The Life and Time$ of Privileged Access Management

Aria Langer

AriaDear: ~$ whoami

- Aria Langer – ~~Security Engineer (Morningstar)~~ *Senior Security Engineer (KraftHeinz)*
- WiCyS Chicago Affiliate - ~~Events Lead~~
- ~~Fast as lightning~~; Scared of lightning
- ~~Geriatric DDR Player~~ *Bemani Boomer*
- ~~DuckTales~~ *Uncle $crooge*

Rosa, D. (2010). The Life and Times of Scrooge McDuck Vol 1. BOOM! Kids

What the @*%# is DuckTales doing in a PAM talk?

Uncle Scrooge metaphors as a teaching tool to help understand technical concepts and retain knowledge through storytelling.

CAPTION:
Donald Duck: Uncle Scrooge? Is that really you?
Young Scrooge: Nephew?! What the @%# are you doing here?!*
Donald: It is you! Foul little mouth and all!

Rosa, D. (2010). The Life and Times of Scrooge McDuck Companion. BOOM! Kids

Who is Scrooge McDuck?
(Unca $crooge)

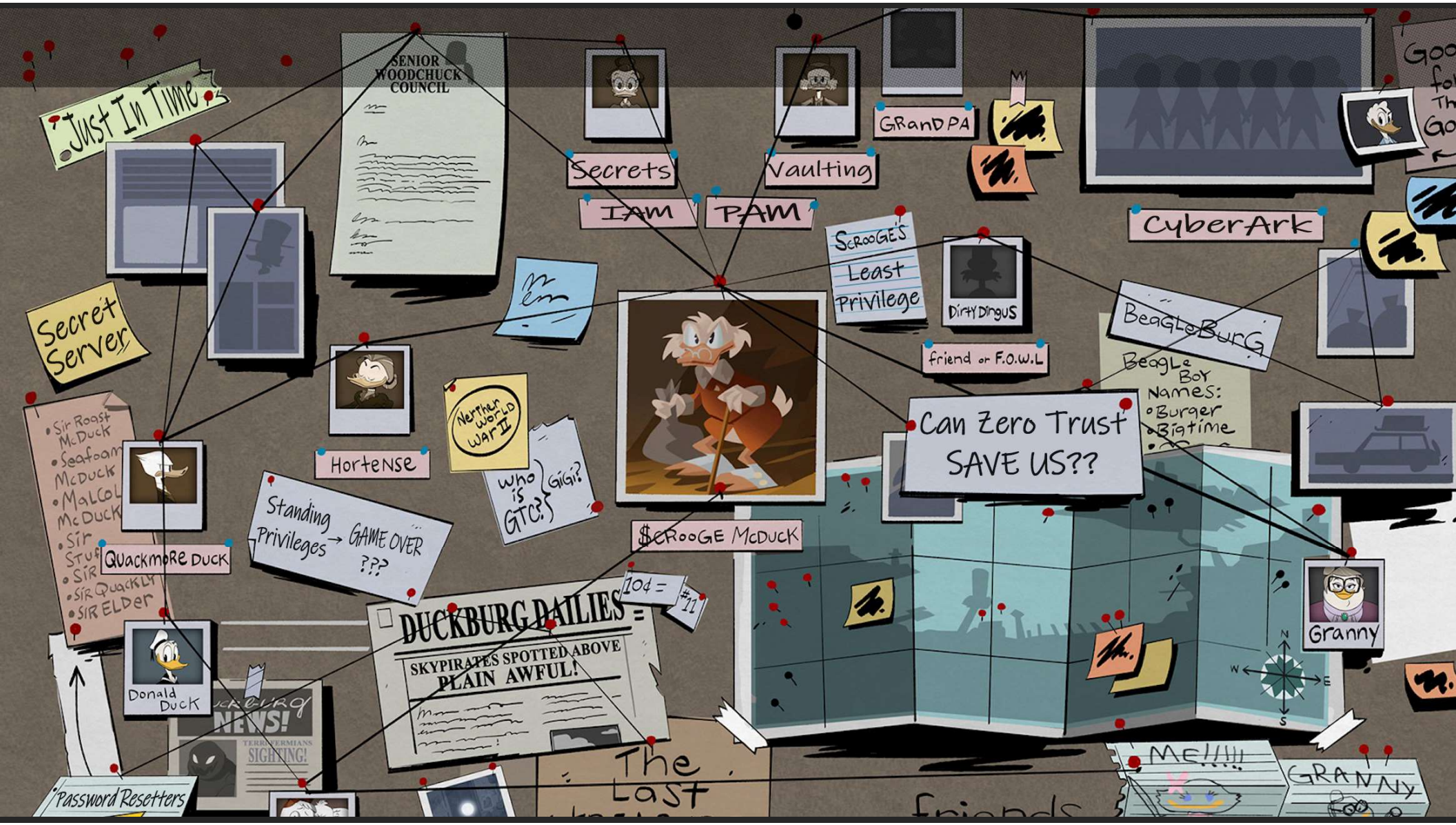
"I like to dive around in my money like a porpoise! And burrow through it like a gopher! And toss it up and let it hit me on the head!"

