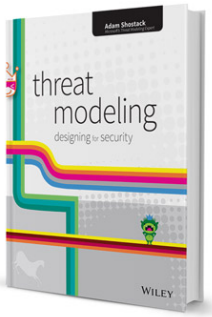
black hat ASIA 2021
May 6-7, 2021
BRIEFINGS

Reverse Engineering Compliance

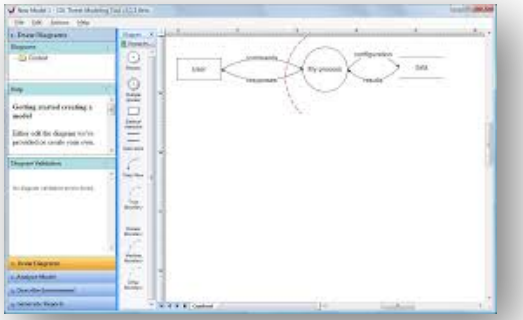
Adam Shostack

About Adam Shostack



Shostack & ASSOCIATES
https://associates.shostack.org

IriusRisk

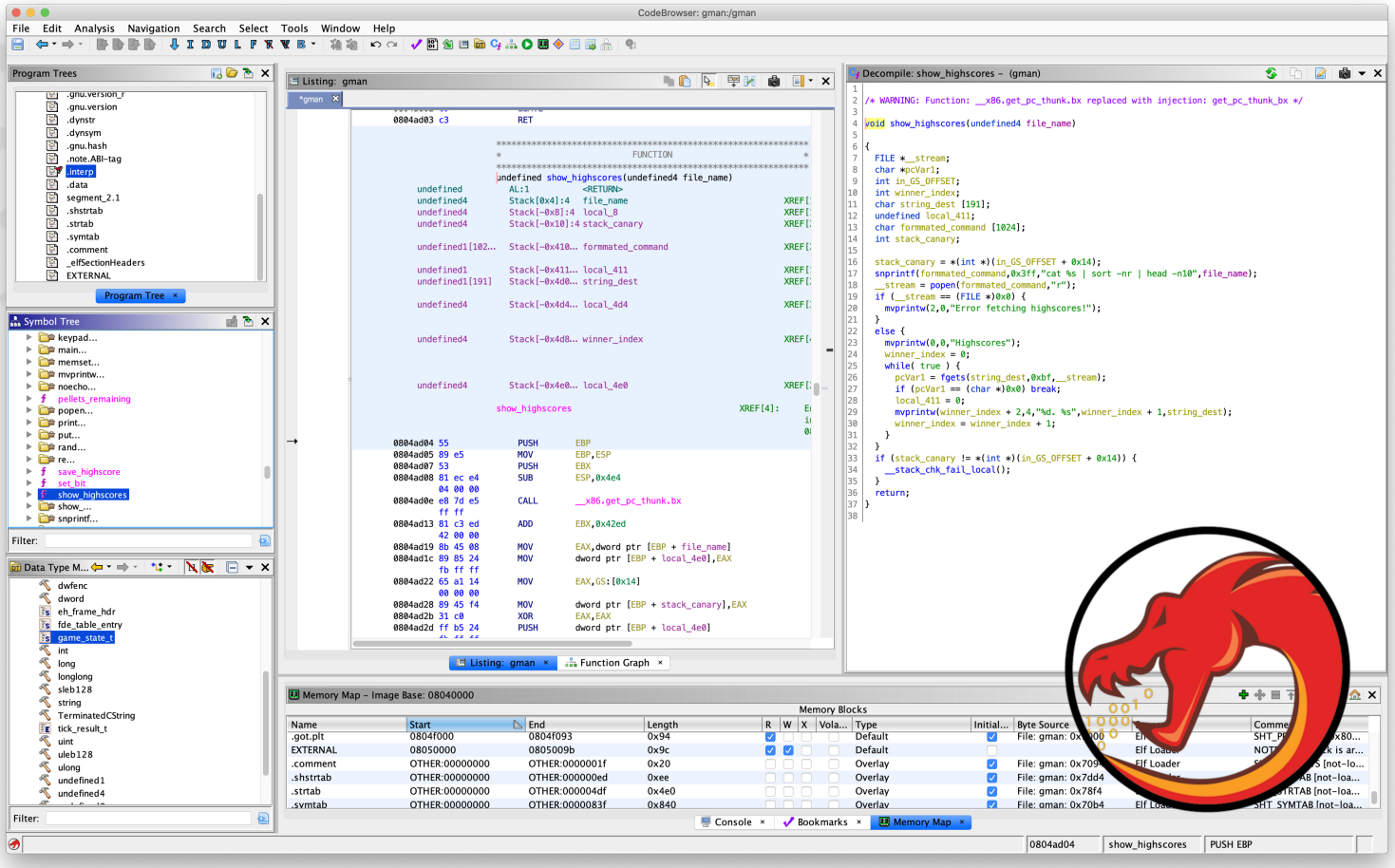


Agenda

- Reverse engineering
- Compliance systems & threat modeling
- Reverse engineering PCI
- Why bother? 🤷‍♀️

