# 23 For 23
# 23 Things to Know/Try for a Better 2023

January 18, 2023

By Aaron Grothe
NEbraskaCERT

# Introduction

23 for 23?

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

# 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.

# Tip - Cyber Insurance vs Nation States.

Cyber Insurance rates are going up very quickly and what is covered is being reduced.

2023 will be a make or break year for Cyber Insurance.

# Tip - Cyber Insurance vs Nation States.

Cyber Insurance might be getting interesting.

Mondelez International owner of Oreo cookies, Ritz and a bunch of other stuff has been in a multi-year lawsuit with their cyber insurance provider Zurich America over a $100 million dollar bill over cleanup of the 2017 NotPetya outbreak

ZA didn't want to pay out because NotPetya has been attributed to the Russian Military - being the actions of a Nation State.

With North Korea and other countries doing this kind of stuff, will be interesting to see how this changes Cyber

# Tip - Confidential Computing

With many companies moving data to the cloud Confidential Computing is an interesting concept.

The Confidential Computing Consortium defines CC computing as the "The Protection of data in use by performing computations in a hardware-based Trusted Execution Environment (TEE)"

In the TEE all code must be signed, no data in the TEE can be modified outside the TEE

Interesting as multiple cloud providers are implementing these standards

# Tip - Confidential Computing.

There are companies working at software only solutions as well.

This is interesting as you have multiple cloud vendors fighting between complying with a standard and attempting to get the total lockin this might allow you to do.

# Tip - 4G LTE Modems - $10 Computer.

On Aliexpress and other vendors you can buy a USB 4G LTE Data Modem.

Modems have a regular Qualcomm 400 chip and the bootloader is unlocked on most of them.

The modems can be modified to run regular mainline Linux. Debian, OpenWRT, and others are supported.

Will leave it to the reader to think of options for what you can do for these for good or ill.

# Tip - 4G LTE Modems - $10 Computer

On Aliexpress and other vendors you can buy a USB 4G LTE Data Modem.  Powered over USB, have wifi, and 4g lte capabilities

Specs

- 512mb or 1gb of Ram
- 4gb of Storage
- 4-core 1Ghz A53-based Qualcomm 9600 chip

# Tip - 4G LTE Modems - $10 Computer.

Modems have a regular Qualcomm 400 chip and the bootloader is unlocked on most of them.

The modems can be modified to run regular mainline Linux. Debian, OpenWRT, and others are supported.

Will leave it to the reader to think of options for what you can do for these for good or ill.

# Tip - CHI Ransomware Attack

CHI was the victim of a Ransomware attack. Few details have been made public about it so far.

48,000 Lakeside patients were impacted offered 12-months of credit monitoring.

Pharmacy at CHI Health Clinic La Vista actually was writing down orders in a notepad to put them into the system at a later date. Good to see they were still filling orders and then taking care of the billing later.

# Tip - CHI Ransomware Attack

Am following this one closely since both my parents and myself have been patients of CHI.

So far haven't see any notification or information from CHI.

# Tip - Post Quantum Crypto

NIST is working on potential replacements for our current factoring heavy Public Key encryption key systems.

They are running a similar competition to the one ran for Symmetric key encryption which resulted in AES and the Hashing competition which resulted in SHA-3.

They are down to the 4-finalists.  Sike one of the contenders was cracked on a 2013-era 1-core Xeon in less than an hour.

The author of the Sike algorithm suggests this might be addressed with some changes to the code base.

# Tip - Post Quantum Crypto.

This matters as the consensus is that public-key crypto will fall to Quantum computers in the next 5-50 years.

The fact that this a pretty open process is great. It builds confidence in the project and allows people to find bugs early resulting in us not seeing issues like the Wep algorithm.

# Tip - OpenSSL Bugs.

OpenSSL at the beginning of November 2022 announced that there would be fixes for two critical bugs in OpenSSL 3.x

Initial fears were this would be a log4j, heartbleed type of event

Fedora pushed off the release of Fedora 37 by two weeks to allow time for patching this vulnerability.

Initial CVE ratings where in the high 9s.  Later revised to high from critical due to difficulty in executing the compromise.

# Tip - NSA Recommends not to use C/C++.

The NSA has released guidance suggesting people not use C/C++ or any other languages that aren't memory safe.

They suggest the usage of languages such as "C#, Go, Java®, Ruby™, Rust®, and Swift"

Interesting as the NSA usually doesn't come out with a guidance document like this.

