Inside the Head of a Database Hacker

Mark Fallon
Architect/Security Lead
Database

ORACLE

Safe Harbor Statement

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Analyzing Threats

- Intent
- Capability
- Opportunity
- Impact

Intent

- Different hackers have different motivations
  - Financial
  - Information gathering
  - Idle curiosity
  - Malicious intent
  - Leveraging resources
- Verizon Data Breach results
  - 73% Financial, 21% Espionage, 6% FIG (Fun, Ideology, Grudge)
- If the data or system is valuable to you, it is valuable to someone else

Capabilities

- Anything that can be automated, will be
- Anything with a known vulnerability will be leveraged
- There is market for tools / exploits
- Not everyone is a state sponsored actor
  - Though we have seen their tools leak out
  - Criminal organizations take similar approaches

Trawling the web

- Last year, systems without passwords
  - 2.2 Million records “terrorist database” used by banks leaked online
  - 154 Million US voters
  - 93 Million Mexican voter records
  - 1 Million BeautifulPeople dating records
- This year, data leaks turned to ransomware
  - Read the records
  - Delete the records
  - Leave the ransom note
- Lists of unsecured systems easily available
  - Search engines exist for IoT

Phases of attack

- Recon
- Compromise
  - Infiltration
  - Command and control
- Lateral Movement
- Elevation of Privilege
- Completion of Mission

What is this used for?

