PCI-DSS Q&A LOL

Daniel Adinolfi
Senior Security Engineer, IT Security Office
Cornell University

Agenda

- What is PCI-DSS?
- Who Needs to Care?
- Scoping and You.
- Solutions.
- The DSS is neither secure nor a standard. Discuss.

What is the PCI-DSS?

- http://www.pcisecuritystandards.org/
- 12 Major Requirments
- Few hundred sub-requirements
- Technical, Procedural, Policy-oriented
- Firewalls, IDS, Application Firewalls, password strength, encryption, etc.

Who Needs to Care?

- Business Offices
- Treasury
- Audit
- Anyone taking credit cards!
  - Professors, summer camps, development/ alumni affairs

Scoping and You

- Anything that is involved in credit card transactions is in scope.
- Anything that stores credit card data is in scope.
- Any network on which in-scope systems reside is in scope.
- Any host on the same network as in-scope hosts is in scope.

Scoping and You, continued

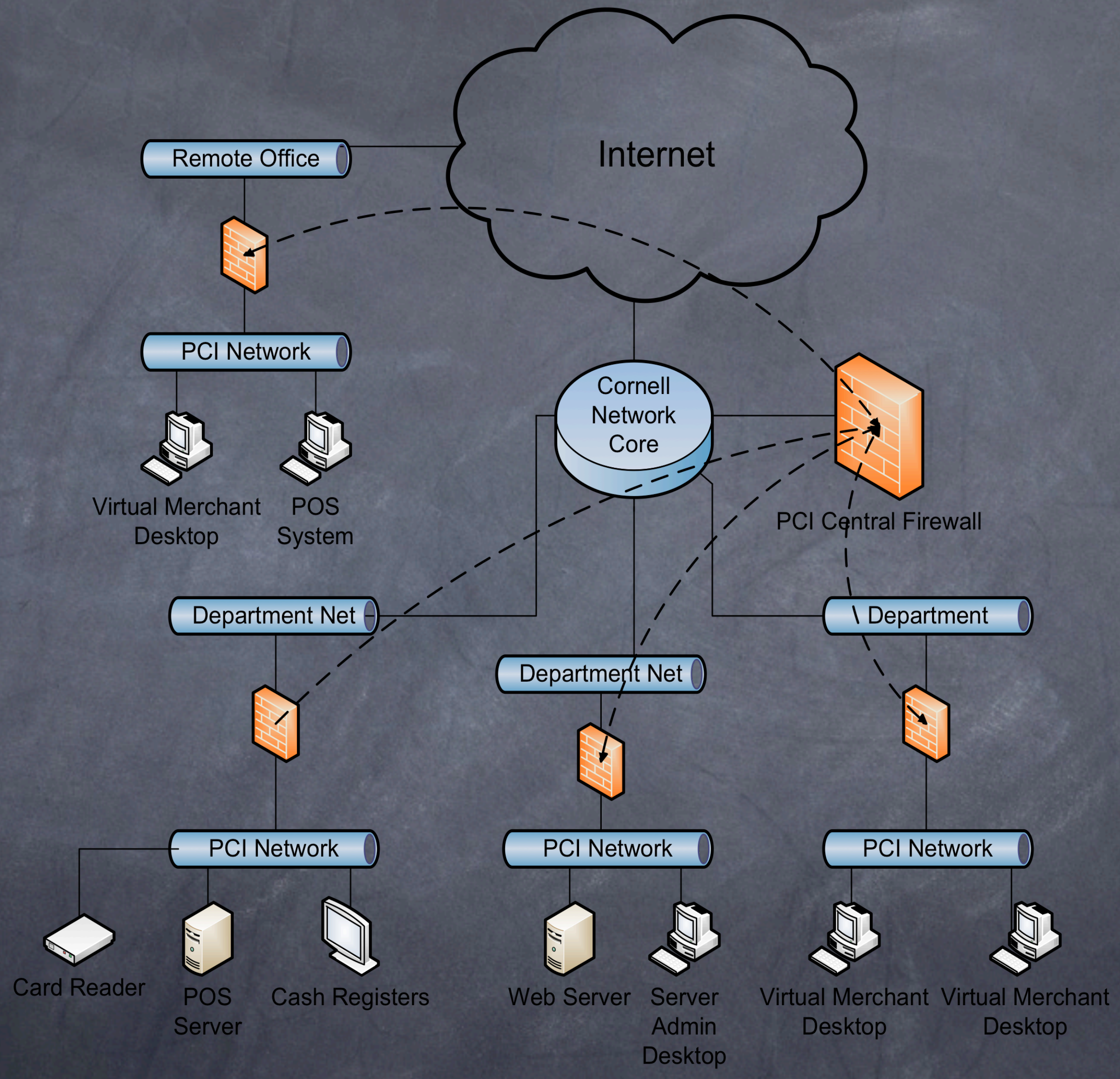
- Partitioning is key!

Scoping and You, continued

- Tricky, tricky
  - Web server hosting a shopping cart that takes credit card payments
  - Web server with PayFlow Link
  - Desktop visiting a web server.
  - Kiosk in the Library

Solutions

- Partition, partition, partition.
- Use card readers on telephone lines.
- Avoid credit card payments when possible.
- Limit who can take credit cards.
- Outsource!
- Audit like crazy and be hard-nosed.


Internet
Remote Office
PCI Network
Virtual Merchant Desktop
POS System
Cornell Network Core
PCI Central Firewall
Department Net
Department Net
\ Department
PCI Network
PCI Network
PCI Network
Card Reader
POS Server
Cash Registers
Web Server
Server Admin Desktop
Virtual Merchant Desktop
Virtual Merchant Desktop

Discuss

- What have other schools done?
- What are you planning?
- Questions? Opinions?

Thank You!

- dra1@cornell.edu
- http://www.pcisecuritystandards.org/