RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: IDY-901

Are you worthy? The Laws of Privileged Account Management

SPEAKER: **Jackson Shaw** @JacksonShaw

Sr. Director, Product Management, IAM
Dell Security Solutions

Jackson.Shaw@software.dell.com

#RSAC

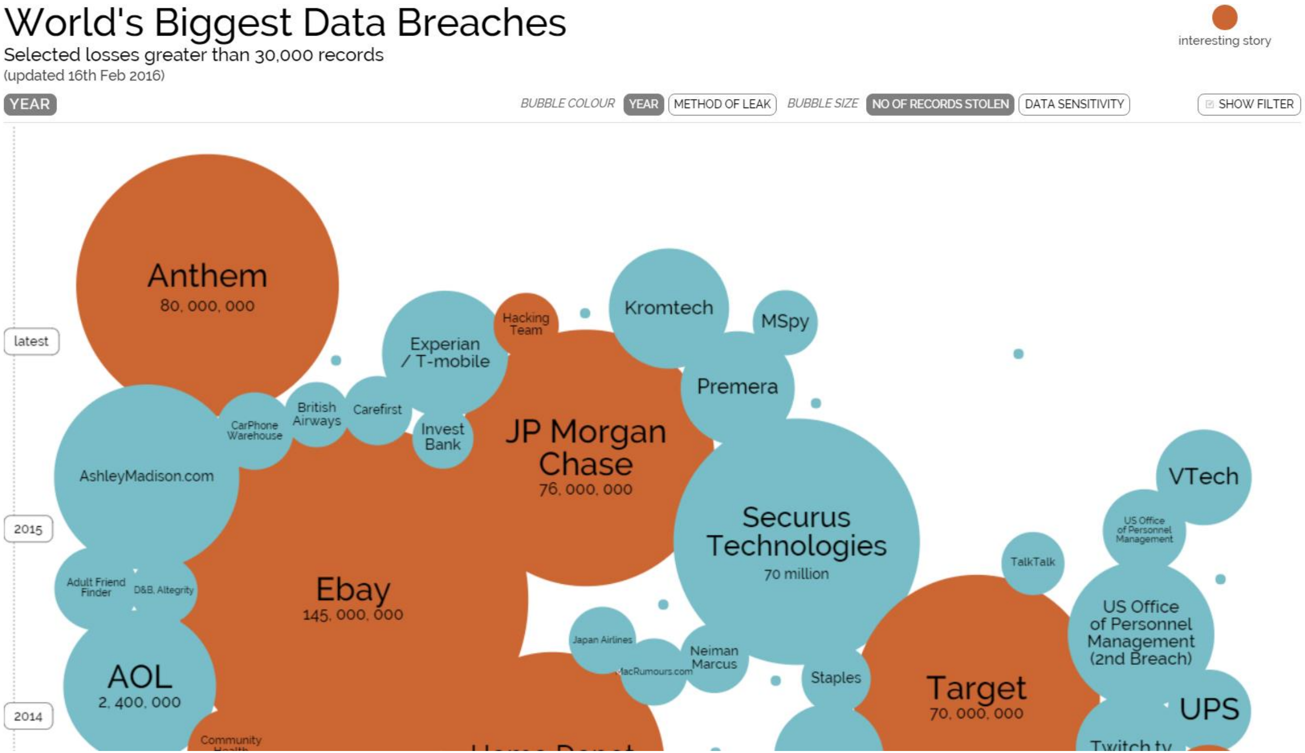
Agenda

- Why this is important to everyone
- The Laws of **P**rivileged **A**ccount **M**anagement
- Call to Action

The "why"…

- The Verizon *2015 Data Breach Investigations Report* noted that 96% of the nearly 80,000 security incidents analyzed could be traced to nine basic attack patterns that vary from industry to industry. **Insider misuse** ranked third out of nine, and 55% of the misuse was privileged accounts abuse.
- A review of recent FBI cyber investigations revealed victim businesses incur significant costs ranging from $5,000 to $3 million due to cyber incidents involving **disgruntled or former employees**
- The Target attackers were able to gain access to the retailer's system by way of **stolen credentials from a third-party vendor**.
- **Passwords stolen from a contractor** led to the OPM breach
- **Hackers exploit systems** to gain access to enterprise networks and leapfrog onto other corporate systems

These firms were “hacked”



World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 16th Feb 2016)

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

If we do not wish to fight, we can prevent the enemy from engaging us even though the lines of our encampment be merely traced out on the ground. All we need to do is to throw something odd and unaccountable in his way.

