WELCOME TO

THE BLAME GAME

WHAT I WANT TO COVER

- Our world and a brief history of security standards in our industry
- "Shit Auditors Said"
- Current state of affairs
- "Shit Auditors Still Say"
- Our approach and toolbox
- Tips, tricks and what little advice we have

WHY AM I HERE?

- Used FreeBSD since ~2000
- Love open source
- Been working in the payment industry since 2003
    - Gone from wild west to "Westworld"

- Have talked about this for years, but mostly over beer and probably to people who couldn't care less..

WHY ARE _WE_ HERE?

- Hosting in-house-developed SW on FreeBSD since 2003
- Authenticating users during on-line card payments
- SW for card issuers (your bank), merchants and processors (Amazon, PayPal) and card companies (that other logo on your card)
- Protocol is called 3-D Secure - "Three Domain Security"

THE 3-D SECURE PROTOCOL

- Lets banks intercept the payment process to authenticate
- Sold as a benefit to you, but really is about their risk
- Merchants given a "free ride" - moves liability to the banks
- Banks choose their own authentication methods
- Risk-based authentication helps reduce nuisance factor

HELPING PEOPLE SPEND MONEY THEY DON'T HAVE ...SAFELY

Unnamed Modirum manager, long ago

THE WORLD WE LIVE IN

- Three players
  - Those writing the requirements
  - Those covering their asses
  - Those who are blamed in the end
- Several sets of requirements
  - PCI DSS and 3DS
  - Payment systems (Visa, MC, etc.)
  - Legal (PSD2, GDPR, local law, etc.)
  - Customer specific

EARLY '00 – THE WILD WEST

- No relevant security requirements were being enforced
- Everyone did their own thing
- Massive fallout, lots of fraud
- Server under the desk
- Receipts with full card data
- What is this "crypto" you are talking about?

THE REQUIREMENTS ARE-A-COMING!

- 2004 - PCI DSS
  - Immature, copy-paste job, incoherent and inflexible
  - "Qualified" auditors popping up everywhere
  - Terrible.
- Visa 3-D Secure security requirements
  - Mostly key management and physical security
  - Not entirely terrible....
    - ...but subsequent revisions turned u-g-l-y!

ABSURDITIES

- Looking for data that cannot exist
- Photos of password files
- "Please document that grep(1) supports regular expressions"
- "Please take this alpha-version binary blob and run it on your system"
- Two employees, single office, still need visitor badge system
- Auditor storing evidence collected from clients on Desktop (WinXP)
  - ..also used for adult entertainment..

THE LOW POINT

Modirum

WE ARE NOT IN THE BUSINESS OF LEVEL PLAYING FIELDS

Auditing authority, April 2014

SOME GROW UP, OTHERS GROW OLD

- PCI DSS becomes more flexible
  - Focusing more on the problem than the solution
  - Less tied to specific platforms (but their password policies still suck)
- Visa req's become more absurd
  - Logically impossible
  - Actively reduces security

ABSURDITIES

- "root account must have a strong password under split knowledge and dual control"
  - No, disabling your root account won't do.
- "You must treat OTPs exactly the same as static passwords"
  - Encrypt them using HSMs
  - Recipient must carry a HSM
- Talking TLS to SMS gateways, etc:
  - "If the server decides on the crypto, can't you be the server and they be the client?"

SANITY ON THE HORIZON?