- Richest Duck in the World
- Was originally created by Carl Barks as a villain for Donald Duck
- Grows up to become the Walter White / Heisenberg of Disney
- Constantly fighting threats against the Money Bin

("I am the one who knocks!" vibes anyone?)

CAPTION:
Scrooge McDuck: OH, SO? WELL, ANY LOAFERS OR MISCREATNS WHO THINK THEY'LL GET THEIR FINGERS ON MY MONEY WILL TANGLE WITH SCROOGE MCDUCK!

Rosa, D. (2012). The Life and Times of Scrooge McDuck. Vol 2. BOOM! Kids


Just In Time
SENIOR WOODCHUCK COUNCIL
Secrets
Vaulting
GRanDPA
IAM
PAM
CyberArk
Secret Server
ScRooGE'S Least Privilege
DirtyDirgus
friend or F.O.W.L
BeagleBurG
Beagle Boy Names:
•Burger
•Bigtime
Sir Roast McDuck
•Seafoam McDuck
•MaLCoLm McDuck
•Sir Stu
•Sir
•Sir Quackly
•Sir Elder
Hortense
Nether world War II
Who is GTC? GiGi?
Standing Privileges → GAME OVER ???
Can Zero Trust SAVE US??
$cRooGE McDuck
Quackmore Duck
DUCKBURG DAILIES
SKYPIRATES SPOTTED ABOVE PLAIN AWFUL!
10¢ = #11
Donald Duck
NEWS!
SIGHTING!
Granny
Password Resetters
The Last
friends
Me!!!!!
GRANNY
N
W
E
S

Jumping off points

- Too many highly privileged accounts with standing privileges* that also are being used for day-to-day tasks
- Your Org is subject to adherence to these:
  - GDPR Compliance
  - SOX Compliance
- Cybersecurity Insurers require PAM controls

A “Launchpad” if you will. ;)

CAPTION:
Huey: There is only one way to find answers, men—in the Junior Woodchucks' Guidebook and Reservoir of inexhaustible knowledge!

Barks, C. (2014). The Complete Carl Barks Disney Library. Disney Enterprises, Inc.

What does the Junior Woodchuck Guidebook say about Privileged Access Management??

- *…a domain within Identity and Access Management (IAM) focusing on* ***monitoring*** *and* ***controlling the use of privileged accounts***

-Nist.gov

(……Alright, so what does the Junior Woodchuck Guidebook say ***about privileged accounts****?)*

Standard User Account

- Routine Tasks
  - Signing into your device
  - Checking email
  - Basic access to normal system resources
  - Limited permissions to make changes
- Interactive Account

CAPTION:
Donald Duck: Wotta Job! Uncle Scrooge wants me to inventory all the large bills in the bin! There's not enough time in the world for this job!

Rosa, D. (2015). Uncle Scrooge and Donald Duck: "Treasure Under Glass". Disney Enterprises, Inc.

Privileged Account

- Password “Resetters”
- Administrator Roles/Rights to a system
- Active Directory group memberships to these to name a few:
  - Enterprise Admins
  - Domain Admins
  - Builtin/Administrators
  - Account Operators
- And any Local Administrator

Rosa, D. (2018). Uncle Scrooge and Donald Duck: “The Old Castle’s Other Secret”. Disney Enterprises, Inc.

Standing Privileges

- Privileges on a system that are “always on” 24/7/365
- If account is compromised, attacker also has always on privileges
- Easy to overlook when roles change internally
- Standing privileges granted as quick fix to resolve access issues, then are forgotten

What happens when…

- The nephews have the magic lamp all the time? (And nobody knows that they have it?)
- When the nephews LIVE full time at McDuck manor (and the money bin)?
- When an interactive account has Account Operators AD group membership?
- When a nested group has Builtin\Administrators group membership--and that group contains standard user accounts?
- When L1 “password resetters” can change passwords to highly privileged accounts to ***blatherskite123****?*

CAPTION:
Scrooge: Well? Isn't your shift over? I don't want you hanging around here getting underfoot!