Sun Tzu

The Laws

The Laws

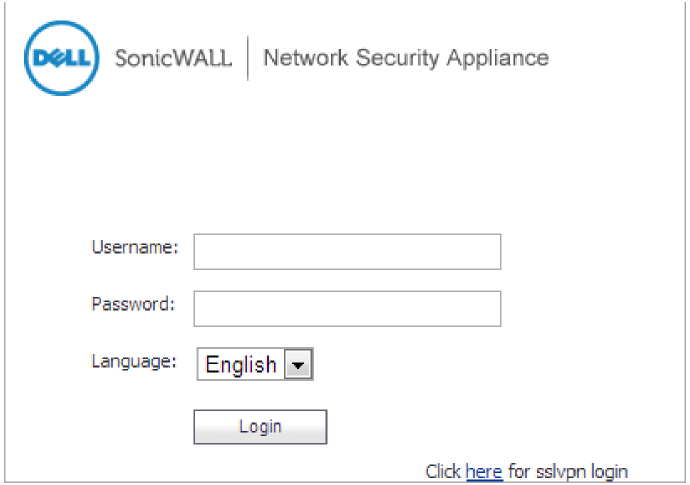
Inventory every privileged account

- Who owns it?
- Who should own it?
- Don’t forget LDAP or Active Directory groups like Domain Admins and nested groups
- Every *nix box has a *root* account
- Every mainframe has system admins
- Don’t forget database, business and other high risk apps like SAP
- Don’t forget network devices like firewalls, routers, phone switches, …
- Don’t forget applications & scripts

The Laws

Change Default Passwords

- Sorry that I have to mention this
- Tie authentication of network devices to a directory – preferably Active Directory
- Lifecycle of these users should be part of your standard identity lifecycle



The Laws

Protect Service Accounts

- Biggest offenders
  - Windows
  - *nix
- Biggest hole
  - SSH keys on *nix

The Laws

Extend your protection bubble past the firewall

- Social media
- SaaS applications
- Partners
- Contractors
- Customers

The Laws

No more shared accounts

- Eliminate all shared accounts
- Move towards non-repudiation and eliminate “that wasn’t me”
  - Makes administrators accountable for their actions
  - Irrefutable evidence about events/actions is generated
  - Used to settle disputes about the occurrence or non-occurrence of an event

The Laws

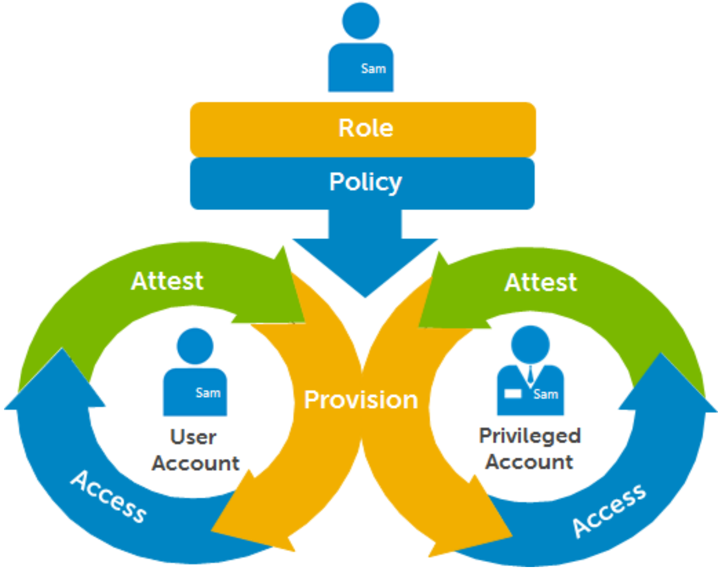
Record Everything – Record Everyone

- Privileged Session Management
  - Record all privileged account access
    - Imagine a DVR that you can replay, fast forward, rewind and search by command
    - Store for forensic purposes
  - Extend to non-privileged accounts
    - Record <u>all</u> contract access
    - Record <u>all</u> partner access
    - Record <u>all</u> customer access
    - Record <u>all</u> user access (Yes, some firms are going this far!)