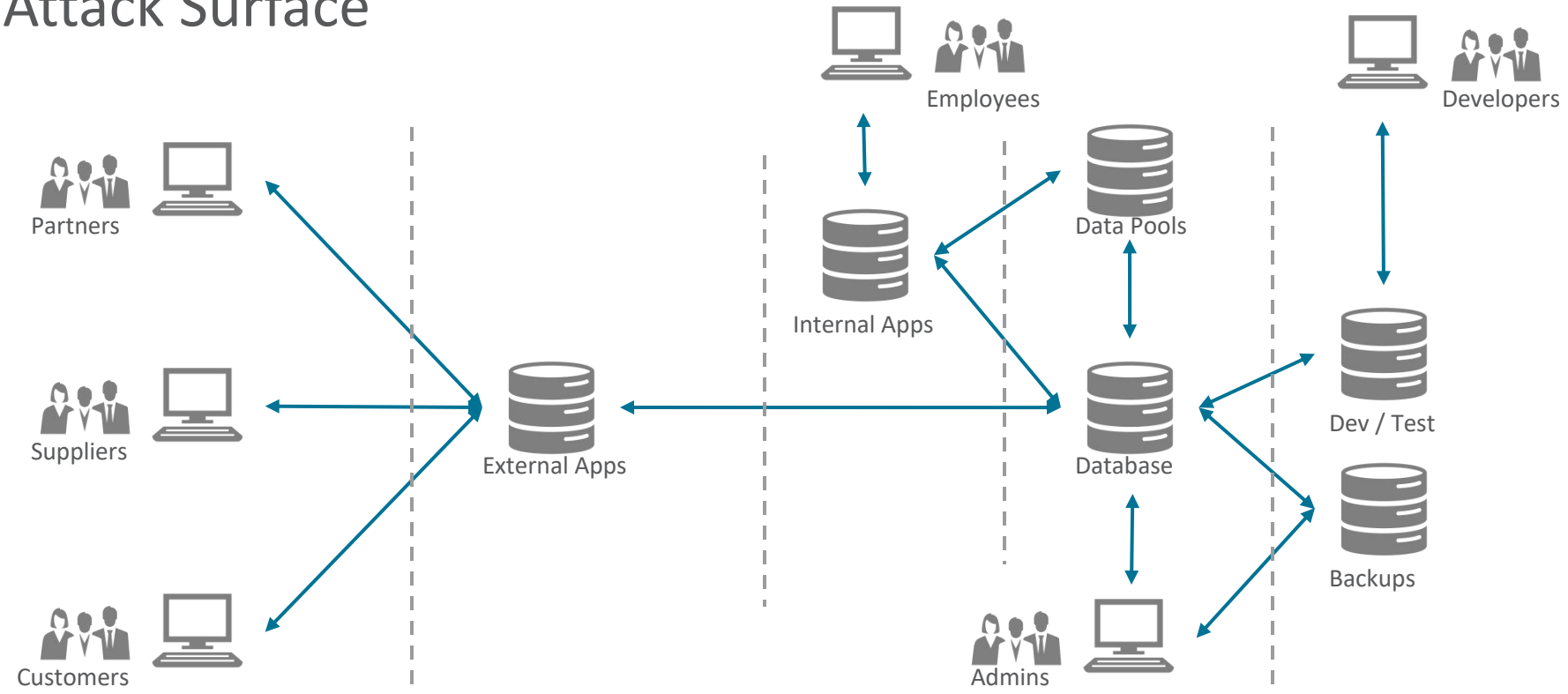
Designer's View
- Currency token

Hackers View
- Lever
- Screwdriver
- 0.200 oz weight
- Magic Prop
- History lesson
- Decision maker
- Weapon
- Force open an electrical fuse
- …

How do I get in?

Recon / Infiltration / Lateral Movement

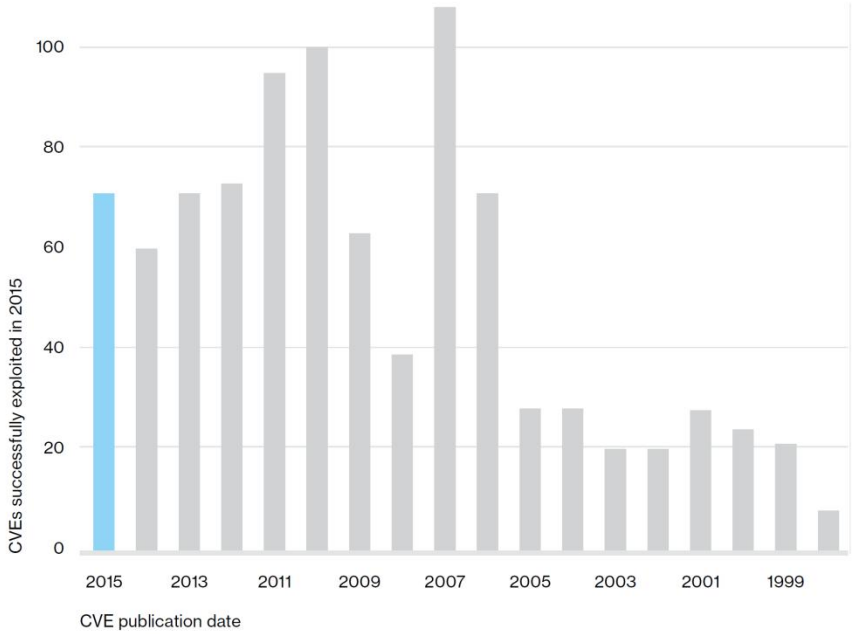
Attack Surface



Attack Vectors

- Verizon Data breach Report
  - 63% involved stolen credentials
    - Hacking, Phishing, Malware, Weak or Default Passwords
  - 40% involved a Web Application
    - 95% financially motivated
    - SQLi, Web Shells
  - 8% involved insiders abusing privileges
    - 14% C-Level, 14% Admins
- Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Old Bugs Live On



Source: http://www.verizonenterprise.com/verizon-insights-lab/dbir/

Equifax & other Stories

- Equifax
  - Initial breach through web application
    - Known vulnerability in Apache Struts component
      - Patch released March 6th, attack started March 10th
  - Hackers setup Web Shells to maintain access
- Deloitte
  - Credentials stolen for e-mail server in Microsoft cloud
- After news broke researchers had a look a both firms
  - Trivial username/password for other systems
  - Credentials, passwords other details found on GitHub, Google Docs
  - Unprotected RDP (Remote Desktops) discovered

OPM Breach

- OPM (Office of Personnel Management) breached repeatedly
  - Timeline shows attacks spanning years
- System relied on perimeter defenses
- Compromised by multiple attackers
- Malware planted on machines throughout the organization
- Key-logging malware used to get passwords from DBAs
  - PlugX malware found on SQL Server DBAs machines
- Source: https://oversight.house.gov/wp-content/uploads/2016/09/The-OPM-Data-Breach-How-the-Government-Jeopardized-Our-National-Security-for-More-than-a-Generation.pdf

I’m in, now what?

