MARTIN SNYDER (@MARTINSNYDER)

DATA BREACH RESISTANT SYSTEMS

AGENDA

- Background
- Nightmare Threats
- Response
- Example Application Narrative
- Next Steps

BACKGROUND – TRADITIONAL DISCUSSION

- Application Security
  - Library Vulnerabilities
  - Software Development Practices
- Operational Security
  - Software Stack Vulnerabilities
  - Tools vs. Labor

BACKGROUND - PLAYING THE ODDS

- Exposure
  - How many exploits have existed in your system?
  - If you found evidence of a penetration, how would you know exactly what was “taken”?
- Risk Factors
  - What you have
  - Who you are facing

BACKGROUND - RECENT EXAMPLES

- $5MM/day siphoned from video ad framework
  - https://www.forbes.com/sites/thomasbrewster/2016/12/20/methbot-biggest-ad-fraud-busted
- $100MM+ bank fraud
  - https://www.wired.com/2017/03/russian-hacker-spy-botnet/
- “Unauthorized code” in Juniper Firewalls
  - https://arstechnica.com/security/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/

NIGHTMARE THREATS

- Privileged Operators
  - Whistleblowers
  - Coercion - Bribery, Judicial, etc…
- Hardware Theft
  - Backups
  - DR systems

NIGHTMARE EXAMPLE

- June 2013
  - First media reports based on Snowden disclosures
  - Barack Obama says “I'm not going to be scrambling jets to get a 29-year-old **hacker**.”
- August 2013
  - Lavabit shuts down

RISKS ASSOCIATED WITH ENCRYPTION

- Key Security
- Long-view attacks

SOLUTION BLUEPRINT

- Limited data storage
- Distribute stored data
- Distribute via write-only connections
- Storage in non-reversible formats
- Cryptographic hashing favored over encryption

JSON WEB TOKENS (JWT)

- Claims
- Signature Algorithm
  - HMAC
  - RSA
- Secret Key

COST-BASED CRYPTOGRAPHIC HASHES

- PBKDF2
- bcrypt
- scrypt

EXAMPLE APPLICATION - WRITTEN TEST ADMINISTRATION

- Three classes of user
  - Unauthenticated
  - Administrator
  - Candidate
    - New
    - In Progress
    - Finished

NARRATIVE – 1. ADMIN SETUP

- User navigates to application
- User enters email address
- Email verified against configuration
- Login link emailed to user

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
			Auth Link

NARRATIVE – 2. USER INVITATION

- Admin clicks link to enter application
- Admin enters candidate email address for invitation
- Login link emailed to candidate

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link			Auth Link

NARRATIVE – 3. USER LOGIN

- User clicks link to enter application
- User answers questions related to status
- User reviews instructions

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link	Status Answers		Auth Link

NARRATIVE – 4. USER STARTS EXERCISE

- User clicks button to start exercise
- User works on the exercise

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link	Status Answers	h(email), ‘start’, ts	Auth Link

NARRATIVE – 5. USER FINISHES EXERCISE

- User uploads response
- Status answers uploaded automatically
- System emails complete submission back to administrators

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link	Status Answers	h(email), 'start', ts h(email), 'finish', ts	Auth Link Test Submission

NARRATIVE – 6. SUBMISSION REVIEWED

- Admin clicks link to enter application
- Admin enters candidate email address for response
- Admin selects ‘Accept’ or ‘Decline’
- System emails response to candidate

DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link System Reply	Status Answers	h(email), ‘start’, ts h(email), ‘finish’, ts h(email), ‘reply’, ts	Auth Link Test Submission

FINAL DATA FOOTPRINT

Candidate Email	Local Stg	Database	Admin Email
Auth Link	Status Answers	h(email), ‘start’, ts	Auth Link
System Reply		h(email), ‘finish’, ts	Test Submission
		h(email), ‘reply’, ts	

EPILOGUE

- Other Considerations
  - System security vs. asset security
  - System security vs. process security
  - Accessibility vs. value

FURTHER READING/VIEWING

- Bruce Schneier - “Data Is a Toxic Asset, So Why Not Throw It Out?”
  - https://www.schneier.com/essays/archives/2016/03/data_is_a_toxic_asse.html
- Jarrod Overson - “What Happens When Data Gets Breached?”
  - https://www.infoq.com/presentations/security-protection-2016

NEXT STEPS

- Adopt new perspective for data architecture
- Limit data collection
- Store data in minimally useful representations
- Arrange a personal demo of the application by emailing careers@wingspan.com
- Donate to the The Electronic Frontier Foundation

THANK YOU

Questions?

MARTIN SNYDER (@MARTINSNYDER)

DATA BREACH RESISTANT SYSTEMS