Fraud Detection @salesforce

Robert Fly
VP, Product Security

Your success. Our cloud.

salesforce.com
whoami

- VP, Product Security @salesforce
- Ex-MSFT Senior Security Lead (BPOS)
- Founding member CSA
- Author of crappy book you’ve never read

developer.force.com/security
@securecloudev
@salesforce view of fraud

- Golden Rule: Assume Clients Are Compromised
- Data from Salesforce can be used for:
  - Giant Rolodex
  - Pipeline & Forecasting (Stock Market)
  - Platform (Use Your Imagination)
Robbing a Bank

Physical Controls
Electronic Monitoring
Human Monitoring
Instant Detection and Response
Controlled Access
Multi Factor Auth
Transaction Verification

Attribution: Michael Coates
Would You Bank Here?

- Ineffective Monitoring
- No Real Time Analysis
- Unnecessary Partner Trust
- No Response Capability
- Limited Security Training
- Single Factor Auth
- Alternate Admin Access
- Partial External Controls
- Police
- Tellers
- Safe

Attribution: Michael Coates
Fraud Detection Points

- Client, Server [active], Server [passive]
- Security Touchpoints (Coding/Design Guidelines, Threat Modeling, QA, external assessments, etc)
Client

Client Hash Validator

Client Side Validation

[recommended] AV, Anti-Malware, etc
Server [active]

Customer Options
- Identity Confirmation
- IP Restrictions, Login Time Restrictions
- Account Locking (15m, 30m, Admin) to prevent Brute Forcing
- SSO Options (Delegated Auth, SAML, Two Factor, etc)
- Fine Grained Authorization
- Custom Domains

Request Oddities
- Cookie Reuse from different client
- One Time Token Reuse
- Chewed Cookie Reuse
- Known malicious strings, odd encodings, etc
- Some Referer Checking

Salesforce Security Options
- Honeypots
- Limits, Limits, Limits…
- URL Blocking, User Lockout, Org Shutdown, App Shutdown
Server [passive]

**Customer Security Contacts & Incident Response Process**

**Logging and Auditing**
- Login History
- Administrator Auditing and Logging
- Object Field History Tracking
- Read Level Logging
- Web Logs
- Compromised Credentials

**Transactional Anomalies**
- Impossible Travel
- Impossible Time Travel
- Multi-Tenant Oddities
  - One IP, multiple orgs
  - Similar Actions, Multiple Orgs within X amount of time
- Scripted Unauthorized Attacks
- Feature Overuse
Questions