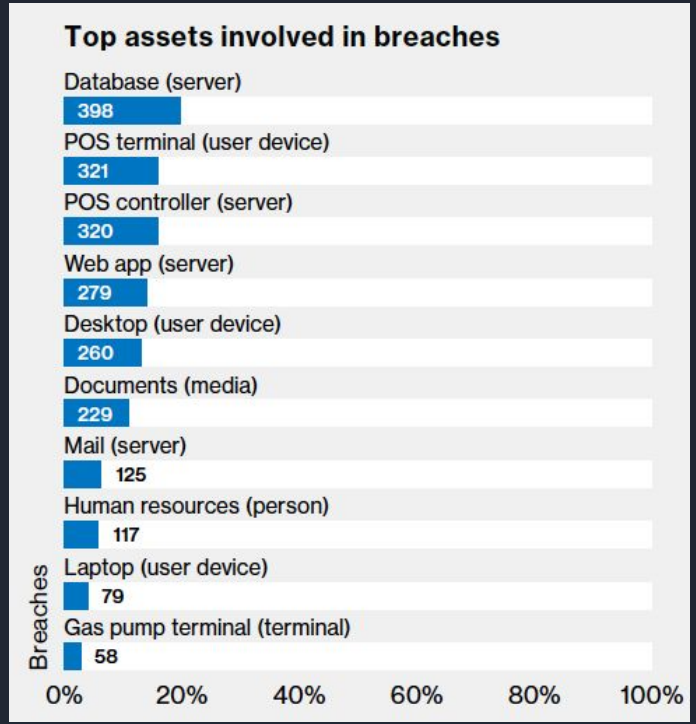
Database Security

Threats and Vulnerabilities

John Bissonette
Aaron McClure

Introduction

- Databases are the crown jewels of a business or organization
  - Security is paramount
  - Vulnerabilities grant attackers “keys to the kingdom”
- Threat Domains
  - Within the DBMS
  - External IS and architecture vulnerabilities
  - Human element
- Types of attacks
  - Data theft
  - Ransom
  - Data destruction
  - Advanced Persistent Threats (APT)



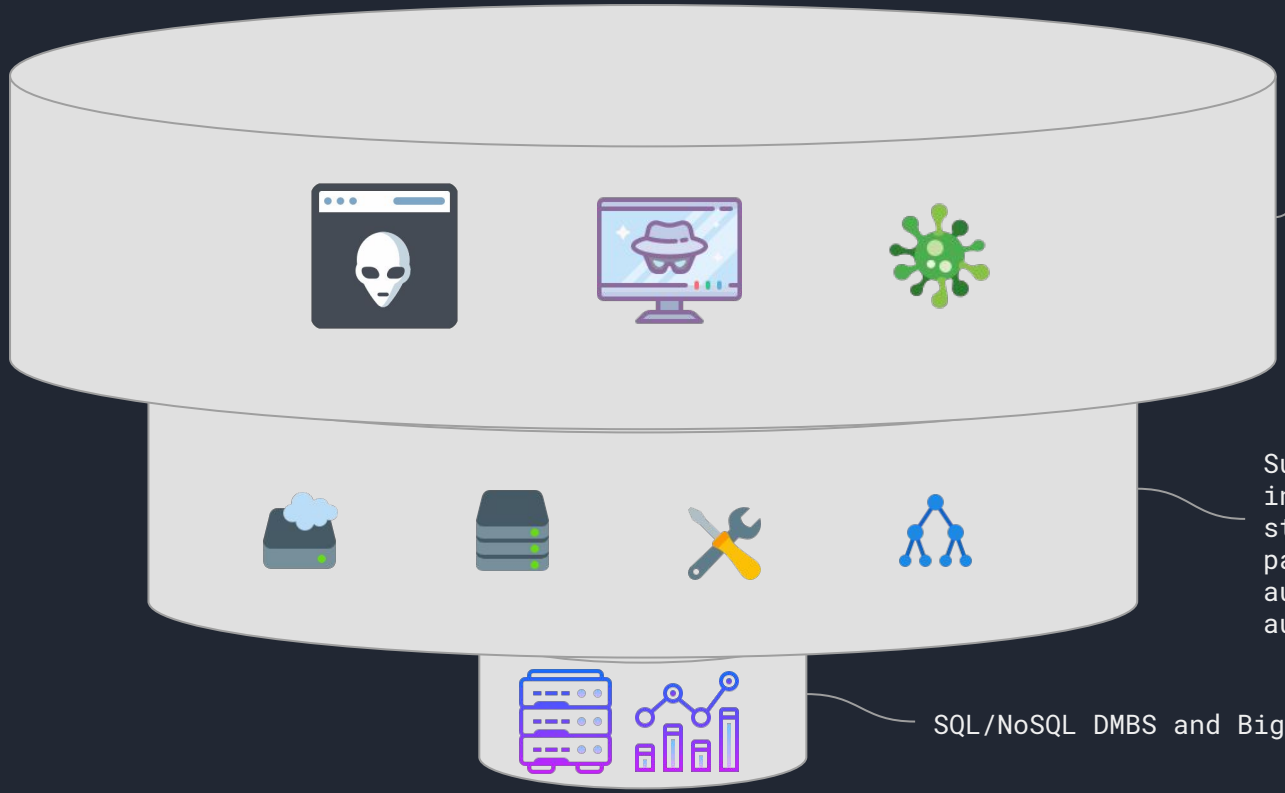
Introduction (cont.)