# Tip - Microsoft Recommends Rust.

Microsoft Azure CTO Mark Russinovich is recommending Rust for new development.

“Speaking of languages, it's time to halt starting any new projects in C/C++ and use Rust for those scenarios where a non-GC language is required. For the sake of security and reliability. the industry should declare those languages as deprecated. “

Microsoft claims 70% of its CVEs since 2006 are memory-safety related.

# Tip - Rust in the Linux Kernel.

Linux is working at accepting Rust into the Linux Kernel.

Right now the Linux Kernel is 95% C with a bit of assembler/shell for the rest.

Rust will primarily be used for device drivers

There are examples driver for NVME devices the 9p filesystem

Will be interesting to see if more of the kernel moves to Rust over time.

# Tip - ESP32 - Covert Pentesting Kit.

The ESP32 is the 32-bit follow on the ESP8266. ESP32 is an arduino chip with wifi built into it.

The cost for an esp32 is about $1.00 in larger purchases. 10+ usually.

The cover pentesting kit can do things like wifi-deauthing, packet capture, denial of attacks, capturing SSIDs from phones etc.

ESP32 doesn't have enough power to do real computation, but is very cheap and can run on a battery for a lloonngg time.

# Tip - Alternative OSes

This goes with the earlier topics about memory safe languages multiple alternative OSes are being developed in this space

Cosmos (c#) - by Microsoft Open Sourced (BSD licensed) operating system. Majority of it written in C#, with a bit of assembler. Being evaluated again for use in containers.

Redox (rust) - Desktop operating system mostly in rust. Developing a full desktop operating system. Is making some pretty impressive project. Well worth firing up in a VM to see how it is coming along.

# Tip - Alternative OSes.

Neither of these OSes are going to replace your desktop for a while.  Each is an example of the work being put into developing systems around Memory Safe languages.

# Tip - Ubuntu Cue.

Ubuntu is working on Cue and has been announcing it is coming. It is supposed to be a new way to show Linux competency besides just being a certification exam.

Believe it will probably be some scenario based training.

Put this one in here largely as a placeholder to see how it evolves.

# Tip - Flipper Zero.

Flipper Zero is a hardware device that can do all sorts of stuff with RFID tags and other devices.

Can read, copy and emulate RFID tags, radio remotes and digital access keys.

Flipper Zero is unique in that is a complete device. It doesn't require a phone or computer to use.

It also doesn't play by the lower power rules so it can send a signal from a lot further than a regular rfid tag.

# Tip - Splunk's State of Security 2022

Every year try and find a new security report.  You should already know the reports like the Verizon Data Breach Investigation Report and the Microsoft Digital Defense Report.

This year decided to do a bit of a dive into the Splunk State of Security 2022 Report

Some interesting stuff in there:

- Cloud hampering security visibility - topics
- Remote workers affecting security

# Tip - Splunk's State of Security 2022.

Remote Work, Rising Attacks

26% - significant increase in attacks
39% - slight increase in attacks
29% - things are about the same
03% - slight decrease
02% - significant decrease

65% - measurable increase due to remote attacks

# Tip - Nix OS - Reproducible Builds

Nix OS is a Linux distro that uses the Nix package manager

Has the interesting concept of the average user being able to install packages so they can use them. E.g. you can install Firefox without root privileges. Multiple versions of the same software can exist in the system.

The Nix package manager makes it a different kind of Linux distro than the usual.

# Tip - Nix OS - Reproducible Builds.

Some of the interesting features

- Declarative configuration model - can control modules and settings from the language setup.  Kind of a built in Ansible
- Atomic upgrades - all upgrades either succeed or fail. System doesn't end up in a partially upgraded state
- Reproducible builds - you can build the package the same way as other people.  This means same checksums in the binaries and all the support files.

# Tip - Fedora Silverblue

Rarely do I say it but THIS might actually be the future of Linux distributions.

Core idea is that you have an immutable desktop and everything you change on the system is changed through being installed in containers.

EVERY Fedora Silverblue installation, everywhere is identical to every other installation  of that release of Silverblue

Any work you do with applications is through Flatpak or containers.  You don't change the base Operating system.

# Tip - Fedora Silverblue.

If you want to do work on the system locally you fire up a container using distrobox and you do the work in there.  Not changing the base OS.

