20 For 20
20 Things to Know/Try for a Better 2020

By Aaron Grothe
NEbraskaCERT

Introduction

20 for 20?

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.

Originally was thinking about doing a recap of the last eight years, but decided to do an all-new one instead

Links are at the end of the talk
Slides will be 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.

Microsoft: Protect Yourself From Tech Support Scams - site.

This one seems to be on the upswing lately. From personal experience I had a couple of very smart family members fall for this one.

Major problem with this can be it is really hard to convince people they've been scammed. It is a combination of embarrassment and the people doing the scam are really well coached/prepared.

Being able to point to a resource from somebody like Microsoft can be a very useful arrow to have in your quiver.

Google Password Checker.

Google has built in a password checker into their browser

It'll check all the passwords you have saved in your browser against some basic rules and also against the "haveibeenpwnd" website as well.

You've probably got a bunch of passwords saved in your google account through android if not using the google chrome browser

There is also an extension which will ask you to reset passwords that show up in a data breach

A Taxonomy of Computer Security Flaws, With Examples.

This is a classic paper from 1974. It is truly amazing how much of it still applies today.

All the "greatest hits" are in here. Buffer overflows, input validation, race conditions, logic errors and more…

Is interesting to see how we seem to keep having the same issues we've been having for the last 30+ years.

Pinephone/Librem 5 Phone, etc

2020 might be an interesting year in the cellphone arena:

Pinephone - linux based phone from the developers who make the Pine64 sbc - currently the early developer items are available. Called the "BraveHeart" edition. Priced at $150.00

Purism is from Librem - another linux based phone. Running the PureOS also from Purism. Early units are starting to get delivered to people who bought them in the Kickstarter campaign. Priced at ~$600.00

Pinephone/Librem 5 Phone, etc.

Both have custom switches to turn off various functions:

For the Pinephone the switches turn off the following functions

LTE (Includes GPS)
Wifi/BT
Microphone / Camera

Purism: Wifi/BT, Camera & Microphone switches with additional switches planned for hardware such as the LTE functionality

Interesting to see if these get any traction

Azure Sentinel

Microsoft has rolled out their own SIEM system.

Pricing as you go $2.50 per GB-ingested, with discounts for volume

Is buzzword compliant

- Machine Learning module - fusion (build-your-own-ml) recognize patterns that you're interested in
- AI enabled
- Dashboard
- Playbooks, etc...

Azure Sentinel.

How it compares to systems such as Splunk, Sumo and others is yet to be seen

Does have a 30-day trial if you use certain features you can incur charges as well

Exited beta in September 2019, so still early but looks a decent option

AWS Code Guru

New AWS service showed at the latest Re:Invent conference

Currently only available for Java

Automated code review and profiling tool

Another project promising machine learning.

Point AWS Code guru to either Github or AWS CodeCommit repo

AWS Code Guru

Consists of two components: Code Review and Profiler

To run profiler program has to run in AWS either EC2, ECS or Fargate

Recommendations based on AWS best practice, concurrency, resource leaks, sensitive information leaks and common coding best practice

Cost of review side $0.75 per 100 lines of code
Profiling $0.005 per sampling hour to maximum of $180.00 per app

AWS Code Guru.

Lots of companies have issues with providing documentation of their code review and other options.

With AWS Code Guru being automated by Git pull requests this might be an interesting part

Still early days on this, did not see options for customization to put your own rules in, and only support Java is a bit limiting. Still a very interesting project.

IAPP - CIPT Beta Exam

International Association of Privacy Professionals has been around since 2000.

They have several certifications

- Certified Information Privacy Professional (CIPP)
- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Technologist (CIPT)
- Privacy Law Specialist (PLS)
- Fellow of Information Privacy (FIP)

IAPP - CIPT Beta Exam

IAPP is doing substantial revisions to their CIPT certification and the new program will be offered in Spring 2020

Schedule

Jan 6, 2020 - CIPT beta exam registration opened
Feb 3 - Feb 9, 2020 - CIPT beta testing
Mar 30, 2020 - CIPT relaunch

IAPP - CIPT Beta Exam.

