, and recommendations for evaluating LLMs.

[Capability-Based Planning for Early-Stage Software Development](#)

Bill Nichols and Anandi Hira introduce capability-based planning (CBP) and its use and application in software acquisition.

[See more podcasts »](#)



Latest Videos

[Generative AI and Software Engineering Education](#)

SEI experts in software engineering discuss how generative AI is influencing software engineering education.

[Secure Systems Don't Happen by Accident](#)

Timothy A. Chick discusses how security is an integral aspect of the entire software lifecycle.



Latest Publications

[On the Design, Development, and Testing of Modern APIs](#)

This white paper discusses the design, desired qualities, development, testing, support, and security of modern application programming interfaces (APIs).

[A Model Problem for Assurance Research: An Autonomous Humanitarian Mission Scenario](#)

This report describes a model problem to support research in large-scale assurance.

[Application Programming Interface \(API\) Vulnerabilities and Risks](#)

This report describes 11 common vulnerabilities and 3 risks related to application programming interfaces and provides suggestions about how to fix or reduce their impact.

[See more publications »](#)



[Upcoming Events](#)

Webcast - [Embracing AI: Unlocking Scalability and Transformation Through Generative Text, Imagery, and Synthetic Audio](#), August 27

In this free webcast, Tyler Brooks, Shannon Gallagher, and Dominic Ross aim to illustrate AI's transformative power in achieving scalability, adapting to changing landscapes, and driving digital innovation.

[DevSecOps Days Washington D.C. 2024](#), September 18

This free, in-person event in Arlington, Virginia, will teach how to integrate security into DevOps practices and transform DevSecOps journeys.

[International Conference on Conceptual Modeling \(ER 2024\)](#), October 28-31

The SEI will host the main international forum for discussing the state of the art, emerging issues, and future challenges in research and practice on conceptual modeling.

[See more events »](#)



[Upcoming Appearances](#)

[Emerging Technologies for Defense Conference & Exhibition 2024](#), August 7-9

Visit the SEI at booth 316.

[Billington CyberSecurity Summit](#), September 3-6

Hear the SEI's Greg Touhill, Mark Sherman, and Nathan VanHoudnos at the leading government cybersecurity summit, and visit the SEI at booth 320.

[TechNet Indo-Pacific 2024](#), October 22-24

Visit the SEI at booth 1411.

[27th Annual Systems & Mission Engineering Conference](#), October 28-31

Visit the SEI booth at this event.

[See more opportunities to engage with us »](#)



[Upcoming Training](#)

[Insider Risk Management: Measures of Effectiveness](#)

October 29-31 (SEI Live Online)

[Risk Program Development - Governance and Appetite Workshop](#)

November 13-14 (SEI Arlington, Va.)

[See more courses »](#)



[Employment Opportunities](#)

[Technical Manager - Cybersecurity Assurance Team](#)

[Software Development Technical Lead](#)

[Senior Administrative Coordinator](#)

[All current opportunities »](#)

Carnegie Mellon University
Software Engineering Institute



Copyright © 2024 Carnegie Mellon University Software Engineering Institute, All rights reserved.

Want to subscribe or change how you receive these emails?
You can [subscribe](#), [update your preferences](#) or [unsubscribe from this list](#).