26 for 26
26 Things to Know/Try for a Better 2026

January 21, 2026

By Aaron Grothe
NEbraskaCERT

Introduction

26 for 26?

I did a 12 for 12 talk in 2012 and have just kept going from there. Used to say I was in a rut now describe it as a groove.

Links are at the end of the talk
Slides are posted at the NEbraskaCERT website http://www.nebraskacert.org/csf I'll also be posting them at my personal website https://www.grothe.us in the presentations section

Introduction (Continued)

If you have questions/comments please feel free to ask them anytime. You don't have to hold them until the end of the talk.

If there are other resources similar to these that you think might be useful to people please let the group know.

Hopefully this will be an interactive and productive session.

Introduction

Something New

Usually I start putting together the talk in August/September from notes earlier in the year and then continue to refine it until I give it in January. Replace a tip with a stronger one and so on.

This year I've made my google doc with the master list of the tips I considered for this year. You can hit the list at https://docs.google.com/document/d/1IDA1JJ4muo9YP_SPFhooQLc4Y2HerR5TN2eamnq5Ge0/edit?usp=sharing

Trends Going into 2026

5 Major Things This Year

1. Cost of computers/computing is going to continue to go up in 2026. Memory is spiking, Nvidia is shipping 40% less consumer GPUs, continued AI use of limited resources
2. AI - everywhere. Impact for the time for a patch being released and an exploit in the wild has shortened dramatically
3. Is Open Source reaching a breaking point. Licenses under attack, Open Source projects are being used by huge companies expecting 24x7 support for free, etc.
4. Innovation is happening. Rust based Kernels, migration to memory safe languages
5. Is this the year the AI bubble bursts???

Tip - Ransomware as a Company

- Ransomware payments dropped significantly in 2024 - Down 35% year over year, even though number of attacks were up
- Victims are refusing to pay: Better backups, earlier detection leading to fewer companies payingLaw enforcement is disrupting the market.
- Improved Law Enforcement Response: Takedowns of major gangs like LockBit and BlackCat, resulting in smaller operations, and more risk

Tip - North Korean: Remote Workers

- Deepfake candidates: A cybersecurity engineer, Dawid Moczadło, encountered job applicants who used AI deepfake technology to alter their appearance during video interviews, attempting to secure remote software development roles.
- Tell-tale signs: Both scammers exhibited red flags such as "glitchy" video feeds, refusal to perform physical tests (like waving a hand in front of their face), mismatched accent
- Suspected espionage: Moczadło suspects these applicants were part of a larger North Korean IT worker scam designed to infiltrate Western companies, steal intellectual property, and funnel wages back to the regime.

Tip - No More Buffer Overflows

- "Unforgivable" Vulnerabilities: The FBI and CISA have labeled buffer overflow defects as "unforgivable" because they are preventable errors that continue to pose significant national and economic security risks
- Shift to Memory-Safe Languages: The agencies urge developers to transition away from memory-unsafe languages (like C and C++) and adopt memory-safe alternatives such as Rust, Go, and Swift to eliminate these types of bugs.
- Immediate Mitigation Strategies: Rewriting codebases takes time, the guidance recommends immediate steps like using compiler flags for protection, implementing rigorous testing (including static analysis and fuzzing)

Tip - Signal Pulling Out of Sweden

- Signal threatens to leave Sweden: Signal has stated that they will withdraw from the Swedish market if the government passes proposed legislation requiring messaging platforms to provide law enforcement with access to encrypted user data.
- Proposed "backdoor" legislation: proposes amending laws to mandate that encrypted messaging apps store chat data for up to two years and make it accessible upon request, a move that would effectively force the end of end-to-end encryption (E2EE)
- Privacy over compliance: Signal emphasized that there is no "safe" backdoor that only authorities can use

Tip - GPL Might Fall

- Threat to Open Source Licenses: A pending decision by the US Court of Appeals for the Ninth Circuit in the case Neo4j v. PureThink could undermine the enforceability of open source licenses like the GNU GPLv3 and AGPLv3 if it upholds a lower court's ruling that allows companies to add binding, irremovable restrictions to these licenses.
- Core Legal Dispute: The case centers on whether Neo4j could modify the AGPLv3—which explicitly permits users to remove "further restrictions"—by adding a "Commons Clause" that forbade resale and support services by non-paying users, and whether users like PureThink were legally entitled to strip those restrictions away.