Exams are offered through Pearson Vue

A different kind of cert.

I am planning on signing up to take this exam

Fifth Domain

In a typical year I read about 15-20 books on information security. This is one of the better ones I read.

Book is by Richard Clarke. Most famous for being the first person after 9/11 to say "your government failed you. … And I failed you"

Is an interesting book in that some ways it talks about the post attack world some companies are working towards. How to recover from an attack so quickly it is almost like it never happened.

Fifth Domain.

Would have appreciated more detail in some areas like how companies are able to recover quickly and so on, but I liked the book

All of Richard Clarke's books have been pretty good.

This book has more HOPE in it than any other book I read in 2019, so I recommend it.

BTW - Fifth domain comes from theaters of war: land, sea, air, space and cyberspace.

Confidential Computing Consortium

CCC is a project of the Linux Foundation project

Concerned with the protection of data when being used and in transit.

Contributed components

- Microsoft's Open Enclave SDK is a framework for Trusted Execution Environment (TEE) applications.
- Red Hat Enarx project committed to providing hardware independence for securing applications
- Intel Software Guard Extensions (SGX) - protected enclave software

Confidential Computing Consortium.

An enclave application partitions itself into two components

1. An untrusted component (called the host)
2. A trusted component (called the enclave)

One of the fields of research in this are the IoT and cloud arenas

An early project but has some big contributors to it so I'm curious to see how this one goes.

Reverse Engineering the Capital One Breach

In July 2019 Capital One had a breach

- 100 million individuals had some of their information disclosed.
- Appears to have been done by an ex-employee with insider knowledge
- Was Amazon S3 bucket related
- Misconfigured web application firewall

Being a large incident from a bank was pretty well examined.

Capital One has posted a facts page about the incident

Reverse Engineering the Capital One Breach.

A couple of other groups have also reverse engineered information about the event as well

- Krebs did some really good analysis on this - link is at the end
- Last Week in AWS also did a really good analysis of this as well with Josh Stella

The analysis of both of them are very interesting as they are largely complementary, but they also tend to assign blame a bit differently

Last Week is a bit tougher on this end

Protection Poker

Protection Poker is a different approach to threat modeling, similar to planning poker.

Basic Steps

1. Value and rank your software assets
2. Calibrate the ease of attack for new requirements
3. Compute the security risk
4. Add mitigation to the iteration

Protection Poker.

Benefits

- Is iterative
- Encourages sharing of software security knowledge between team
- Is less formal and "friendly" than some other methodologies

Cons

- Still being developed
- No single source of rules
- Will be interesting to see if it takes off

Sandboxie.

Sandboxie is a classic tool from 2004 that allowed you to run/test untrusted executables on Microsoft Windows

- Was shareware for years
- Sophos has bought the company
- Software is now free (as in beer)
- Plan is to open source the software and let the community take it forward
- Interesting to see how it moves forward and if it can move to the community successfully

Multipass

Multipass is a Canonical project to make it easier to install Ubuntu on different operating systems

On Windows 10 uses Hyper-V or VirtualBox
On Linux uses KVM
On Mac used HyperKit or VirtualBox

Comparing to WSL2, WSL2 is designed for sharing information. Multipass is designed to be more like regular VMs separate from the underlying OS

Multipass.

Typical commands (docker like)

$ multiplass find # show available images
$ multipass launch ubuntu # load latest LTS image
$ multipass list # who running instances
$ multipass shell imagename # connect to running instance

If you're running Ubuntu it is a snap install.

Will this compete well with Docker and WSL2 possibly. If you're doing cross platform hosts might work out well.

ji32k7au4a83 is a surprisingly bad password.

