PCI Compliance in the Cloud: A working example

John Knoll
jpknoll@ucdavis.edu
https://github.com/jpknoll

Scott Kirkland
srkirland@ucdavis.edu
https://github.com/srkirland

Adam Getchell
acgetchell@ucdavis.edu
https://github.com/acgetchell

UC Computing Systems Conference
July 10-12 2016
University of California Santa Cruz
Goal: Give to UC Davis

- Hired for Centralized Gift Processing
- UC PCI Audit Starts
- Priority Changes: Compliant Website that can take Credit Cards
Why a complete redesign?

- Replace an onsite Windows Server 2003
  - Oracle Forms Driven
  - Difficult Impossible to bring into compliance
- Switch credit card processors
  - TouchNet to CyberSource
- Modernize look and feel
  - Professional mockups & design
- Be ready before the on site audit (less one year)
  - Agile or Bust!
Investigate Payment Processors

- TouchNet
- PayPal
- Stripe
- CyberSource / Authorize.Net
Finalize your gift!
Enter your payment information 🛒

**VISA**

Name:
John Knoll

Card Number:
4111 1111 1111 1111

Expiration Date:
12/34

CVC:
123

Here's what we have so far

John Knoll is making a One Time $100 Donation to UC Davis Annual Fund.
Give to UC Davis

• Demo
What is PCI?

• Set of standards designed to make payment card processing security the responsibility of all parties involved.
  • Merchant -> Processor -> Bank

• Contractually Enforceable via Bank’s Merchant Account
  • Fines, Fee, or Account Termination

• Applies to anyone that accepts credit card payments, even if you don’t store cc details.
<table>
<thead>
<tr>
<th>Goal</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Protect all systems against malware and regularly update antivirus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
</tbody>
</table>
Meeting Compliance

• The Entire PCI Data Security Standard (DSS) applies to all levels and all environment types.

• Merchant Level (based on business size) Determines how you prove compliance:
  • Annual Self Assessment Questionnaire ("SAQ")
  • Annual Report on Compliances ("ROC") by Qualified Security Assessor ("QSA")
### Merchant Levels

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Any merchant — regardless of acceptance channel — processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Any merchant — regardless of acceptance channel — processing 1M to 6M Visa transactions per year.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants — regardless of acceptance channel — processing up to 1M Visa transactions per year.</td>
</tr>
<tr>
<td>SAQ Type</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A</td>
<td>Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage</td>
</tr>
<tr>
<td>B</td>
<td>Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>D-MER</td>
<td>All other SAQ-eligible merchants</td>
</tr>
<tr>
<td>D-SP</td>
<td>SAQ-eligible service providers</td>
</tr>
<tr>
<td>P2PE</td>
<td>Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>SAQ Type</td>
<td>Description</td>
</tr>
<tr>
<td>----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>A</td>
<td>Card-not-present merchants: All payment processing functions fully outsourced, no electronic cardholder data storage</td>
</tr>
<tr>
<td>A-EP</td>
<td>E-commerce merchants re-directing to a third-party website for payment processing, no electronic cardholder data storage</td>
</tr>
<tr>
<td>B</td>
<td>Merchants with only imprint machines or only standalone dial-out payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>B-IP</td>
<td>Merchants with standalone, IP-connected payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>C</td>
<td>Merchants with payment application systems connected to the Internet: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>C-VT</td>
<td>Merchants with web-based virtual payment terminals: No e-commerce or electronic cardholder data storage</td>
</tr>
<tr>
<td>D-MER</td>
<td>All other SAQ-eligible merchants</td>
</tr>
<tr>
<td>D-SP</td>
<td>SAQ-eligible service providers</td>
</tr>
<tr>
<td>P2PE</td>
<td>Hardware payment terminals in a validated PCI P2PE solution only: No e-commerce or electronic cardholder data storage</td>
</tr>
</tbody>
</table>
Choosing a platform

- Build Server + Continuous Integration
- Web Servers
- Load Balancer / Traffic Management
- Database
- Storage
- Logging
- Email
- Search Provider
- Web Jobs
Choosing a platform

- Build Server + Continuous Integration: AppVeyor
- Web Servers: Azure Web Sites
- Load Balancer / Traffic Management: Azure
- Database: Azure SQL Database
- Storage: Azure Storage
- Logging: Stackify
- Email: SparkPost
- Search Provider: Elastic Search via Compose.io
- Web Jobs: Azure Web Jobs
Why the Cloud?