Donald: Umm…perhaps you've forgotten that you haven't paid me yet!

Rosa, D. (2010). Uncle Scrooge and Donald Duck: "The Three Caballeros Ride Again!". Disney Enterprises, Inc.

Just-In-Time (JIT) Access

- Temporary elevated privileged access
- As-needed per task for defined period of time
- Granular access per application/system
- Goodbye standing privileges

$$$$

- JIT dependent on a third/fourth party
- AWS → Okta Access Requests
- Azure → PIM

  (But PIM doesn't work for on-prem)

Cons:

- High Cost
- Limited compatibility depending on the vendor

CAPTION:
Scrooge: $226.00! That's a FORTUNE! You can't mean it!

Nephew: Pay up, or we enforce this contract!

Barks, C. (2012). Uncle Scrooge: "Only a Poor Old Man". Disney Enterprises, Inc.

Session Recording

- Privileged access is tracked
- Sensitive data may get recorded
- Additional auditing requirements
- “Right to be forgotten” requests need to be addressed
- To enable or not to enable?

  (You might not have a choice)

CAPTION:
Scrooge: Oh, so? You have my grudging interest! Please continue!

Donald: This device will scan all communications of any sort in the immediate area for references of ill-will toward you, or threats of theft!

Rosa, D. (2010). Uncle Scrooge and Donald Duck: “The Three Caballeros Ride Again!”. Disney Enterprises, Inc.

CAPTION:
Scrooge: @*%# !

No “silver bullet” to magically undo this.

Rosa, D. (2010). The Life and Times of Scrooge McDuck Vol 2. BOOM! Kids

Rosa, D. (2010). Uncle Scrooge and Donald Duck: “The Three Caballeros Ride Again!”. Disney Enterprises, Inc.

What about Zero Trust? Does it fit in the Life and Times of PAM?

“Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location or based on asset ownership…”

NIST Special Publication 800-207

(Quoted from the Junior Woodchuck Guidebook!)

Never Trust; always verify

- Requires repeated reauthentication from user even after an initial verification

CAPTION:
Scrooge with a cannon (Bertha):
Yes! Yes! Come in!

Barks, C. (2015). Donald Duck: “The Pixilated Parrot”. Disney Enterprises, Inc.

One of the tenets of PAM & Zero Trust

(Not David Tennant ;p)

- Principle of Least Privilege

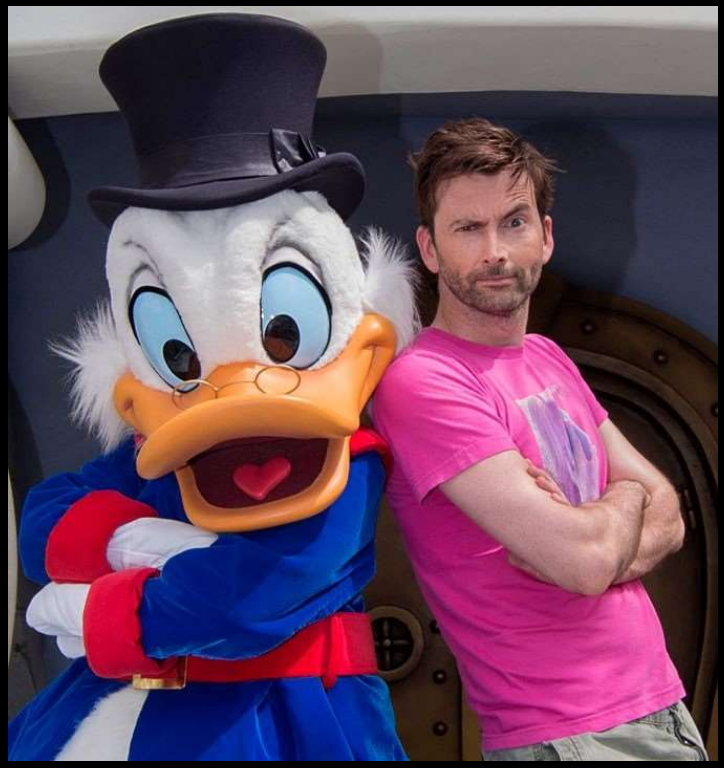
A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

–NIST Glossary

(Quoted from the Junior Woodchuck Guidebook!)

