Patrick Watson

Contact

Cell : 404-966-5497
e-mail : patrick@patrickwatson.org
Location : Atlanta, GA, US

Summary

Patrick Watson is a security architect with over a decade of experience championing secure application development and enterprise architecture in the payments and financial technology industries. He has spoken at multiple public and private conferences and has several patents. His experience ranges from secure application management and full life-cycle product development to enterprise policy authorship and security operations.

Speaking Engagements

Black Hat USA 2016, *Breaking Payment Points of Interaction:* **https://youtu.be/B3CUWh_Q-h4**
DEFCON 24 Skytalks
BSidesLV, *Breaking Payment Points of Interaction*
NCR Innovation Conference 2017, *Blockchain Technologies*
American Express DevCON 2021, *Threat Modeling*

Patents

Virtual Reality Transaction Integration	Granted, 7/5/2022, us 11,379,806
Multifactor Authentication from Messaging Systems	Granted, 12/21/2021, us 11,206,248
Secure Payment Processing Within Messaging Systems	Granted, 4/14/2020, us 10,621,562
Cross-Messaging Identity Mapping	Granted, 10/8/2019, us 10,439,980
Voice Authentication Within Messaging Systems	Granted, 6/11/2019, us 10,318,718
Cooperative Fraud-detection Processing	Pending, filed 9/28/2017, us 15/719,158

Certifications

Certified Information Systems Security Professional (CISSP)	#385815, 2/15/2011 to Present
Certified Information Privacy Professional, US Private Sector (CIPP/US)	6/20/2015 to Present
Certified Secure Software Lifecycle Professional (CSSLP)	#385815, 5/02/2016 to Present

Work Experience

American Express, Inc.

VP, Kabbage Security **2020 to Present**

Kabbage is a financial technology, primarily providing funding to small businesses. Kabbage has recently expanded service offerings to include payment processing, providing business performance insights, and checking account services.

Responsibilities

- ✓ Build and execute integration plan to uplift Kabbage Information Security to American Express standards
- ✓ Maintain Kabbage PCI DSS program, including new product design
- ✓ Act as Kabbage Data Protection Officer
- ✓ Information Security representative on Kabbage Data Governance Committee
- ✓ Support expansion of American Express' security architecture to public cloud
- ✓ Educating American Express personnel on AWS

Notable Accomplishments

- ✓ Administered Kabbage Confidentiality Operating Principles to ensure sensitive competitor data is not inappropriately accessed within American Express
- ✓ Integrated Tanium, Crowdstrike, Prisma, and other enterprise security tools with Kabbage Cloud
- ✓ 97% reduction in Kabbage open source & cloud configuration vulnerabilities
- ✓ Zero-downtime switchover from Kabbage SIEM/SOC to American Express SIEM/SOC, including migration of log ingestion infrastructure and alerting rules

Kabbage, Inc.

Security & Privacy Architect **2018 to 2020**

Kabbage was a financial technology company, providing funding to small businesses. Kabbage expanded service offerings to include payment processing, providing business performance insights, and checking account services. In 2020, Kabbage was acquired by American Express, Inc.

Responsibilities

- Create Kabbage Information Security Program
- Sole dedicated Information Security personnel from 2019
- Provide secure architecture and code review and mentoring to engineering teams (including .NET Core C#, Python, Terraform, Docker)
- Design application architectures to minimize cost while maximize security and compliance
- Lead incident response and facilitate Kabbage's Information Security Council operations
- Advocate for customer privacy and ensuring proper use of Kabbage's data lake
- Key custodian for Kabbage's Hashicorp Vault secrets management system
- Implement AWS based internal security applications using Terraform, AWS Lambda, and Python
- Assist Legal team with contract review and investigations
- Perform evaluation of potential vendors and acquisitions
- Oversee Penetration Testing

Notable Accomplishments

- ✓ Alerted Kabbage to PCI DSS obligations and implemented ongoing compliance programs for 4 services without delaying delivery timeframes
- ✓ Created and administered KaBounty, an internal bug bounty program
- ✓ Drove ratification of Kabbage's first Information Security Policy
- ✓ Created Kabbage's Incident Response Procedure, Encryption Usage Standard, Open Source Usage Standard, and various other standards and procedures
- ✓ Decreased Kabbage Phishing "frequent clickers" from ~87% of personnel to 10% and "serial clickers" from ~12% to < 1%
- ✓ Drove creation of Kabbage's SIEM using Splunk Cloud and ReliaQuest as Kabbage's Managed SOC
- ✓ Creation of automated Vendor security review process using Panorays
- ✓ Created Kabbage's Secure Development training program
- ✓ Information Security due diligence liaison for American Express acquisition, including technical expertise and evidence including generating Kabbage's software bill of materials, technical architectures, policy and procedural documentation, and answering information security questions of all sorts.