• Better
• Faster
• Cheaper
• Stronger
Faster - Deployment Strategies

- Test Instances
  - Staging Slots

- Continuous Integration
  - Automated build + test (Appveyor, OctoDeploy)

- Deployment Notification
  - Slack/Chat, Email, Ticketing System
Cheaper - Costs and Scaling

- Build Server + CI: $40
- Web Server: $40 x 2
- Load Balancer / Traffic Management: Free
- Database: $15 x 2
- Storage: < $1
- Email: $15
- Logging + APM: $40 (10GB / month)
- Search Provider: $50
- Web Jobs: Free

- Total: $255.99 / month
Stronger - Reduced PCI Scope

- Shared Responsibility Model
- Decreased complexity
- Less control over security modes (This is a good thing!)

From Azure PCI DSS Responsibility Matrix 2016
Physical Security

• No access;
  Fully managed
Patch Management

• Infrastructure Patching & Configuration
  • OS, Framework, WebServer
  • Managed by Azure, secure by default

• Application Development
  • Secure SDLC

• 3rd Party Libraries
  • Package management
Network & Firewalls

• Partial Management by Azure
  • Single Endpoint

• DB Servers have firewall rules too!

• Business Justifications
Logging

- Management by Azure
  - OS, IIS, ASP.Net

- Application Level Logging
  - Stackify

- Logs are useless if you don’t watch them
  - Demo
Account Management

• Enforced by Microsoft Live + Internal Policies

Two-step verification
Your account is protected by two-step verification.
Turn off two-step verification

Help us protect your account
Because you've turned on two-step verification, we need to verify your identity. Enter the code generated by your authenticator app.

[Code]

☐ I sign in frequently on this device. Don't ask me for a code.

Submit  Cancel

If you can't use an app right now, get a code a different way.
<table>
<thead>
<tr>
<th>Goal</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network and Systems</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Protect all systems against malware and regularly update antivirus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need to know</td>
</tr>
<tr>
<td></td>
<td>8. Identify and authenticate access to system components</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
<tr>
<td>Goal</td>
<td>Requirement</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data  
2. Do not use vendor-supplied defaults for system passwords and other security parameters |
| Protect Cardholder Data                    | 3. Protect stored cardholder data                                           
4. Encrypt transmission of cardholder data across open, public networks     |
| Maintain a Vulnerability Management Program | 5. Protect all systems against malware and regularly update antivirus software or programs 
6. Develop and maintain secure systems and applications                      |
| Implement Strong Access Control Measures   | 7. Restrict access to cardholder data by business need to know               
8. Identify and authenticate access to system components                       
9. Restrict physical access to cardholder data                                  |
| Regularly Monitor and Test Networks        | 10. Track and monitor all access to network resources and cardholder data    
11. Regularly test security systems and processes                                |
| Maintain an Information Security Policy     | 12. Maintain a policy that addresses information security for all personnel  |
Difficulties – SSL and Early TLS

How can we improve Azure Web Apps (formerly Websites)?
→ Web Apps (formerly Websites)

Disable Insecure Ciphers In Azure Websites

Either through a configuration/scale option, or just blanket by default. I want to be able to disable RC4 ciphers (and any other insecure cipher suites) in Azure Websites so I can get an A rating (or better) from the Qualys SSL Labs SSL Server Test (https://www.ssllabs.com/ssltest/analyze.html).

At present, the only way to do this is not use Azure Websites and host your own VM where you can configure the registry to disable such ciphers.

274 votes
Vote

RC4 Support (2015)

Either sun set TLS 1.0 or give users the means to disable it

We chose Azure App Services to host a new web application which was scheduled to go live by the end of March, 2016. Incredibly, we are now finding that TLS 1.0 cannot be disabled on App Services. Because of that, we cannot pass a PCI DSS 3.1 scan. We’ve looked through all of the posts and replies on MS forums related to this, but there is no answer to the specific question we have. We understand that there are alternative hosting solutions like ASE and Web Roles where MS has the means to disable TLS 1.0. Both of these represent additional time and effort to setup and deploy our QA and production sites, and both represent additional compute costs for resources that we definitely don’t need (i.e., we have no worker processes and would prefer to not pay for worker instances). We also understand that PCI is requiring new applications to be DSS 3.1 compliant even though they have extended the deadline for existing applications to June, 2018.

So, the question is whether Microsoft is planning to give users the ability to disable TLS 1.0 in ordinary (i.e., non-ASE) App Services. Or, will you finally be sun setting TLS 1.0 in ordinary App Services? All of the replies referred to above were extremely vague about what exactly is on the roadmap for App Services. Could we please have a definitive answer whether we will have this ability to disable TLS 1.0 before the June, 2018 deadline? If so, we may be able to prepare a mitigation and migration plan that would grant us an exception to the DSS 3.1 compliance.