- Mitigation and minimization strategies
  - Begins with good policies
  - Monitoring and compliance
  - Is a continuous process
  - Education of workforce and employee buy-in
- Current landscape
  - Threats and responses
- Real World Case Studies
  - Yahoo - Social Engineering
  - Equifax - Improper auditing, platform vulnerabilities, patching
  - Uber - Improper data storage media

Threat Domains and Threat Vectors

Overview

External threats: viruses, ransomware, hacktivists, blackhats, criminal organizations, APTs



Surrounding infrastructure: servers, storage, patching/maintenance, authentication and authorization

SQL/NoSQL DMBS and Big Data

I. Threat Vectors Intrinsic to DBMS

- Database Configuration
  - Broad roles for user assignment
  - Excessive, inappropriate, or unused privileges
  - Leaving default configurations in place
- Authentication and Authorization
  - Uses database authentication instead of Enterprise auth
- Auditing and Monitoring
  - Weak audit trails
  - Not monitoring queries against sensitive data or by privileged users
- Patching and Change Management
  - Not applying regular updates or patches to DBMS
  - Not testing patches against Dev/QA/Stage env before Production

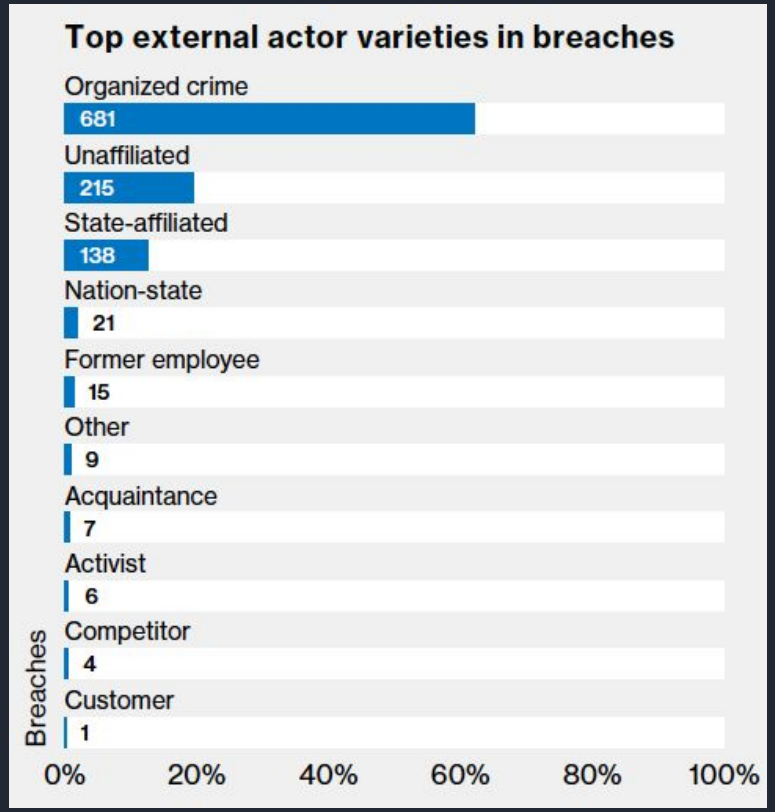
II. Platform, Infrastructure, & Architectural Threats