Tip - NixOS might have stopped XZ Attack

- Attack Vector: The xz backdoor was concealed within test files in the maintainer-provided release tarballs—which are widely used by Linux distributions—but was absent from the public Git repository, allowing it to inject malicious code into liblzma only when built from those specific tarballs.
- Proposed Detection Method: Attacks could be mechanically detected using reproducible builds by rebuilding the software after the bootstrap phase using the trusted Git source; any bitwise discrepancy between this Git-derived build and the tarball-derived binary would flag the presence of unauthorized changes like a backdoor.

Tip - Ubuntu's Shift to Rust based Utilities

- Replacing Core Utilities with Rust: Ubuntu plans to replace traditional GNU command-line utilities (like cp, ls, and find) with Rust-based implementations from the uutils project, aiming to enhance resilience, safety, and performance.
- Testing with "oxidizr": Canonical's VP of Engineering, Jon Seager, has released a tool called "oxidizr" that allows users to easily swap between the traditional GNU utilities and their Rust counterparts to test compatibility and gather feedback before a potential default switch in Ubuntu 25.10.
- Community Reaction: Some concerned about change from GPL-licensed tools to MIT-licensed tools

Tip - AI LLM Crafts Exploit From Patches

- Rapid Exploit Development: Security researcher Matthew Keely demonstrated that Generative AI models (specifically GPT-4 and Claude Sonnet 3.7) can drastically reduce the time needed to create working exploits from hours of manual work to just an afternoon, as shown with a critical Erlang SSH vulnerability.
- AI-Assisted Analysis: The AI models successfully analyzed code differences between vulnerable and patched versions to identify the flaw, explain the logic behind it, and generate proof-of-concept (PoC) code, even debugging their own initial failed attempts.
- Shrinking Defense Window: This capability underscores a significant shift in the threat landscape where exploits can be weaponized almost immediately after a vulnerability is disclosed, forcing defenders to treat every new CVE as an immediate threat.

Tip - Stop NK hackers with one question

- The "Killer" Question: During job interviews, asking a simple provocative question like "How fat is Kim Jong Un?" is reportedly highly effective at identifying North Korean imposters, as they typically disconnect immediately to avoid saying anything negative about their leader.
- Infiltration Tactics: North Korean operatives are infiltrating Western companies by using generative AI to create fake profiles, deploying "front men" for interviews and utilizing US-based "laptop farms" to mask their true location.
- Dual Threat: Once hired, these workers often perform well to gain trust and promotions, but their ultimate goals are to funnel wages back to the North Korean regime and steal intellectual property, which can lead to extortion if they are discovered

Tip - Ironclad Os Project

- Unique Language Choice: Unlike most Unix-like kernels written in C or Rust, Ironclad is built using Ada and its formally verifiable subset, SPARK, aiming to achieve mathematical proof of correctness similar to the seL4 microkernel.
- Security and Real-Time Focus: The project targets small-footprint, embedded systems with hard real-time capabilities and includes enterprise-grade security features like Mandatory Access Control (MAC) by default.
- Full OS Environment: Ironclad serves as the kernel for a broader operating system called Gloire, which leverages GNU tools and the mlibc library to support standard Linux-like environments, including the ability to run the MATE desktop.