For what it’s worth, we came to Microsoft because it appeared to be the clear Paas leader. Please tell us that MS thought this through and has a cost effective Paas strategy that is consistent with the entire industry regarding secure protocols. If not, then what differentiates Azure VMs from AWS VMs?

4 votes
Vote

TLS 1.0 Support (2018)

Either sun set TLS 1.0 or give users the means to disable it

We chose Azure App Services to host a new web application which was scheduled to go live by the end of March, 2016. Incredibly, we are now finding that TLS 1.0 cannot be disabled on App Services. Because of that, we cannot pass a PCI DSS 3.1 scan. We’ve looked through all of the posts and replies on MS forums related to this, but there is no answer to the specific question we have. We understand that there are alternative hosting solutions like ASE and Web Roles where MS has the means to disable TLS 1.0. Both of these represent additional time and effort to setup and deploy our QA and production sites, and both represent additional compute costs for resources that we definitely don’t need (i.e., we have no worker processes and would prefer to not pay for worker instances). We also understand that PCI is requiring new applications to be DSS 3.1 compliant even though they have extended the deadline for existing applications to June, 2018.

So, the question is whether Microsoft is planning to give users the ability to disable TLS 1.0 in ordinary (i.e., non-ASE) App Services. Or, will you finally be sun setting TLS 1.0 in ordinary App Services? All of the replies referred to above were extremely vague about what exactly is on the roadmap for App Services. Could we please have a definitive answer whether we will have this ability to disable TLS 1.0 before the June, 2018 deadline? If so, we may be able to prepare a mitigation and migration plan that would grant us an exception to the DSS 3.1 compliance.

For what it’s worth, we came to Microsoft because it appeared to be the clear Paas leader. Please tell us that MS thought this through and has a cost effective Paas strategy that is consistent with the entire industry regarding secure protocols. If not, then what differentiates Azure VMs from AWS VMs?

Either sun set TLS 1.0 or give users the means to disable it

We chose Azure App Services to host a new web application which was scheduled to go live by the end of March, 2016. Incredibly, we are now finding that TLS 1.0 cannot be disabled on App Services. Because of that, we cannot pass a PCI DSS 3.1 scan. We’ve looked through all of the posts and replies on MS forums related to this, but there is no answer to the specific question we have. We understand that there are alternative hosting solutions like ASE and Web Roles where MS has the means to disable TLS 1.0. Both of these represent additional time and effort to setup and deploy our QA and production sites, and both represent additional compute costs for resources that we definitely don’t need (i.e., we have no worker processes and would prefer to not pay for worker instances). We also understand that PCI is requiring new applications to be DSS 3.1 compliant even though they have extended the deadline for existing applications to June, 2018.

So, the question is whether Microsoft is planning to give users the ability to disable TLS 1.0 in ordinary (i.e., non-ASE) App Services. Or, will you finally be sun setting TLS 1.0 in ordinary App Services? All of the replies referred to above were extremely vague about what exactly is on the roadmap for App Services. Could we please have a definitive answer whether we will have this ability to disable TLS 1.0 before the June, 2018 deadline? If so, we may be able to prepare a mitigation and migration plan that would grant us an exception to the DSS 3.1 compliance.

For what it’s worth, we came to Microsoft because it appeared to be the clear Paas leader. Please tell us that MS thought this through and has a cost effective Paas strategy that is consistent with the entire industry regarding secure protocols. If not, then what differentiates Azure VMs from AWS VMs?
Difficulties - Network Scanning

- Uncontrolled Ports & Services
  - 454/455/1001: Internal Web Service Apps
Difficulties - Penetration Test

- Advanced Notice Required
  - Disruptive to Cloud Platform

- Unknown protective measures, responses, reactions

- Black Box by default
Difficulties – Understanding the Cloud

- Auditor didn’t understand our infrastructure

Results

• Passed our Audit!

• Started our SAQ-A-EP last week
Results

• 746 unique funds

• 5000+ gifts, 173 recurring
  • Recurring is a new feature

• $1,495,055.41 raised
  • 20% increase over previous year
Reference

• PCI FAQs:

• Microsoft Trust Center
  – https://www.microsoft.com/en-us/TrustCenter/Compliance/PCI
  – Azure PCI DSS Responsibility Matrix 2016

• Amazon Web Services (AWS) Cloud Security

• Azure UserVoice