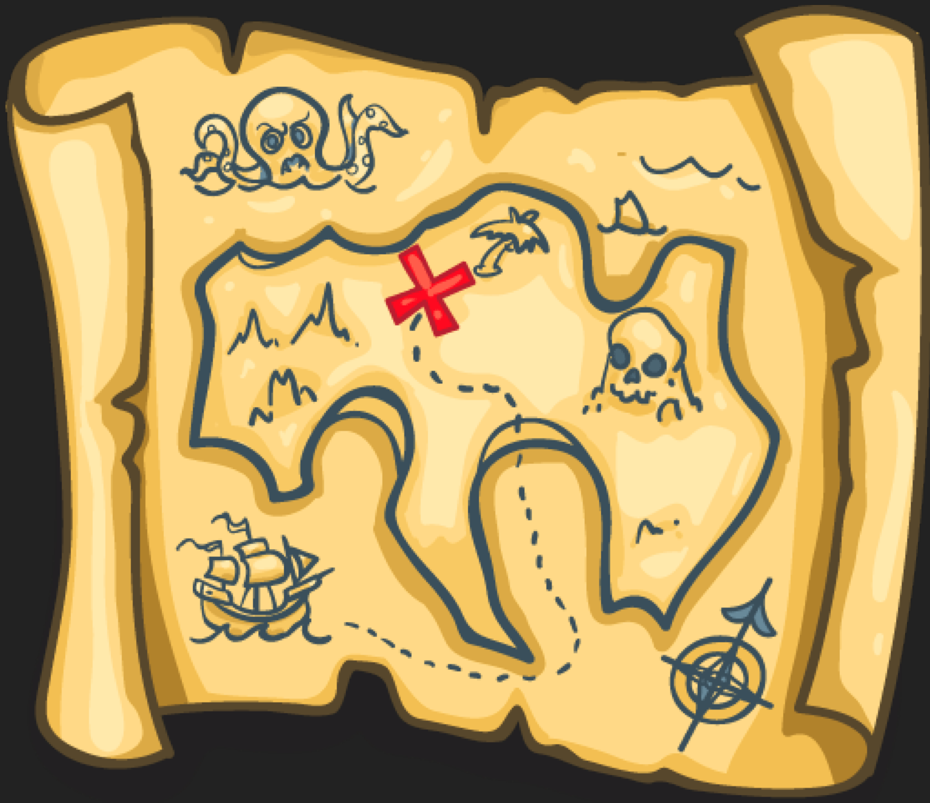
- 2018 - Visa requirements are no more
- PCI DSS has a new friend - the PCI 3DS
- GDPR and PSD2 helps guide the requirements

BUT…

- Many clueless or downright cheating auditors
- Payment systems still meddle
- Still many homegrown requirements

ABSURDITIES

- "Please specify the type of street lighting outside your premises"
- "How often does police patrol the area"
- "Do you have a priority phone number for the emergency services in your area"
- "Your data is worth one impossibillion dollars", says a document the auditor carries in his laptop case



OUR APPROACH

- Always think security first, not compliance
- Trust no-one, not even yourself
- Know why you do what you do
  - **..and be prepared to prove it's deliberate**
- Detection is more important than prevention
  - Go for both, but spend your efforts wisely
- Dual (physical) control is king!

OUR TOOLBOX

- Kernel auditing and bsmtrace
  Audit log for forensics, real-time intrusion detection
- freebsd-update and pkg
  File integrity monitoring
- nginx+modsecurity
  Web Application Firewall
- MySQL/Galera
  Auditing of access to data
- pfSense and Suricata
  Firewall and network IDS
- Puppet
  Configuration, change management
- ZFS
  Immutable backups, rollback
- poudriere
  Package building and signing
- /bin/sh
  Tying it all together

KERNEL AUDITING

- audit(4): Captures system calls as events (BSM standard)
- Huge amounts of data - be selective of what you collect
- Ship the data elsewhere for forensics
- bsmtrace(1): Stateful inspection of events from the audit pipe, can fire alerts
  - e.g. "www user just forked a process" (should never happen - it's the JVM!)

WHY IS THIS HARD?

- Incompatible philosophies
- Expectations of a large organisation
- Not open source friendly
  - Proprietary hardware, no drivers, etc.
- Compliant != secure, secure != compliant
- **Interpretation is everything!**
  - Choose your auditor wisely (if you can)

HOW TO CHOOSE YOUR AUDITOR

- Auditing _is_ technical, your auditor _must_ know more than the requirements and buzzwords
- How do they handle alternative solutions?
- Will they work with you to find solutions?
- Do they trust their own judgement?
- If warned about an auditor, listen
    - If recommended an auditor, listen even more
- Remember: You are the client, you're paying the bill.

...BUT WHAT IF YOU CAN'T?

- Explain your platform and key concepts early
- Be prepared to use generic terminology
  - VM instead of jail, Unix (or Linux) instead of BSD
- Map their requirements back to the PCI DSS
  - Most requirements come from the same place
  - PCI is generally recognised (but not always)

COMPLAINTS AND WHINES

- Kernel auditing feels half-baked
  - Missing good examples and documentation
  - Does anyone actually use this stuff? (Call me!)
  - And seriously, no jail ID in audit records?!?
- Packaged base - pretty please?
  (Yes, I know, nearly there now..)
- Jail orchestration

THANK YOU ALL!

- Contributors of all kinds
- Organisers of this event
- Everyone working to make the community tick
- My esteemed colleagues
- Tommi Pernilä from Nixu

So long, and thanks for all the fi^H^Hbeer!

.....questions?