Reverse engineering

Reverse engineering tools



Reverse engineering is more than tools

- A way of thinking
  - What does this do?
  - Why does it work that way?
  - How can I change it?
- Treating RE as toolsets is like treating pen testing as Kali

Reverse engineering is powerful

- Thought process applies broadly

Compliance systems

Rulebooks

- Thou shalt!
- Imposed by contract or regulation
- But…why those things?

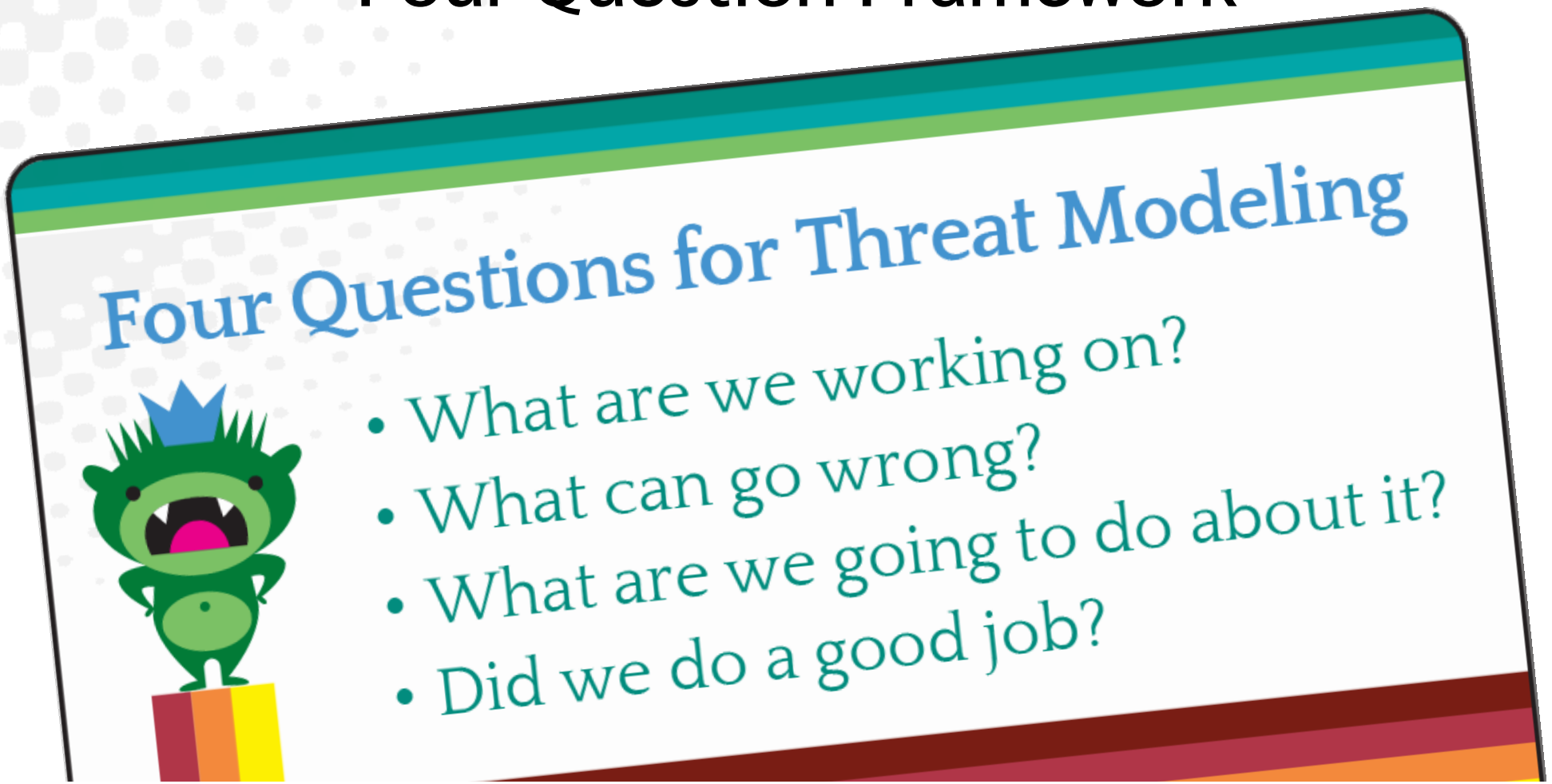
Behind every powerful rulebook

- There’s a committee
- With an implicit threat model
- Which they hide 🤯

What's an implicit threat model?

