SSH USER KEYS
THE FORGOTTEN CREDENTIALS

THE ACCESS GAP

Fouad Khalil
Director of Compliance
March 21st, 2016

WHO IS SSH COMMUNICATIONS SECURITY

We provide the means to discover, monitor and control privileged access and encrypted traffic without disrupting the flow of information, processes or business practices

Quick Facts:

- Inventors of the SSH protocol
- Listed: NASDAQ OMX Helsinki (SSH1V)
- 3,000 customers including 6 of the 10 largest US banks
- Original source of OpenSSH

What We Do:

- Privileged Access Control
- Encrypted Channel Monitoring
- SSH User Key Management
- Data-in-Transit Encryption

AND WHAT DOES THAT EQUATE TO FOR AN ENTERPRISE?

IN SOME 10,000 UNIX/LINUX HOSTS IT EQUATES TO:

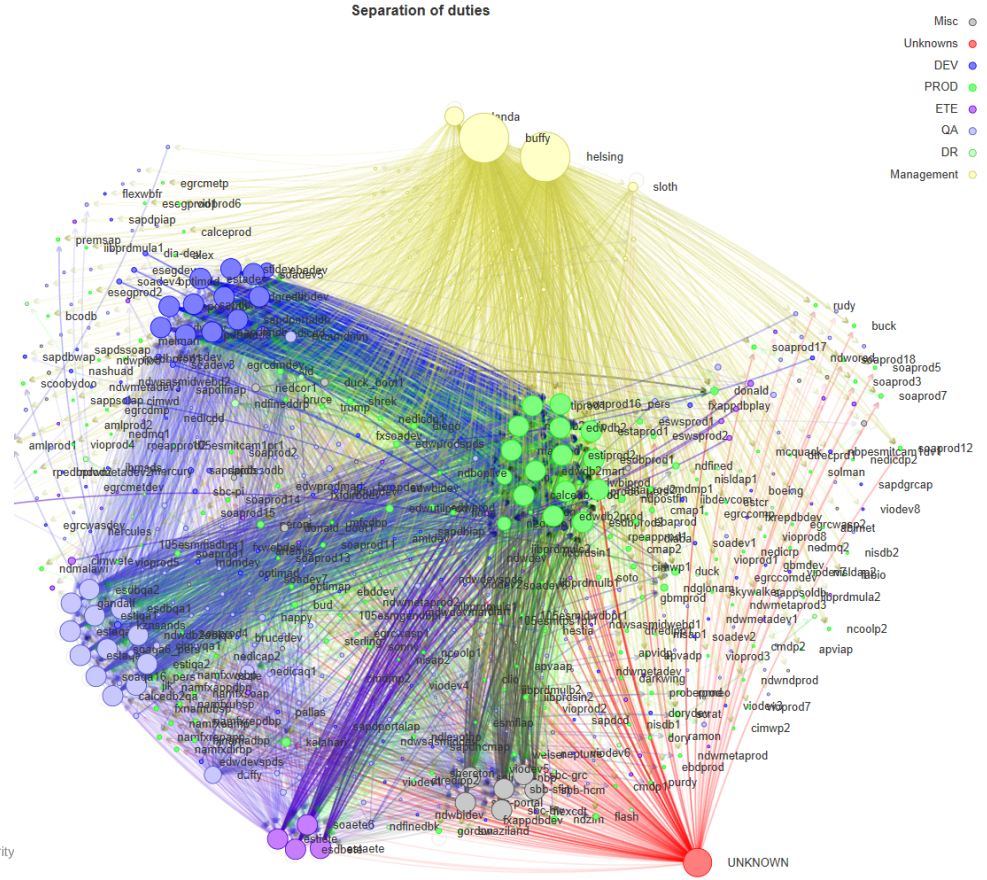
- 1.5 MILLION APPLICATION KEYS GRANTING ACCESS
- 70K DATABASE ADMINSTRATOR KEYS GRANTING ACCESS
- 70K SYSTEM ADMINSTRATOR KEYS GRANTING ACCESS
- 7K MONITORING KEYS GRANTING ACCESS
- UP TO 1 BILLION AUTHENTICATIONS PER YEAR GRANTING ACCESS
- UP TO 30 MILLION AUTHENTICATIONS FOR THE MOST ACTIVE KEY GRANTING ACCESS
- UP TO 90% OF THE ACCESS IS OBSOLETE

SO WHAT'S THE GAP?