Upgrades are atomic like NixOS

Is not as easy an environment as the regular Fedora desktop, but it is a cool idea and could spread to other distros in the future.

Worth firing up in a VM and experimenting with.

# Tip - Russian Company claims to be USA

Pushwoosh a software company with headquarters in Siberia claimed to be a US based software company in Social media and US regulatory filings

Pushwoosh offered software to profile online activities of smartphone app users and create custom push notifications from Pushwoosh's servers

Pushwoosh's code made it into 8,000 apps and they claim to have 2.3 billion devices in their database.

# Tip - Russian Company claims to be USA.

Pushwoosh's code was used by the CDC and US Army. Both groups thought they were dealing with a US company.

Is interesting as the company claims the false US claims were made by a marketing company it hired.

# Tip - PyPI malicious Stego File.

There was an application named apicolor that was uploaded to PyPi on October 31, 2022. Stayed on the system for about a week.

Looks to be a legit package except for a rogue import statement that brings in a package named judyb. Judyb included an image hosted on imgur.

Judyb package extracts python code hidden in image and then downloads code from a remote server and runs it on the system.

Is interesting as an example of using Stego to get code onto a system.

# Tip - PyPi Typosquatters

Trust of third party repositories is going to be an ongoing issue for some time. Regardless of what language you are using. Python, Perl, Ruby, NodeJs is turning out to be a real issue.

The PyPi Typosquatters are taking a regular package and putting up a slightly different version. These can be as simple as a malicious import statement being the only difference between the two repos.

The fewer changes here the better as they are trying to impersonate another package.

# Tip - PyPi Typosquatters.

Some of the sample repos are like algorithmic, colorsama, cypress, curlapi, faq, iao, installpy and others.

Most of them seem to be using the w4sp infostealer.

Others such as threadings and pystile include the GyruzPIP malware.

If the scanners are only searching the main project it looks good.

Third-party repo protections are going to continue to be an issue.  Signing of code and trust are going to be issues.

# Tip - Shufflecake

One of the first projects that Julian Assange (of WikiLeaks fame) worked on was the Rubber Hose filesystem. This was a filesystem that would allow you to have 2 different encrypted filesystems on the same disk. The idea was if somebody was beating you with a rubber hose you could give them the password for the system that would allow them to see a set of encrypted files, but these weren't the important files.

There have been other projects such as Veracrypt and StegFS that have attempted to keep the idea alive.

# Tip - Shufflecake.

Shufflecake is a new attempt at this. It is currently for Linux only.

Has a lot of caveats. E.g. if you have multiple volumes but you don't mount them all so the shufflecake software knows not to overwrite the blocks.

Is a nice idea, but think I'll still stick with Luks and wait for the hose.

# Tip - Sigstore.

Sigstore is a Linux Foundation project to work towards easily signing code.

You use your OpenID and use that to sign any piece of code.

This is starting to be supported by Fedora and other projects.

Has been described as being the code signing equivalent to Letsencrypt.

Interesting to see how this evolves over time.  Will more people start using it.

# Tip - Sigstore.

Has support from OpenSSF, Chainguard, Cisco, Google, HPE, Red Hat and others.

Idea is you use your OpenID to generate an ephemeral key to sign your code. Others can validate to make sure you signed the software with your OpenID.

Will be interesting to see if projects such as PyPi, CPAN, NPM and others start to require this.

# Tip - A Million Bad Apps.

Article talking about malicious apps that have managed a million plus downloads on the google play store.

Malware Bytes labs goes into details for a bunch of apps that have managed more than a million downloads.

The methodology of this is great.

Delayed gratification - apps are waiting longer to go rogue. Attempt to get around google's automated app checking tools.

LogCat doing deep analysis of apps.

# Tip - Fixing a Million Vulnerabilities..

Open Bug Bounty recently passed a million vulnerabilities that they have helped remediate.  A pessimist might say "only a trillion to go"

Is an Open system for the responsible disclosure for XSS and other types of issue with websites discovered through non-intrusive methods.

Is a great resource to see the whole bug-bounty process.

# Tip - CycloneDX

CycloneDX is a tool from the OWASP group that helps you track the Bill of Materials (BOM) standards, use it application security contexts and supply chain component analysis.

Has a lot of official and community supported tools.

An interesting project to track and possibly consider contributing to.