The Verge has an article talking about how "Ji32k7au4a83" is a bad password. Ji32k7au4a83 has appeared in 141 data breaches according to haveibeenpwned

Why? Looks pretty random to me.

Turns out if you've got a Taiwanese keyboard with the Zhuyin Fuhao layout the string spells out "my password" in Mandarin.

As the internet continues to get more global phrases like "au4a83" or password are going to show up more and more as well :-)

McAfee - Cloud-Native: IaaS Adoption and Risk Report

McAfee's 2019 Cloud Adoption and Risk Report is available

Overview is available without registering (20 slides)
Full report requires registration

Unfortunately cloud migration still lacking some metrics and info

They are supposed to be doing these yearly will be interesting to track over time

McAfee - Cloud-Native: IaaS Adoption and Risk Report.

Some Interesting findings

- 5.5% of AWS S3 buckets have world read permissions (aka open to the public)
- 80% of all orgs experience at least 1 compromised account threat per month
- 92% of all orgs have stolen cloud credentials for sale on the Dark Web
- Amount of files with sensitive data have increased 53% YoY

Some good guidance, assume your IaaS is misconfigured so do the basics

Mitre 2019 CWE Top 25 Most Dangerous Software Errors

The Common Weakness Enumeration (CWE) list from Mitre is a guide that lays out the most dangerous software errors

A couple of sample errors

- CWE-125 - Out-of-bounds Read
- CWE-798 - Use of Hard-coded Credentials
- CWE-200 - Information Exposure
- CWE-416 - Use After Free
- CWE-119 - Improper Restriction of Operations within the Bounds of a Memory Buffer

Mitre 2019 CWE Top 25 Most Dangerous Software Errors.

What is nice about this list is that they also provide more info for each error

- Applicable Platforms
- Common Consequences
- Likelihood of Exploit
- Examples
- Potential Mitigations

Very good resource and the mitigation stuff is very good

Small Business CyberSecurity Corner.

The NIST Small Business Cybersecurity Act became law on August 14, 2018.

The law directs NIST to "disseminate clear and concise resources to help small business concerns identify, assess, manage and reduce their cybersecurity risks."

Is a great resource for small and not small businesses

Google Sandbox2

Sandbox2 is a C++ security sandbox designed to allow you to run programs in a confined environment so that security bugs such as buffer overflows can't escape the sandbox.

One idea is that there will be a set of apis and tools that allow you to create code that is constrained so it will be able to run in a public cloud and have less potential to impact other instances.

Sandbox2 replies on Linux kernel facilities such as seccomp and BPF to write custom syscall filters

Google Sandbox2.

Creates 2 processes

- Executor runs regular c++ code using the sandbox2 api
- Sandboxee child program running in the sandboxed environment

Interesting concept don't know what the overhead of this but has a lot of cool ideas in it.

Binary Planting with the npm CLI

NPM - Node Package Manager is used by almost everybody that uses NodeJS

Versions of npm prior to 6.13.3 an entry in the package.json bin field would allow a package publisher to modify and/or gain access to arbitrary files on user's system when package installed

Versions of npm prior to 6.13.4 possible for a globally-installed package with a binary entry to overwrite existing binary

Binary Planting with the npm CLI

Parsing libraries for npm have been updated to sanitize paths used to install binaries

Npm is used millions of times a month by people especially running in Devops mode.

Npm at this point is almost a utility

Binary Planting with the npm CLI.

Also keep in mind there are other issues that happened with npm in 2019 as well.

- Developer pulled bunch of basic packages like center text, which was the developer's right
- Advertising has been attempted to be added as well via a custom package
- Npm is attempting to turn a profit as well and several competitors are popping up as well

Facebook Phone O/S.

Facebook is working on its own operating system for phones and other devices so it can control everything

There was a Facebook phone in 2013 that used HTC hardware but it was a huge failure almost as big as Microsoft's Kin. Fortunately you could drop the Facebook skin off the HTC hardware and turn it back into an almost stock device.