Tip - Cybercrime vs. State-backed Ops

- Cybercrime Eclipse: Former White House advisor says that for most US organizations, cybercrime threats like ransomware and business email compromise are "orders of magnitude" larger than nation-state operations
- Government Cuts Impact: warnings that recent budget and staffing cuts to the Cybersecurity and Infrastructure Security Agency (CISA) and other federal bodies will weaken the nation's ability to combat these threats and support critical infrastructure sectors.
- Call for Support: advocates for increased federal assistance to help under-resourced entities, such as rural hospitals and local governments, recover from attacks and disrupt the cyber-criminal ecosystem, particularly by targeting the financial pipelines and nations that harbor criminals.

Tip - AI Finds 0-day in Kernel (ksmbd)

- AI Discovers Linux Zero-Day: Used OpenAI's o3 model to identify a previously unknown "zero-day" vulnerability (CVE-2025-37899) in the Linux kernel's SMB implementation. The bug was a complex race condition leading to a "use-after-free" error, a type of flaw that is notoriously difficult for traditional automated tools like fuzzers to detect.
- Outperforming Human Analysis: The AI not only found the new bug but also correctly analyzed a separate benchmark vulnerability, pointing out that the researcher's own manual fix for it was insufficient due to threading issues—a subtle detail the researcher had initially missed.
- High "Noise" Remains a Hurdle: Despite the success, the process was highly inefficient. Generated a lot of false positives.

Tip - TrueNAS "AI" Support Failure

- The Incident: Researcher Kyle Kingsbury (Aphyr) contacted TrueNAS support regarding an operating system migration and received responses that were factually incorrect and hallucinatory, such as claiming the new Linux-based "Scale" OS used FreeBSD jails and conflating RAID with High Availability (HA).
- The Cause: Kingsbury concluded he was interacting with an LLM-based support system (or a human relying heavily on one) that generated plausible-sounding but completely fabricated technical details, effectively lying to a customer seeking safety-critical advice for data storage hardware.
- The Consequence: The incident highlights the dangers of replacing human expertise with generative AI in technical support roles, where accuracy is paramount

Tip - Just The Browser

- Declutters Mainstream Browsers: It provides automated scripts and configuration files to strip away "bloat" from popular browsers like Chrome, Edge, and Firefox, removing annoyances such as generative AI features, telemetry, sponsored content, and shopping integrations.
- Open Source & Customizable: The project is fully open-source on GitHub, offering users the ability to inspect exactly what is being changed, manually adjust the configuration files to their liking, or easily revert the changes if desired.
- Potential Issues: if your browser is enterprise managed might not work, also is limited in some situations such as Chrome/Linux. Can be used to generate enterprise policies

Tip - 23andMe Bankruptcy

- Bankruptcy Puts Sensitive Data at Risk: 23andMe filed for Chapter 11 bankruptcy, raising significant concerns that its database of over 15 million customers' genetic profiles could have been sold as a corporate asset to pay off creditors, potentially placing deeply personal and immutable data into the hands of insurers, pharmaceutical companies, or other third parties.
- Limited Legal Protections: While 23andMe's privacy policy states that customer data would be subject to the same protections in a transfer, legal experts warn that bankruptcy courts can override these promises.
- Even account deletion might not remove backup data which can still be sold off as an asset.

Tip - Asterinas - Linux-compatible kernel

- Rust-Based "Framekernel" Architecture: Asterinas is a new operating system kernel written in Rust that utilizes a unique "framekernel" design, which splits the kernel into a safe "OS Framework" (managing resources and isolation) and "OS Services" (drivers and file systems), confining unsafe code strictly to the framework layer.
- Security and Safety Focus: By leveraging Rust's memory safety features, the project aims to eliminate common vulnerabilities found in C-based kernels, ensuring that the majority of the kernel (the OS Services) is written in safe Rust.
- Linux Compatibility: The kernel is designed to be ABI-compatible with Linux (specifically on x86-64).