- Threat modeling is ways of thinking about a system …
  - "What's your threat model?"
  - "Let's threat model this"
- Ways of documenting that work
- All of the above!

Four Question Framework



STRIDE Mnemonic

- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privileges

...Helps us structure how we address “what can go wrong”

Reverse engineering PCI

Context

- “PCI” : Payment Card Industry Data Security Standard 3.2.1
- They have a hard job and I don’t mean to pick on them
- Standard is easily available, familiar

PCI Overview (from the standard)

PCI Data Security Standard – High Level Overview

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 anti-virus 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

PCI overview (2)

- 139 pages
- Frequent source of arguments
  - Security team vs the rest of the business
  - Everyone vs the QSA

Randomly chosen page of PCI

PCI DSS Requirements	Testing Procedures	Guidance
1.1.5 Description of groups, roles, and responsibilities for management of network components	**1.1.5.a** Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components.	This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.
	1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**1.1.6.a** Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification and approval for each.	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed. Approvals should be granted by personnel independent of the personnel managing the configuration.
	1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service.	
	1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	

We need to talk about the whys

- “Why” motivates the business to move past the checkbox
- “Why” enables innovation by engineers
- “Why” can inform conversation with assessors

- PCI’s Guidance (3rd column) can head that way

Let’s reverse engineer that! (1)

- Why, why, why?
- I expected to go right to the threats
- The answers didn’t make any sense!
  - What does 1.1.15 even mean?
  - (“1.1.5 Description of groups, roles, and responsibilities for management of network components…”)
  - Where’s the problem?
  - It’s not a characteristic of the firewall…

Let’s try again…

- Why can’t we understand what’s going on?

Four Question Framework

- Four Questions as north stars
- Tied to the reverse engineering viewpoint: why is it that way?

Let’s reverse engineer PCI! (2)