Elevation of Privilege / Completion of Mission

Aims

- Depends on motivation
- Three main aims:
  1. Retrieve Data
  2. Modify Data
  3. Elevate Privileges and Pivot

Retrieve Data

- Reading the data may be enough
  - PII, Credentials, Document retrieval etc.
- Data retrieval method depends on access vector
  - Direct SQL connection
    - Lost credentials / SQL Injection
    - May be signaled by high loads / volume of data
  - Indirect exfiltration
    - Blind SQL injection – leveraging requests with side effects
    - May be signaled by volume of requests
  - Direct Copy
    - APT collating files and then shipping them out

Modify Data

- Adding or modifying transactions
  - Balance adjustments
  - Transfer funds
  - Grant Privileges
  - …..
- Harder to do with a SQL injection issue
- Attacker needs to understand schema and business logic
  - Scanning of metadata may be a signal
- Auditing needed to monitor sensitive tables

Elevate Privilege and Pivot

- System privileges, ability to change non-schema objects
  - Ability to modify objects or settings across schema / system
- Non-public object privileges
  - Grants on SYS owned packages
- Access to the OS
  - ACLs / Directory Objects / External Jobs / Java Privileges
- Access to other systems
  - Dblinks, inside the same firewall

Security Needs to be a Collaboration

- Database Security
- Application Security
- Network Security
- End-point Security
- Process
- Employee Education
- Physical Security
- Supply Chain Security

Impact

- Loss of business
  - Recovery
  - Reputation
- Fines / Compensation
  - HIPAA
  - GDPR
  - Class actions
  - ……
- Resignation / Firings

What can I do?

- Identify your assets
  - Know what data you have and where it is copied to
- Secure all databases
  - Make sure that there are no insecure settings, default passwords etc.
  - Make sure all databases are patched and there is a patching plan in place
- Reduce your attack surface
  - Remove unnecessary copies of data
- Backup your data
  - Ensure you can recover from the backups
- Start with encryption
  - Backups, Networks and Tablespaces

What can I do?

- Monitor your systems
  - Enable auditing
  - Make sure that the audit records are actually useful / been looked at.
- Start to mitigate the risk from password loss / weak passwords
  - User profiles
  - Deploy Database Vault, Train DBAs on best practices
  - Remove unnecessary privileges
  - Strong Authentication for privileged users
- Compartmentalize
  - Ensure a breach of one database is not a breach of all
    - Use lockdown profiles with Pluggable Databases

What can I do?

- Work with application development
  - Deploy AVDF (Audit Vault Database Firewall)
  - See if Redaction is applicable to current applications
  - Develop application with RAS (Real Application Security)

Solutions

Problem	Technology
Poor configuration	DBSAT, Cloud Control
Identify Assets	Cloud Control, Sensitive Data Discovery
Spreading of production data	Masking
Stolen Credentials	Database Vault, Privilege Analysis, RAS, Strong Authentication
Application Vulnerabilities	AVDF (Audit Vault Database Firewall)
Infrastructure Compromise	TDE / Network Encryption / Key Vault
Insider	Redaction / RAS / VPD / OLS
Abuse of privileges (Insider / stolen)	Privilege Analysis / Database Vault / AVDF
System Monitoring	AVDF