Tip - Vet - Tool for Vetting SBOMs

- Software Supply Chain Security Tool (vet): Open-source CLI tool for identifying and mitigating risks in open-source dependencies (npm, PyPI, Maven). Features include malicious package detection and vulnerability scanning.
- Policy-as-Code Enforcement: Uses Common Expression Language (CEL) to define and enforce security policies (e.g., license compliance, vulnerability thresholds, OpenSSF Scorecard metrics) in CI/CD pipelines.
- Advanced Risk Analysis: Integrates with SafeDep Cloud for real-time malware analysis, going beyond standard scanning.

Tip - Ghost/Stealth Laptop

- Hardware Modifications: Physically remove internal tracking components from the laptop, including the hard drive (to eliminate persistent data storage), Wi-Fi/Bluetooth cards (to prevent MAC address tracking), and the microphone/webcam (to prevent surveillance), ensuring the device is "deaf, dumb, and blind"
- Operating System & Software: The system relies on Tails OS (The Amnesic Incognito Live System) booted from a USB drive, which routes all internet traffic through the Tor network for anonymity and wipes the computer's RAM upon shutdown to leave zero forensic evidence on the machine.
- Connectivity & Operational Security: To mask identity and location, the user must connect to the internet using external, disposable Wi-Fi adapters

Tip - Rayhunter

- Tool Purpose and Functionality: Rayhunter is a new open-source tool developed by the Electronic Frontier Foundation (EFF) designed to detect cell-site simulators.
- Hardware and Accessibility: Rayhunter is designed to run on affordable consumer hardware, specifically the Orbic RC400L mobile hotspot (available for ~$20), making it accessible to journalists, activists, and non-technical users who want to monitor for surveillance on modern 4G networks.
- Surveillance Research Goal: The project aims to crowdsource empirical data to shed light on how law enforcement agencies use these surveillance devices globally, specifically looking for suspicious patterns like forced 2G downgrades or unusual IMSI requests

Tip - Microsoft - A/V out of the Kernel

- Kernel Access Removal: Following the massive CrowdStrike outage that affected millions of machines, Microsoft is preparing to move antivirus and endpoint detection and response (EDR) applications out of the Windows kernel entirely to prevent similar future crashes.
- New Framework Development: Microsoft is collaborating with major security vendors to create a new, safer framework and API set that operates outside the kernel, allowing security tools to function effectively without risking system-wide stability.
- Future Expansion: While the initial focus is on security software, Microsoft plans to eventually move other types of software, such as invasive anti-cheat systems (often described as rootkits), out of the kernel as well.

Tip - Azure Turns off Default Outbound

- Mandatory Security Shift: Starting September 30, 2025, Microsoft will retire default outbound internet access for all new Azure Virtual Machines as part of a "secure-by-default" strategy
- Required Admin Action: To provide internet connectivity for new deployments, administrators must now manually configure specific solutions such as Azure NAT Gateways, Load Balancers, or Firewalls, effectively ending the era of "click-and-go" internet access for Azure VMs
- Impact on Workflows: While existing VMs created before the deadline will remain unaffected, this change is expected to break deployment pipelines for developers accustomed to automatic access

Tip - Libxml2's No Security Embargoes

- Rejection of Security Embargoes: Maintainer of the widely used XML toolkit libxml2, will no longer honor security embargoes due to the unsustainable workload they place on unpaid volunteers.
- Criticism of Corporate "Freeriding": The decision highlights a breakdown in the open-source social contract, calling out tech giants like Apple, Google, and Microsoft for building profitable products on top of libxml2.
- New Standards for Maintainer Boundaries: The incident has sparked a broader movement to adopt explicit "Maintenance Terms" (such as a MAINTENANCE-TERMS.md file) that legally and socially empower open-source maintainers to disclaim response obligations and say "no" to corporate demands for free labor.