Also Facebook is working on a brain computer interface. Hoping it is read only :-)

7 Security Incidents that cost CISOs their jobs.

CSO Online had an interesting summary of 7 security events

- Capital One, Equifax, Uber, Facebook
- Target, JP Morgan, San Francisco State University

Provides some high level information about each event also has a very nice section entitled "if you keep your job, incidents can be good"

Nice little article to point management to, it is short and has good points.

Q & A

Questions???

Links

Tip - Microsoft: Protect yourself from tec support scams

https://support.microsoft.com/en-us/help/4013405/windows-protect-from-tech-support-scams

Tip - Google Password Checkup Extension

https://chrome.google.com/webstore/detail/password-checkup/pncabnpcffmalkkjpajodfhijclecjno

https://password.google.com

Links

Tip - A Taxonomy of Computer Program Security Flaws, with Examples by Carl Landwehr from 1994

http://www.landwehr.org/1994secflawtaxcsurv.pdf

Tip - Pinephone/Librem 5 Phone, etc…

https://www.pine64.org/pinephone/

https://puri.sm/products/librem-5/

Links

Tip - Azure Sentinel

https://azure.microsoft.com/en-us/services/azure-sentinel/

Tip - AWS Code Guru

https://aws.amazon.com/codeguru/

https://www.theregister.co.uk/2019/12/24/exploring_aws_codeguru/

Links

Tip - CIPT Beta Exam

https://iapp.org/certify/cipt/#

Tip - Fifth Domain

https://www.amazon.com/dp/B07JKHF7VM/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1

Links

Tip - Confidential Computing Consortium

https://confidentialcomputing.io/

https://www.linuxfoundation.org/press-release/2019/08/new-cross-industry-effort-to-advance-computational-trust-and-security-for-next-generation-cloud-and-edge-computing/

Links

Tip - Reverse Engineering the Capital One Breach

https://www.lastweekinaws.com/podcast/screaming-in-the-cloud/reverse-engineering-the-capital-one-breach-with-josh-stella/

https://krebsonsecurity.com/2019/08/what-we-can-learn-from-the-capital-one-hack/

https://www.capitalone.com/facts2019/

https://www.lastweekinaws.com/podcast/screaming-in-the-cloud/reverse-engineering-the-capital-one-breach-with-josh-stella/

Links

Tip - Protection Poker

https://opensource.com/article/19/3/protection-poker-agile-security-game

Tip - Sandboxie

https://www.sandboxie.com/

Links

Tip - Multipass

https://www.theregister.co.uk/2019/12/18/multipass/

https://github.com/canonical/multipass

Tip - ji32k7au4a83 is a surprisingly bad password

https://www.theverge.com/tldr/2019/3/5/18252150/bad-password-security-data-breach-taiwan-ji32k7au4a83-have-i-been-pwned

Links

Tip - McAfee - Cloud-Native: IaaS Adoption and Risk Report

https://www.mcafee.com/enterprise/en-us/assets/skyhigh/white-papers/cloud-adoption-risk-report-2019.pdf

https://www.mcafee.com/enterprise/en-us/solutions/lp/cloud-adoption-risk.html

Links

Tip - Mitre 2019 CWE Top 25 Most Dangerouse Software Errors

https://cwe.mitre.org/top25/archive/2019/2019_cwe_top25.html

Tip - NIST Small Business CyberSecuity Corner

https://www.nist.gov/itl/smallbusinesscyber

Links

Tip - Google Sandbox2

https://developers.google.com/sandboxed-api/docs/sandbox2/overview

Tip - NPM Binary Planting

https://blog.npmjs.org/post/189618601100/binary-planting-with-the-npm-cli

Links

Tip - Facebook wants to make own Phone OS

https://techcrunch.com/2019/12/19/facebook-operating-system/

Tip - 7 Security Incidents that cost CISOs their jobs

https://www.csoonline.com/article/3510640/7-security-incidents-that-cost-cisos-their-jobs.html