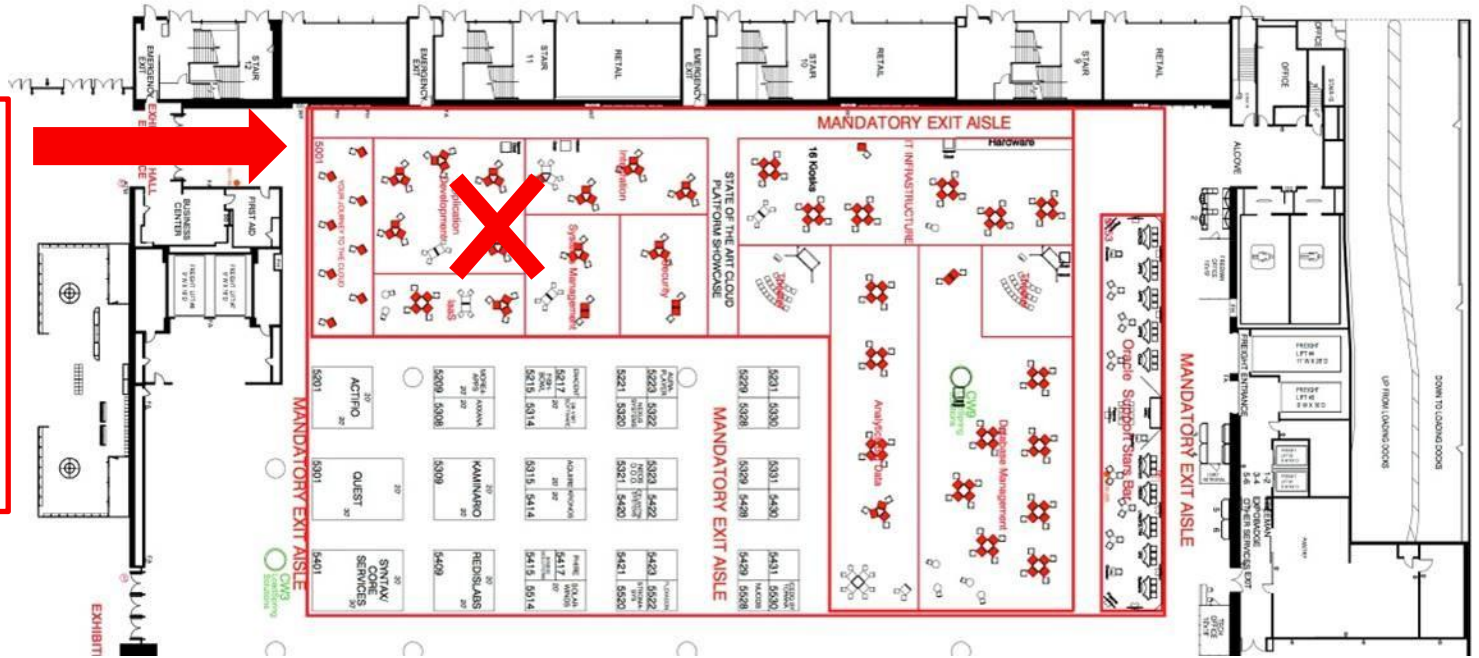
Visit Database Security in the Demo Grounds

SOA-71

SOA-72

SOA-73

SOA-74



Moscone West

Database Security at Oracle OpenWorld 2017

Session	Title	Speaker	Location	Date & Time
CON6574	NEW FEATURE! Centralized Database User Management Using Active Directory	Oracle Epsilon	Moscone West - 3011	Mon., 3:15-4:00
CON6575	NEW! Database Security Assessment Tool Discovers Top Security Risks	Oracle	Moscone West - 3011	Mon., 5:45-6:30
CON6573	Data Management and Security in the GDPR Era	Oracle Capgemini	Moscone West - 3011	Tues., 3:45-4:30
CON6580	Encrypt Your Crown Jewels and Manage Keys Efficiently with Oracle Key Vault	Oracle	Moscone West - 3011	Tues.,4:45-5:30
CON6576	Accelerate Your Compliance Program with Oracle Audit Vault and Database Firewall	Oracle, Symantec	Moscone West - 3011	Tues., 5:45-6:30
CON6572	Inside the Head of a Database Hacker	Oracle	Moscone West - 3014	Wed. 11:00-11:45
CON6618	Sneak Preview: Oracle Data Security Cloud Service	Oracle	Moscone West - 3011	Wed.,2:00-2:45

Safe Harbor Statement

The preceding is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.