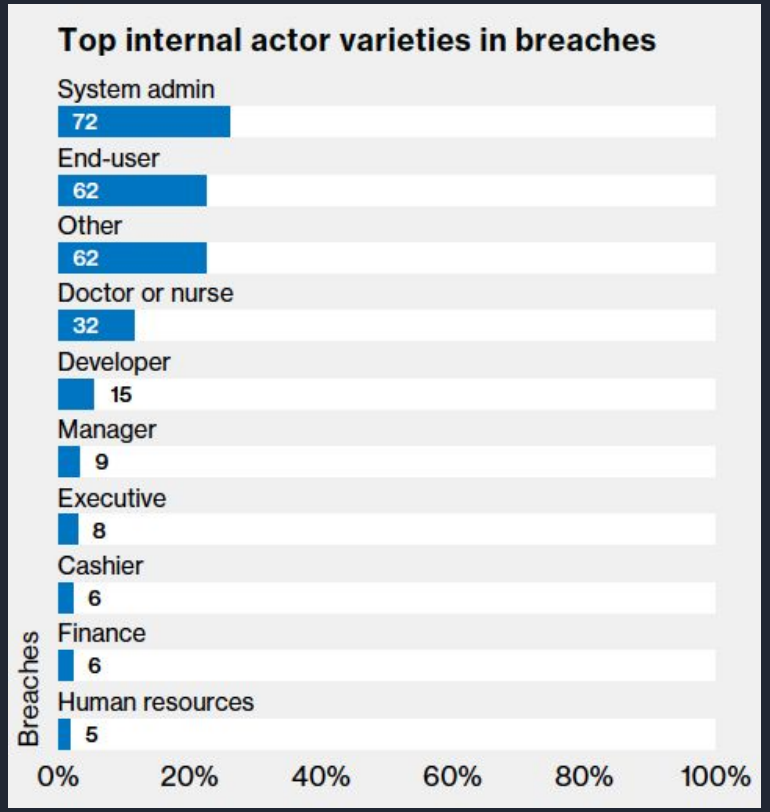
- DBMS Servers
  - OS exploits
  - Hypervisor exploits (if virtual)
  - Container exploits (Kubernetes, Docker)
  - No secondary or backup cluster
  - Allows direct client access
- Network Architecture
  - Improper segmentation of network
  - Config of h/w firewalls, edge routers
  - No strict firewall rule change procedures
  - Monitoring of network traffic
- Backup Strategy & Storage Media
  - Unencrypted backups
  - Lax key management
  - Untested recovery procedures
- Web/Application Servers
  - Unsecured files/source code
  - Environment variables exposed
  - Open ports
  - 2FA not enforced
  - SQL injection vulnerabilities
- Enterprise Architecture
  - ACLs unused, too broad
  - Weak password policy
  - Poor change management controls
- Compliance & Auditing
  - Weak audits for compliance with relevant laws and regulations (HIPAA, SOX, FERPA)

III. Human Element

- Insider Threats
  - Disgruntled employees
  - No criminal background checks
  - Hacktivists
- Outsider Threats
  - Criminal organizations (mafia, cybermilitias)
  - Blackhats
  - State-sponsored groups
- Social Engineering
  - Manipulation, trickery, blackmail, etc.
  - Requires awareness and low power distance within org.
  - Confidence tricks
    - Phishing and derivatives
    - Pretexting
    - Water holing

Internal & External Threat Actors





Advanced Persistent Threats (APT)