Tip - Silent Courier - MI6 Deaddrop

- Digital Dead Drop Launch: Britain's Secret Intelligence Service (MI6) has launched "Silent Courier," a secure dark web portal designed to allow whistleblowers and informants globally—to anonymously send secrets and classified information to the UK.
- Modern Recruitment Tactics: Promoting the platform through verified YouTube instructional videos, MI6 is modernizing its tradecraft to recruit new agents advising users to access the site via the Tor browser on unlinked devices for safety.
- Allied Intelligence Concerns: While the tool aims to gather intelligence on terrorism and global instability, its accessibility has raised questions among some US intelligence veterans about the potential for Americans or others to bypass US agencies

Tip - Chinese used ArcGIS as a backdoor

- Long-Term Backdoor Access: A Chinese state-sponsored group, Flax Typhoon, compromised an ArcGIS server and maintained undetected access for over a year by modifying a legitimate server object extension (SOE) to function as a web shell.
- Stealthy "Living off the Land" Tactics: The attackers avoided traditional malware by using valid credentials to deploy the malicious extension, allowing them to execute commands via the REST API while masquerading as routine system operations.
- Backup Poisoning: The intrusion was so deeply embedded that the malicious component was included in system backups, causing organizations to unwittingly re-infect themselves when attempting to restore their systems.

Tip - Vibe Coding Security Issues (Cont'd)

- Inherent Logic Flaws: Research by security firm Tenzai found that applications created through "vibe coding"—where developers rely entirely on AI agents like Claude Code, Cursor, and Devin—consistently contained critical security vulnerabilities, particularly regarding authorization and business logic (e.g., allowing unauthorized users to delete data or process negative quantities in orders).
- False Sense of Security: While AI agents effectively avoided some common technical vulnerabilities like SQL injection, they frequently missed broader security best practices such as implementing proper security headers or preventing Server-Side Request Forgery (SSRF), often generating code that appeared functional but failed under scrutiny.

Tip - Vibe Coding Security Issues

- Risk of Unskilled Development: The study highlights a growing risk where unskilled developers use AI to build applications they cannot properly audit; for example, one AI agent generated code that enforced permission checks only if a user was logged in, but completely bypassed checks for unauthenticated users.

Tip - Rust dev writing Rue with Claude

- New Language "Rue": Rust veteran Steve Klabnik is developing a new systems programming language called "Rue," which aims to provide memory safety without garbage collection while being more ergonomic and easier to use than Rust or Zig.
- AI-Assisted Development: Klabnik is heavily utilizing Anthropic's Claude AI model to build Rue, with the AI reportedly writing most of the 70,000 lines of code produced in the first two weeks, while Klabnik directs the design and reviews the output.
- Vibe Coding & Skill: Klabnik emphasizes that effectively using LLMs like Claude is a distinct skill that improves with practice, noting that while AI can lower the barrier to entry for small projects, larger engineering efforts still require deep software expertise to guide the AI effectively.

Tip - IBM Bob AI agent will do bad things

- Vulnerable AI Agent: IBM's new AI coding agent, "Bob" (currently in tech preview), was found to be vulnerable to prompt injection attacks that can trick it into executing malware, despite being marketed as a secure development partner.
- Security Bypass: Researchers discovered that attackers could bypass Bob's "human-in-the-loop" safeguards by chaining malicious commands (via operators like >) with benign authorized commands (like echo), allowing malware to run even if the user only approved the safe command.
- Data Exfiltration Risk: Beyond command execution, Bob's IDE interface is susceptible to zero-click data exfiltration attacks, where malicious output can trigger network requests that leak sensitive data to attackers.

Links

Ransomware as a Company

- https://www.theregister.com/2025/02/07/ransomware_costs_analysis/

North Korean: Remote Workers

- https://www.theregister.com/2025/02/11/it_worker_scam/

Links

No More Buffer Overflows

- https://www.theregister.com/2025/02/13/fbi_cisa_unforgivable_buffer_overflow/

Signal Pulling out of Sweden

- https://www.theregister.com/2025/02/26/signal_will_withdraw_from_sweden/

Links

Ubuntu Beginning Shift to Rust based Utilites

- https://www.theregister.com/2025/02/27/adverse_appeals_court_ruling_could/?td=rt-3a