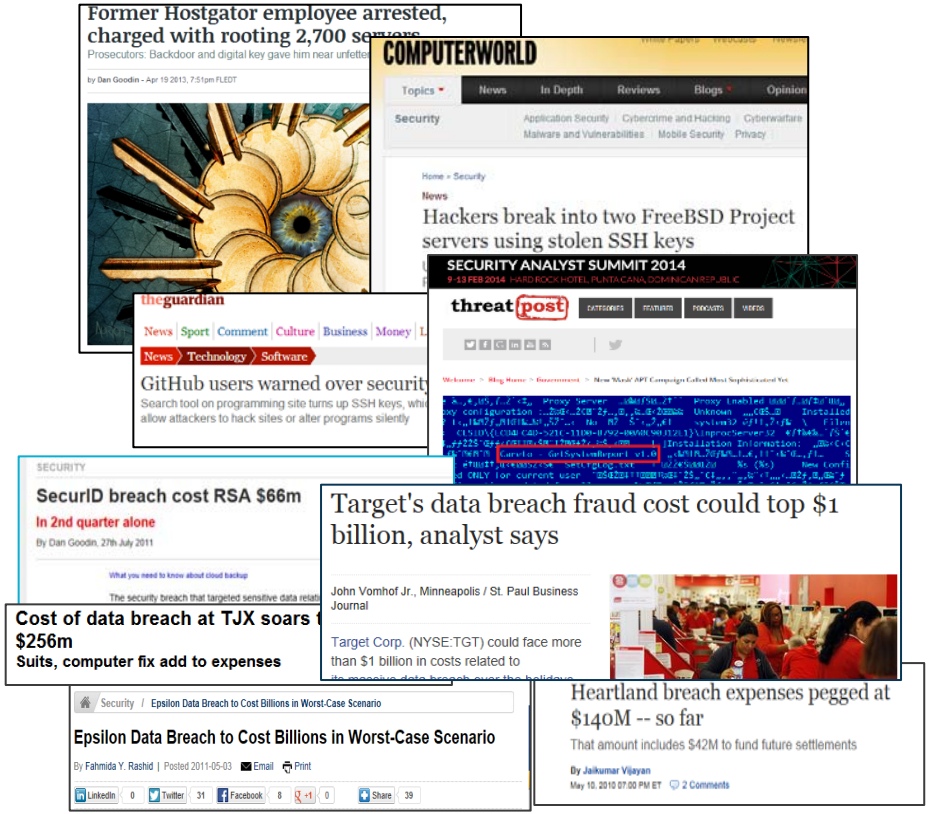
1. Lack of visibility of SSH user key based trusts for interactive and M2M access
2. Lack of monitoring capabilities of key based trust access
3. Lack of provisioning ownership process (on premise, to cloud, 3rd parties)
4. Lack of revocation processes
5. Lack of rotation processes
6. Lack of ability to remediate non-compliant access
7. Lack of ownership of the access being provided
8. Lack of clear policies of SSH user key based access

SO WHAT'S THE GAP LOOK LIKE?

THE UNAUTHORIZED DEV TO PROD CONNECTION



CHAINED SERVER PRIVILEGED ACCESS: BUSINESS DISRUPTION



Sony Pictures
Hijacked SSH private keys

“Its understood that a single server was compromised and the attack was spread from there”

“It was discovered that private keys used for authentication were taken”

ssh

THE REMEDIATION PROCESS AND ONGOING GOVERNANCE

PHASE 1
DISCOVERY & MONITORING

PHASE 2
LOCKDOWN

PHASE 3
REMEDIATION

PHASE 4
RECERTIFICATION
&
IDENTITY GOVERNANCE

JUST THE TIP OF THE ICEBERG

NIST-IR 7966

Security of Interactive and
Automated Access Management
Using Secure Shell (SSH)

This publication is available from:
http://dx.doi.org/10.6028/NIST.IR.7966

LEAVING YOU WITH ONE THOUGHT

SSH Keys = **Credentials** = **Access**

THANK YOU!!

To Learn More, Please Stop By Our Booth

FOLLOW US
@SSH

VISIT US AT
WWW.SSH.COM