# Summary

So that is 23 for 23.  Have a couple of themes this year

- Code signing and supply chain are going to be an issue
- Still some interesting stuff happening in the OS Space
- Memory Safe languages have a real good chance of displacing a lot of our legacy languages over the next 3-5 years
- Attackers are getting more patient and going after upstream sources to get into the software

# Links

Tip - Cyber Insurance vs Nation States

- https://www.theregister.com/2022/11/02/mondelez_zurich_notpetya_settlement/
- https://www.theregister.com/2022/11/08/government_cyber_insurance/

Tip - Confidential Computing

- https://www.theregister.com/2022/11/07/confidential_computing_crypto_heists/
- https://www.ibm.com/cloud/learn/confidential-computing

# Links

Tip - 4G LTE Modems - $10 Computer

- https://liliputing.com/this-dirt-cheap-4g-lte-modem-on-a-usb-stick-can-be-hacked-to-run-mainline-linux/

# Links

Tip - CHI Ransomware Attack

- https://www.hipaajournal.com/chi-health-ransomware-attack-impacts-48000-lakeside-patients/#:~:text=CHI%20Health%20Ransomware%20Attack%20Impacts%2048%2C000%20Lakeside%20Patients,of%20approximately%2048%2C000%20patients%20has%20potentially%20been%20compromised.
- https://www.3newsnow.com/news/local-news/chi-ransomware-attack-what-we-know-and-dont-know

# Links

Tip - OpenSSL Bugs

- https://www.theregister.com/2022/11/01/openssl_downgrades_bugs/

Tip - NSA Recommends not to use C/C++

- https://www.theregister.com/2022/11/11/nsa_urges_orgs_to_use/
- https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3215760/nsa-releases-guidance-on-how-to-protect-against-software-memory-safety-issues/

# Links

Tip - Microsoft Recommends Rust.

- https://www.theregister.com/2022/09/20/rust_microsoft_c/

Tip - Rust in the Linux Kernel

- https://lwn.net/Articles/907685/
- https://lwn.net/Articles/908347/

# Links

Tip - ESP32 - Covert Pentesting Kit

- https://hackaday.com/2022/08/05/esp32-powers-covert-pentesting-device/
- https://hackaday.com/2021/05/27/wifi-penetration-testing-with-an-esp32/
- https://www.theverge.com/23412661/deauther-watch-wifi-hacking-chip-network-deauthorization-secure-oled

# Links

Tip - Alternative OSes

Cosmos

- https://www.gocosmos.org/

Redox OS

- https://www.redox-os.org/

# Links

Tip - Ubuntu Cue

- https://www.theregister.com/2022/11/10/ubuntu_skills_informal_certifications/

Tip - Flipper Zero

- https://flipperzero.one/

# Links

Tip - Splunk's State of Security 2022

- https://www.splunk.com/en_us/form/state-of-security.html

Tip - Nix OS - Reproducible Builds

- https://nixos.org/

# Links

Tip - Fedora Silverblue

- https://getfedora.org/en/silverblue/

Tip - Russian Company claims to be USA

- https://www.reuters.com/technology/exclusive-russian-software-disguised-american-finds-its-way-into-us-army-cdc-2022-11-14/

# Links

Tip - PyPI malicious Stego File

- https://thehackernews.com/2022/11/researchers-uncover-pypi-package-hiding.html

Tip - PyPi Typosquatters

- https://www.bleepingcomputer.com/news/security/dozens-of-pypi-packages-caught-dropping-w4sp-info-stealing-malware/
- https://blog.phylum.io/pypi-malware-replaces-crypto-addresses-in-developers-clipboard

# Links

Tip - Shufflecake

- https://research.kudelskisecurity.com/2022/11/10/introducing-shufflecake-plausible-deniability-for-multiple-hidden-filesystems-on-linux/

Tip - Sigstore - Signing your Code

- https://blog.trailofbits.com/2022/11/08/sigstore-code-signing-verification-software-supply-chain/

# Links

Tip - A Million Bad Apps

- https://www.malwarebytes.com/blog/news/2022/11/malware-on-the-google-play-store-leads-to-harmful-phishing-sites

Tip - Fixing a Million Vulnerabilities

- https://appdevelopermagazine.com/open-bug-bounty-has-fixed-1-million-vulnerabilities/
- https://www.openbugbounty.org/

# Links

Tip - CycloneDX

- https://owasp.org/www-project-cyclonedx/