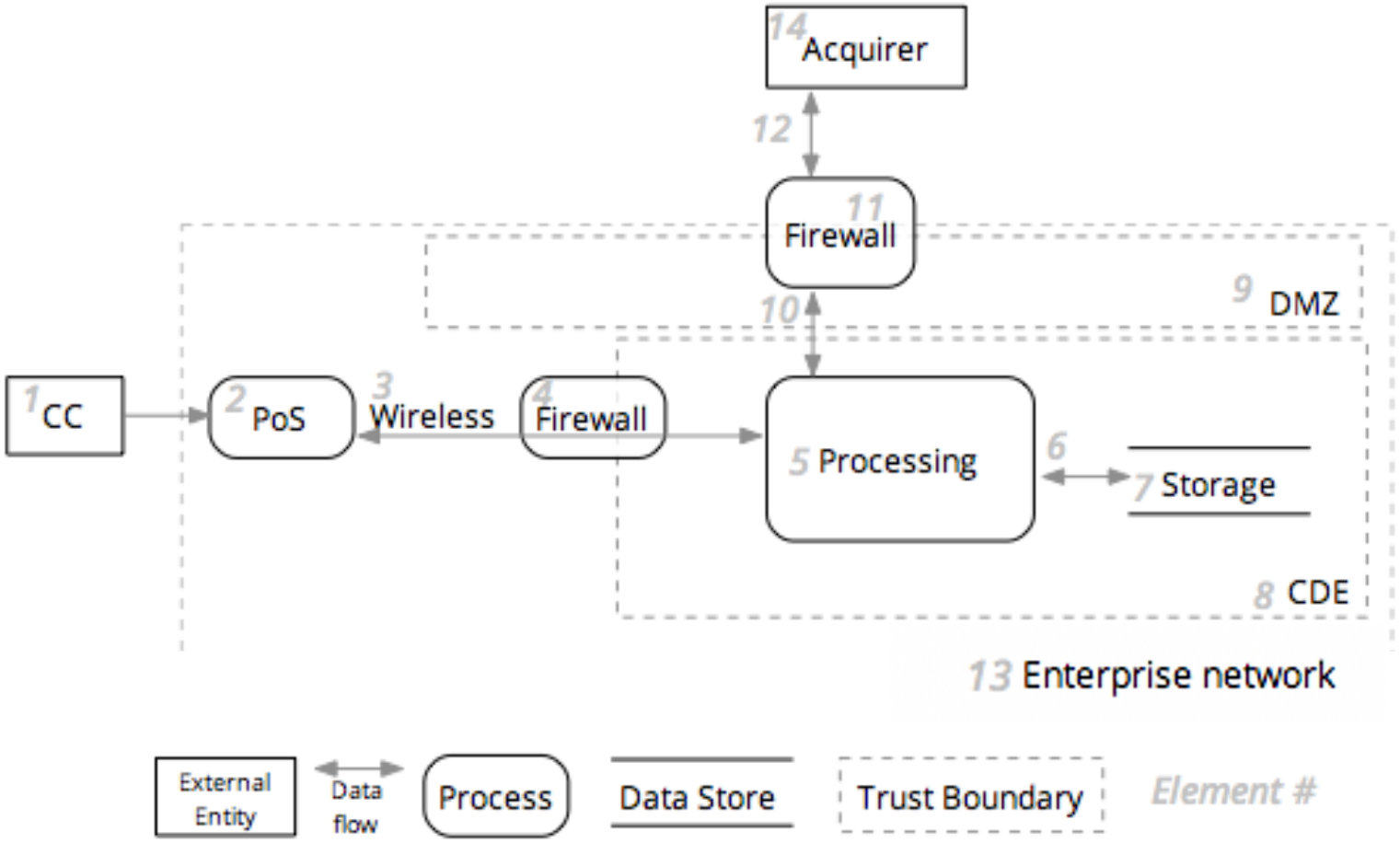
- PCI has two distinct system models!
  - Process, technology, ~~people~~
- 1.1.5 is almost all about process, not the computers
  - (“1.1.5 Description of groups, roles, and responsibilities for management of network components…”)

The boring bits

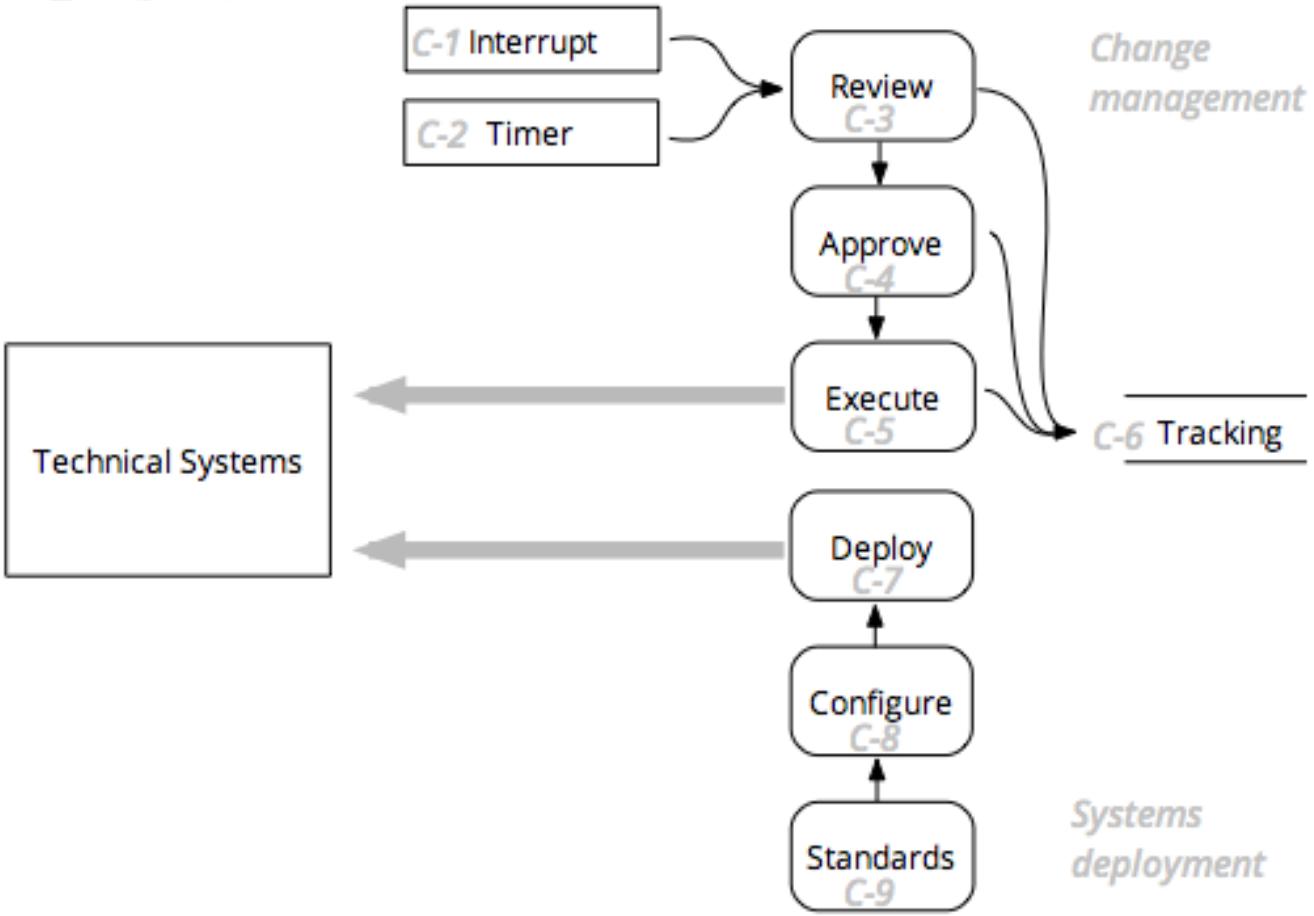
- Going through each line in PCI takes time…a lot of time
- Iterate between controls and threats and system models