Privileged Access Management with AND without traditional PAM vault:

- Restrict Lateral Movement
- Limit Who Can Access Those Accounts
- Limiting Interactive Logon



Celestino, M. (2017, July 25). PHOTOS: "DuckTales" star David Tennant meets alter-ego Scrooge McDuck at Disneyland. Inside the Magic. http://www.david-tennant.co.uk/2017/07/photos-ducktales-star-david-tennant.html

Lateral Movement

Lateral Movement consists of techniques that adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it. Reaching their objective often involves pivoting through multiple systems and accounts to gain.

-MITRE ATT&CK

(Thanks Junior Woodchuck Guidebook!!!!)

CAPTION:
Arpin Lusene (Adversary): But I bow to your wishes! If you do not want me to use the front door, I will enter in my own style!

Rosa, D. (2018). Uncle Scrooge and Donald Duck: “The Old Castle’s Other Secret”. Disney Enterprises, Inc.

Restricting Lateral Movement

- Microsegmentation
  - “Breaking” networks into smaller segments
  - More of a Networking & or Infrastructure component
  - But PAM can be seen as the “identity” based component to microsegmentation
- Use LAPS!
  - Windows only
  - Local admin password stored in AD attribute:
    - ms-mcs-AdmPwd
  - When attribute is viewed, AD automatically rotates the password (scheduled rotation)
  - Local admin password is unique per host

CAPTION:
Scrooge: We used Gyro’s Diamond-Dust Paint to coat the ENTIRE room—walls, floor, ceiling, and door! Your OMNISOLVE™ can’t cut diamond! You’re trapped!

Now take off that armor and slowly back away!

Donald (to the Black Knight): Eh…bonjour.

Rosa, D. (2018). Uncle Scrooge and Donald Duck: “The Old Castle’s Other Secret”. Disney Enterprises, Inc.

Limit who can access those accounts

Break glass accounts with different administrative privileges.

- Pros:
  - Limits who can check out the password
  - Set a password rotation policy to make it temporary access
  - Centrally managed

- Cons
  - Not a 1-1 Just-In-Time replacement.

Rosa, D. (2018). Uncle Scrooge and Donald Duck: “The Old Castle’s Other Secret”. Disney Enterprises, Inc.

Limiting Interactive Logon

- Interactive – prompted for further action or information (enter a password)
  - “Most” Standard User Accounts
- Non-Interactive – Machine-to-Machine Connection
  - Group Managed Service Accounts (gMSAs)
- Service Accounts “should not” perform interactive logon
- *(Some service accounts NEED to be interactive to work!!!)*

CAPTION:
Gyro Gearloose:
My helper!

Rosa, D. (2010). Uncle Scrooge and Donald Duck: “The Three Caballeros Ride Again!”. Disney Enterprises, Inc.

Final Words

The King of the Klondike

- Don’t let Unca Donald get GLORPED by the Omnisolve
- Password vaults = a cog in the machine; not the entire solution
- The Life and Times of Privileged Access Management is a journey of much trial and error.
- Unca Scrooge cannot do it alone. PAM and Zero Trust are a shared responsibility.
- We fight to protect the org to live to see another adventure.

Rosa, D. (2010). The Life and Times of Scrooge McDuck Companion. BOOM! Kids

To Learn more

- Zero Trust Architecture
- https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-strategy
- Just In Time Access Definitions
- https://delinea.com/what-is/just-in-time-access
- https://www.cyberark.com/what-is/just-in-time-access/
- Standing Privileges (Why they bad)
- https://www.ssh.com/blog/gartner-standing-privileges-are-a-risk
- https://www.darkreading.com/endpoint-security/standing-privilege-the-attacker-s-advantage
- Interactive Logon
- https://learn.microsoft.com/en-us/windows-server/security/windows-authentication/windows-logon-scenarios
- Least Privilege
- https://www.professormesser.com/security-plus/sy0-601/sy0-601-video/personnel-security/
- https://www.ssh.com/academy/pam/what-is-least-privilege
- LAPS
- https://4sysops.com/archives/how-to-install-and-configure-microsoft-laps/
- https://adsecurity.org/?p=3164

Special Thanks

- *Staff and CFP Review Board of Blue Team Con*
- *Infosec Team @ Morningstar*
- *Infosec Team @ KraftHeinz*

- *Mike @ Graham Cracker Comics of Naperville*

- *And my husband GTC for your support---I love you very AriaDearly.*

Contact

LinkedIn:
https://www.linkedin.com/in/aria-langerdrome
X (Formerly Twitter):
@Ariadear
Discord:
ariadear