NCR Corporation

Application Security Architect **2014 to 2018**

NCR Corporation is a global technology company specializing in financial, payment, and retail software and hardware. The Software Solutions Application Security (SWSAS) team is responsible for ensuring that NCR's applications are developed securely, exposing NCR and its clients to a minimum of risk.

Responsibilities

- As a founding member of the SWSAS team, establish policies and grow the team within NCR
- Dedicated application security architect for the Epsilon, NCR EPS, RPOS (PCR/CFR), Fuel Connect, and Common Client products. Interim application security architect for ODSP, NCR's next generation cloud platform, and Optic.
    - Conduct security design and code review
    - Perform risk assessment for application changes
    - Oversee internal and external penetration testing
    - Create client facing security and Payment Application Data Security Standard (PA-DSS) compliance documentation
    - Manage product PA-DSS compliance program, including facilitating 3rd party assessment
    - Address client security questions and incident reports
    - Primary point of contact for internal secure development guidance
    - Initial point of contact for incident response
    - Privacy advocate & advisor
- Key custodian for Epsilon and NCR EPS encryption keys
- Provide PA-DSS and PCI DSS expertise to NCR Legal, including contract & patent review

- Develop security talent within engineering teams

Notable Accomplishments

- ✓ Drove compliance project for ODSP, taking the product from undeployed and with informal policies to a PCI-DSS compliant level 1 Service Provider in 3 months. This included policy drafting, reviewing product architecture, DevOps pipeline review, and running the PCI DSS audit project itself.
- ✓ Conducted PA-DSS assessments for over 30 major releases of NCR software.
- ✓ Grew SWSAS team from 2 to 10 members.
- ✓ Co-developed NCR's open source component vulnerability management program, including tool procurement, policy creation, and implementation
- ✓ Evaluated and selected NCR's standard container vulnerability scanning and protection engine
- ✓ Drove adoption of standardized code signing solutions within NCR
- ✓ Create SWSAS internal portal including secure coding guidelines, PA-DSS compliance tracking programs, and stack-exchange-like questions system.

Awards

- ❖ Runner up NCR Innovator of the Year 2016
- ❖ Nominated for 2018 NCR R&D Excellence Award. (Departed prior to award)

NCR Corporation

Application Developer I, II, III (Electronic Payment Systems) **2004 to 2014**

NCR Corporation acquired Radiant Systems in 2011. Radiant was a provider of both off the shelf and customized point of sale software and hardware. The Electronic Payment Systems (EPS) team was responsible for implementing and customizing the Epsilon/NCR EPS interfaces to 3rd party payment systems, allowing the partner points of sale to tender transactions via credit, debit, fleet, EBT, ACH, etc. The system also allows loyalty point accumulation or redemption and 3rd party gift card activation.

Responsibilities

- Design and implement new credit network interfaces and enhancements to existing products & support tools including the core Epsilon application framework.
- Epsilon maintenance, compliance, and security technical lead.
- Investigate Epsilon escalated cases, provide temporary workarounds, and implement permanent fixes
- Design and implement security enhancements to the core Epsilon application framework.
- PA-DSS technical point of contact for the EPS team. This includes creating customer-facing compliance documentation such as implementation guides and high-level security models, answering customer questions regarding PCI-DSS, and supporting certifications and audits.
- Train new hire employees and customers in EPS development standards, software architecture, and support techniques.
- Implement payment industry mandates such as Visa/MasterCard partial authorizations and compliance with new State and Federal laws such as FACTA.
- Maintain and support more than 100 credit products.
- On call 24/7/365 for emergency escalated support cases.
- Develop high performance software, ensuring that the electronic payment system can run under constrained resources (<32MB RAM, <20MB storage, <400MHz SH3 CPU) while maintaining sub second transaction times.

Education

2000 to 2003 **Bachelor of Science with Honor, Computer Science**
Georgia Institute of Technology, Atlanta, GA
Specializations in Networking, Databases, and Artificial Intelligence
Computer Science GPA: 3.5, Overall GPA: 3.3

References

References available upon request