- And the results
  - Next slides and
  - https://associates.shostack.org/whitepapers/

PCI's model of technology*



PCI's model of process



PCI’s model of threats

- Prevent, detect, respond [P], [D], [R]
- Information disclosure, comply, manage [I], [C], [M]

Threats to processes

Element	Threat/Problem/Vulnerability/Notes	PCI Requirement/ Test Process
C-1 Interrupt	Firewall rulesets go out of date [M]	1.1.7
C-2 Timer	Old data not deleted/not deleted securely	3.1* bullet 2
	Old data not deleted/not deleted securely	3.1* bullet 4
	Malware might be published for new systems	5.1.2
	Anti-malware sw goes out of date	5.2
C-3 Review		1.1
C-4 Approval		
	Firewall config fails to prevent [C]	1.1.1.a
	Anti-virus fails to protect [P, D, R]	5.1.1
C-5 Execution		
C-6 Tracking & documentation		
	Approval process failures (network connections) [M]	1.1.1.b
	Approval process failures (firewall) [M]	1.1.1.c

Threats to technology

Element	Threat/Vulnerability/Problem/Notes	PCI Requirement
1 Credit Card		
2 Point of Sale		
3 Wireless network & data flows	Eavesdropping [P, I]	4.1*
4 Wireless firewall	[P]	1.2, 1.2.1, 1.2.3,
5 Processing	Full PAN displayed [I]	3.3
6 Processing to storage (Data flows)		
7 Storage	Authentication data stored [I]	3.2
	Full track data stored [I]	3.2.1
	Card verification code/values stored [i]	3.2.2
	PIN block/encrypted PIN block stored [i]	3.2.3
	PAN disclosed [i]	3.4
	Account access allows file access [i]	3.4.1
	Crypto keys stored securely [I, 2nd order]	3.6.3
8 Card Data Environment		
9 DMZ		

The last five slides are my RE analysis

- Why?
  - Because PCI doesn't share them
  - I had to do a lot of (painful) work
- RE turns out to be super-helpful in understanding PCI
  - Both the work & the deliverable help

Why bother?

Reverse engineering for fun and profit

- Increase your understanding
- Show gaps in the rules, expose places defenders ignore
- It may not reduce conflict with auditors in the short term
  - But that's never a goal of reverse engineering all the things. ☺️

Threat model your systems

- Threat modeling acts as a language across teams
  - Four Question Framework
- Compliance requirements make more sense with TMs
  - They're answers to 'what are we going to do'

Time to show your threat model

- Why should every organization do this analysis? 🤔
- Demand standards bodies show their threat models
- Improve standards
  - When their models don’t represent your systems
  - Either the requirements or controls are adjusted or invalidated
- Complexity includes
  - Gaming the standard
  - Cost of assessment may shift

Thank you

adam@shostack.org

Resources