The Laws

Apply Governance & SOD to Privileged Accounts

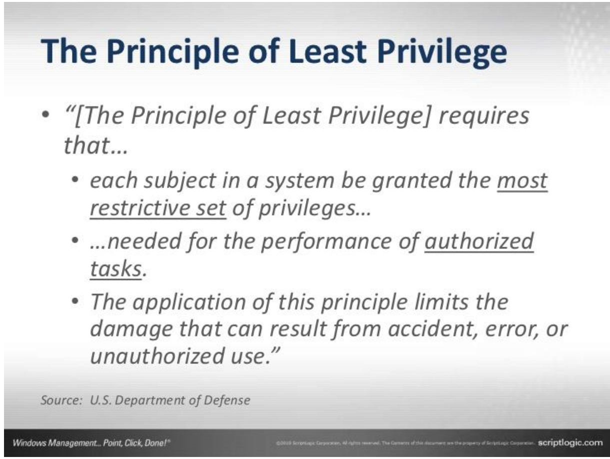
- Governance & Separation of Duties is already a strategic benefit of modern IAM systems
  - Extend these capabilities to privileged accounts.
- Privileged account governance & lifecycle are as, if not, more important than user account governance & lifecycle



The Laws

Apply Least Privilege to Privileged Accounts

- Sadly, many privileged accounts have no limits to their power
  - *nix systems
- Define privileged roles & assign users to those roles
- Do you understand the privileges required by programs that are installed on your systems? <u>Ask your vendors.</u>
  - Installation, day-to-day, upgrades



The Principle of Least Privilege

- *"[The Principle of Least Privilege] requires that…*
  - *each subject in a system be granted the <u>most restrictive set</u> of privileges…*
  - *…needed for the performance of <u>authorized tasks</u>.*
  - *The application of this principle limits the damage that can result from accident, error, or unauthorized use."*

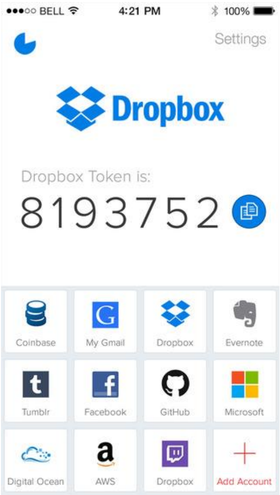
Source: U.S. Department of Defense

Windows Management.. Point, Click, Done!™ scriptlogic.com

The Laws

Protect the "Keys to the Kingdom" with two-factor

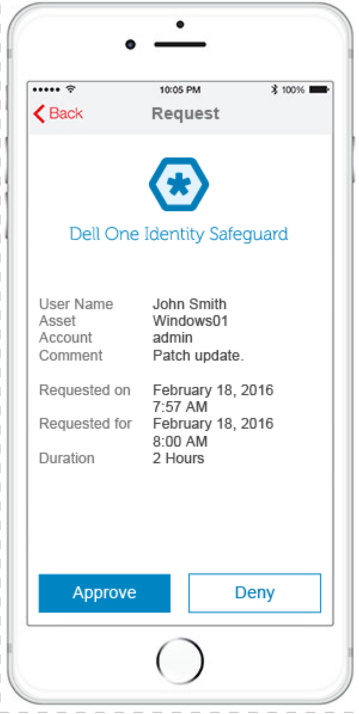
- Strong authentication is easy now
- Many form factors available
  - "Hard" tokens
  - "Soft" tokens
  - Push-to-authenticate/approve
- Recent advances
  - NFC
  - Bluetooth "beacons"
  - GPS/location information
- A password alone is NOT ENOUGH