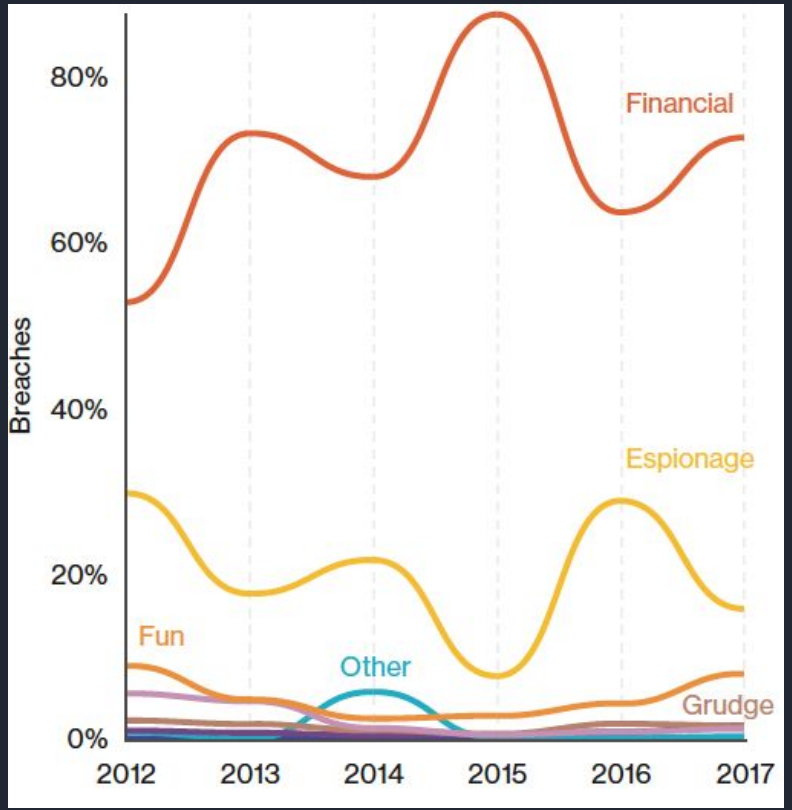
- Complex, long-term, pervasive, stealthy attacks
- Use multiple threat vectors throughout the kill chain
- Target entire sectors and industries
- Extremely well-resourced, typically by a nation-state
- Can take months or years to detect and mitigate
- Are mostly motivated by espionage, advancing the goals of a nation-state

Notable Examples:

- GhostNet (China, 2009)
- Operation Aurora (China, 2009)
- Stuxnet (US/Israel, 2010)
  - Also Duqu, Flame
- Red October (unknown, 2012)

Attacker Motivations

- Financial
  - Identity theft, PII
  - Financial account credentials
  - Ransom
- Espionage
  - State-sponsored (spying)
  - IP theft
  - Cyberwarfare
- Grudge
  - Political/Ideological
    - Not state-sponsored
  - Disgruntled employee
- Fun
  - Celebrity hacks
  - Script kiddies



Case Study: Yahoo (Social Engineering)

- Largest data breach of the 21st century, occurring in 2013-2014
- Yahoo was the victim of an ATP, sponsored by the Russian Government
- 3 billion user accounts compromised.
- Initial attack vector was a spear-phishing email
- Hackers gained access to Yahoo’s network, located user database and Account Management Tool and installed backdoors to not lose access
- Hackers located a backup of Yahoo’s user database and transferred it to their servers
- Names, phone numbers, security questions, recovery emails, and a unique cryptographic value assigned to each account were compromised
    - These unique cryptographic values (called “nonces”) were ran through a script on Yahoo’s server to generate cookies that gave access to users email accounts without the need for the passwords

Case Study: Equifax

Equifax was the victim of data hack in 2017 that affected at least 143 million consumers and resulted in the revelation of at least 209,000 consumer credit card details. Equifax was notified in 2016 about a XSS (Cross-site Scripting) vulnerability but failed to address it. (3) XSS is described as a type of injection: “in which malicious scripts are injected into otherwise benign and trusted web sites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user.“ This is an issue when a user is able to send input that is not validated and used to produce output. Ultimately, Equifax failed to address the issue which highlights an issue in their security protocols.

The actual hack was the result of RCE (Remote Code Execution) which does not require privileged users to interact with data but rather is a complete compromise of a web server. Exploitation of CVE-2017-6638 led to the successful hack of Equifax data. Apache Struts 2 which is an open source web application framework Equifax relied on experienced a security vulnerability involving the manipulation of HTTP headers. GET/POST requests initialized when viewing/interacting with webpages involve the transmission of HTTP headers. Attackers found that by modifying these headers in a certain way, system commands could be executed on affected systems. Apache quickly announced steps companies should take to prevent this, however, Equifax failed to act quickly. As a result, this exploitation was used to hack Equifax’s sensitive information. This case highlights the importance of maintaining updated security infrastructure and responding quickly as new threats are discovered.

Case Study: Uber

- Late 2016 Uber gets hacked, exposing over 57 million users and 600,000 drivers were exposed
- Incident occurred after hackers gained access to Uber’s GitHub account, finding credentials to Uber’s AWS (Amazon Web Services) account
  - Therefore, hackers were able to simply login and access *everything*
  - This information should never have been store in plain text (in code) on a GitHub profile and demonstrates the importance of not placing secure information on unsecure platforms.
- As a result, Uber stopped using GitHub for anything other than open source projects
- Uber admits to not using multifactor authentication on its GitHub account
  - Multifactor authentication is an important trend in the security industry that requires users to use more than one authentication method from independent sources to confirm a user’s identity