NixOS might have stopped XZ Attack

- https://www.osnews.com/story/142000/how-nixos-and-reproducible-builds-could-have-detected-the-xz-backdoor-for-the-benefit-of-all/

Links

GPL Might Fall

- https://lwn.net/Articles/1014002/

AI LLM crafts exploit from patches

- https://www.theregister.com/2025/04/21/ai_models_can_generate_exploit/

Links

Stop NK hackers with one question

- https://www.theregister.com/2025/04/29/north_korea_worker_interview_questions/

Ironclad - OS Project

- https://www.theregister.com/2025/11/10/ironclad_os_unix_like_kernel/

Links

Cybercrime vs. State-backed Ops

- https://www.theregister.com/2025/05/24/cyber_crime_bigger_than_nation_state/

Links

AI Finds 0-day in Linux Kernel (ksmbd)

- https://www.youtube.com/watch?v=jDimK-89rfw
- https://sean.heelan.io/2025/05/22/how-i-used-o3-to-find-cve-2025-37899-a-remote-zeroday-vulnerability-in-the-linux-kernels-smb-implementation/

TrueNAS "AI" Customer Support Failure

- https://www.osnews.com/story/142417/truenas-uses-ai-for-customer-support-and-of-course-it-goes-horribly-wrong/
- https://aphyr.com/posts/387-the-future-of-customer-support-is-lies-i-guess

Links

Just The Browser

- https://justthebrowser.com/

23andMe Bankruptcy

- https://www.osnews.com/story/142417/truenas-uses-ai-for-customer-support-and-of-course-it-goes-horribly-wrong/
- https://aphyr.com/posts/387-the-future-of-customer-support-is-lies-i-guess

Links

Asterinas – Linux-compatible kernel

- https://www.osnews.com/story/142631/asterinas-a-new-linux-compatible-kernel-project/
- https://asterinas.github.io/

Vet - Tool for Vetting SBOMs

- https://github.com/safedep/vet

Links

Ghost/Stealth Laptop

- https://dicloak.com/video-insights-detail/build-a-ghost-untraceable-laptop-ultimate-guide-to-online-anonymity-and-privacy-diy
- https://www.youtube.com/watch?v=lUVKSwO_ZNw
- https://www.franksworld.com/2024/12/03/how-to-build-a-ghost-untraceable-laptop-ultimate-guide-to-online-anonymity-and-privacy-diy/

Links

Rayhunter

- https://github.com/EFForg/rayhunter
- https://www.eff.org/deeplinks/2025/03/meet-rayhunter-new-open-source-tool-eff-detect-cellular-spying

Links

Microsoft - A/V out of the Kernel

- https://www.osnews.com/story/142647/microsoft-is-moving-antivirus-providers-out-of-the-windows-kernel/

Azure Turns off Default Outbound

- https://www.theregister.com/2025/06/24/outbound_access_vms_azure/

Links

Libxml2's No Security Embargoes

- https://lwn.net/Articles/1025971/

Silent Courier - MI6 Deaddrop

- https://www.npr.org/2025/10/14/nx-s1-5564056/security-mi-6-uk-secrets-foreign-intelligence-silent-courier
- https://www.nprillinois.org/2025-10-14/new-dark-web-dead-drop-lets-anyone-pass-secrets-to-britains-mi6

Links

Chinese used ArcGIS as a backdoor

- https://www.theregister.com/2025/10/14/chinese_hackers_arcgis_backdoor/?td=rt-9bs

Vibe Coding Security Issues

- https://www.npr.org/2025/10/14/nx-s1-5564056/security-mi-6-uk-secrets-foreign-intelligence-silent-courier
- https://www.nprillinois.org/2025-10-14/new-dark-web-dead-drop-lets-anyone-pass-secrets-to-britains-mi6

Links

Rust dev writing Rue with Claude

- https://www.theregister.com/2026/01/03/claude_copilot_rue_steve_klabnik/

IBM Bob AI agent will do bad things

- https://www.theregister.com/2026/01/03/claude_copilot_rue_steve_klabnik/