Dropbox

Dropbox Token is:

8193752



Dell One Identity Safeguard

User Name	John Smith
Asset	Windows01
Account	admin
Comment	Patch update.
Requested on	February 18, 2016 7:57 AM
Requested for	February 18, 2016 8:00 AM
Duration	2 Hours

The Laws

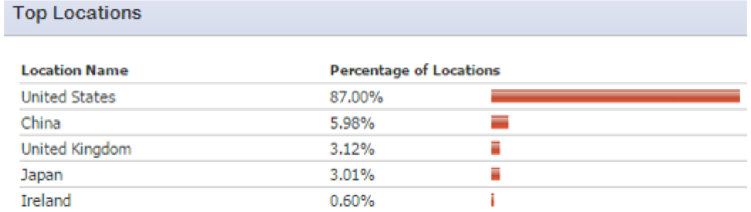
Incorporate analytics & risk into PAM

- Is Bob more risky if he’s accessing his account from outside the firewall?
- Is Carol more risky if she has never accessed a privilege account at 2:38am in the past?
- Is Ted more risky if he logged on at the start of the day and he is accessing a privileged account at 4:23pm but he’s still at work?
- Is Alice more risky if she usually only accesses privileged accounts on three Unix systems but today she is accessing many more?

The Laws

Practice safe PAM computing

- Never assume you are safe – even in your own office
- Use a wired computer for privileged access
- Leave it turned off and disconnected until you need it
- No e-mail client, no web browser, no programs other than what you need to accomplish your tasks
- Boot a secure virtual image and work from there
- You are ***NOT*** safe at home
  - My home network…



Top Locations

Location Name	Percentage of Locations
United States	87.00%
China	5.98%
United Kingdom	3.12%
Japan	3.01%
Ireland	0.60%

Conclusions & Rules-of-Thumb

- Privileged account inventories are temporally inaccurate
- Privileged accounts belong in a safe or a vault
- There is no one solution for all attack vectors mentioned
- There will always be a weaker link as you strengthen your PAM capabilities. PAM fortification is exceptionally important yet only one piece of the bigger puzzle.

Action Plan & Additional Reading

Your Action Plan

- 0-30 days
  - Inventory your systems and bucket them by OS; stack rank systems by risk
  - Document current PAM, fire-call/break-glass & routine maintenance practices
  - Look for and change all default passwords
  - Management education checkpoint #1 – Inventory & Risk report
- 30-60 days
  - Inventory service account and SSH key usage by system risk
  - Document current service account password & SSH key rotation practices, if any
  - Management education checkpoint #2 – Learnings & Discoveries
- 60-90+ days
  - Inventory all SaaS apps & administrators
  - Document current SaaS PAM best practices & SaaS shadow app inventory
  - Management education checkpoint #3 – Recommendations & Action Plan

Get Educated and Educate Others

- Security of Interactive and Automated Access Management Using Secure Shell (SSH)
  http://nvlpubs.nist.gov/nistpubs/ir/2015/NIST.IR.7966.pdf
- Privileged Access Management for Active Directory Domain Services (AD DS)
  https://technet.microsoft.com/en-us/library/dn903243.aspx
- 9 employee insiders who breached security
  http://www.csoonline.com/article/2692072/data-protection/data-protection-165097-disgruntled-employees-lash-out.html
- Keys to the Kingdom: Monitoring Privileged User Actions for Security and Compliance
  https://www.sans.org/reading-room/whitepapers/analyst/keys-kingdom-monitoring-privileged-user-actions-security-compliance-34890
- Twelve Best Practices for Privileged Access Management (you must be a Gartner client)
  http://www.gartner.com/document/3145917
- Dell's Library of Best Practice and Related Videos
  http://software.dell.com/video-gallery/#bysolutionprivilegedaccountmanagement

The best victory is when the opponent surrenders of its own accord before there are any actual hostilities... It is best to win without fighting.

Thank you for being here! Questions?

Jackson.Shaw@software.dell.com