MANTOR ORGANIZATION

Grow on secure grounds

Broken by Design

- The need for some better foundation

- Security by Isolation
- Trusted Computing
- Security Processes

Danny Fullerton
CISSP GCIH GHTQ
dfullerton@mantor.org

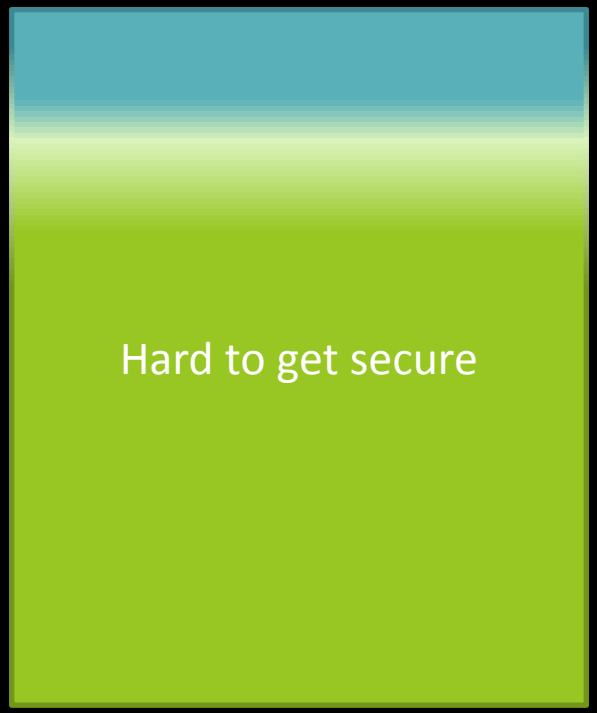
2010-08-10

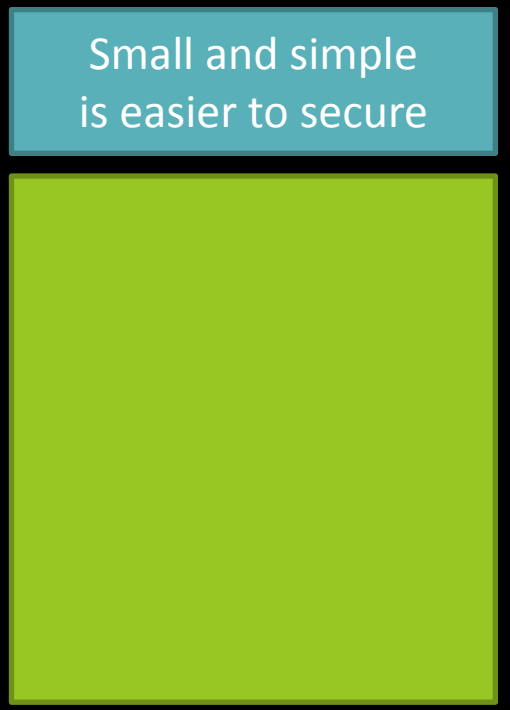
Platform/OS Design

Current State

Security by Isolation / Security by Correctness – Concept

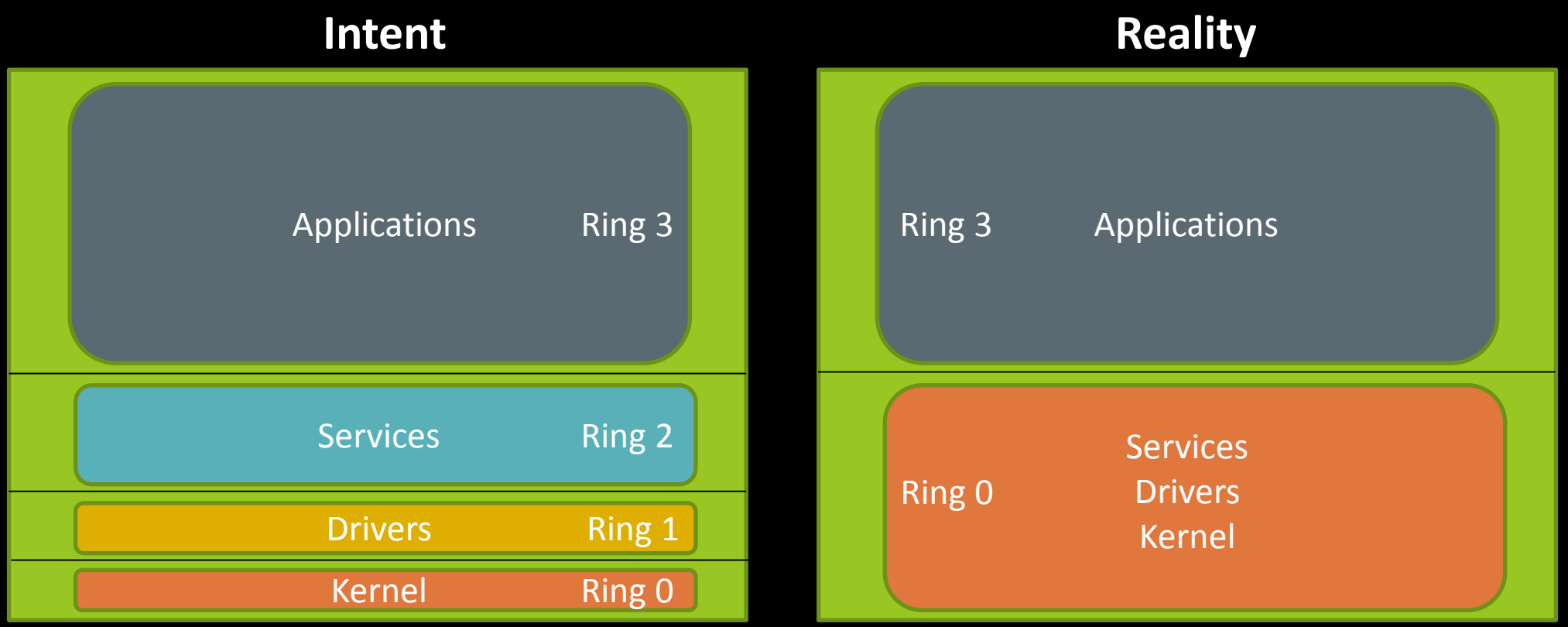
- Security by Isolation
  - Isolate different environments from each other
- Security by Correctness
  - Perfectly secure code





Platform/OS Design – Searching for isolation

- Anyone using Ring 1 and Ring 2?
- No! We all love chubby kernels.



Platform/OS Design – Searching for isolation

- Servers
  - Different process / different user / chroot / jail
  - But still not by default and still overlook
- Desktops
  - Admin vs User
  - All software we execute run under our authority
  - Why do my mp3 player has access to my financial reports?

Platform/OS Design – searching for isolation

- Firewire / PCMCIA / PCI
  - DMA access
  - What does this mean?
  - Complete memory access

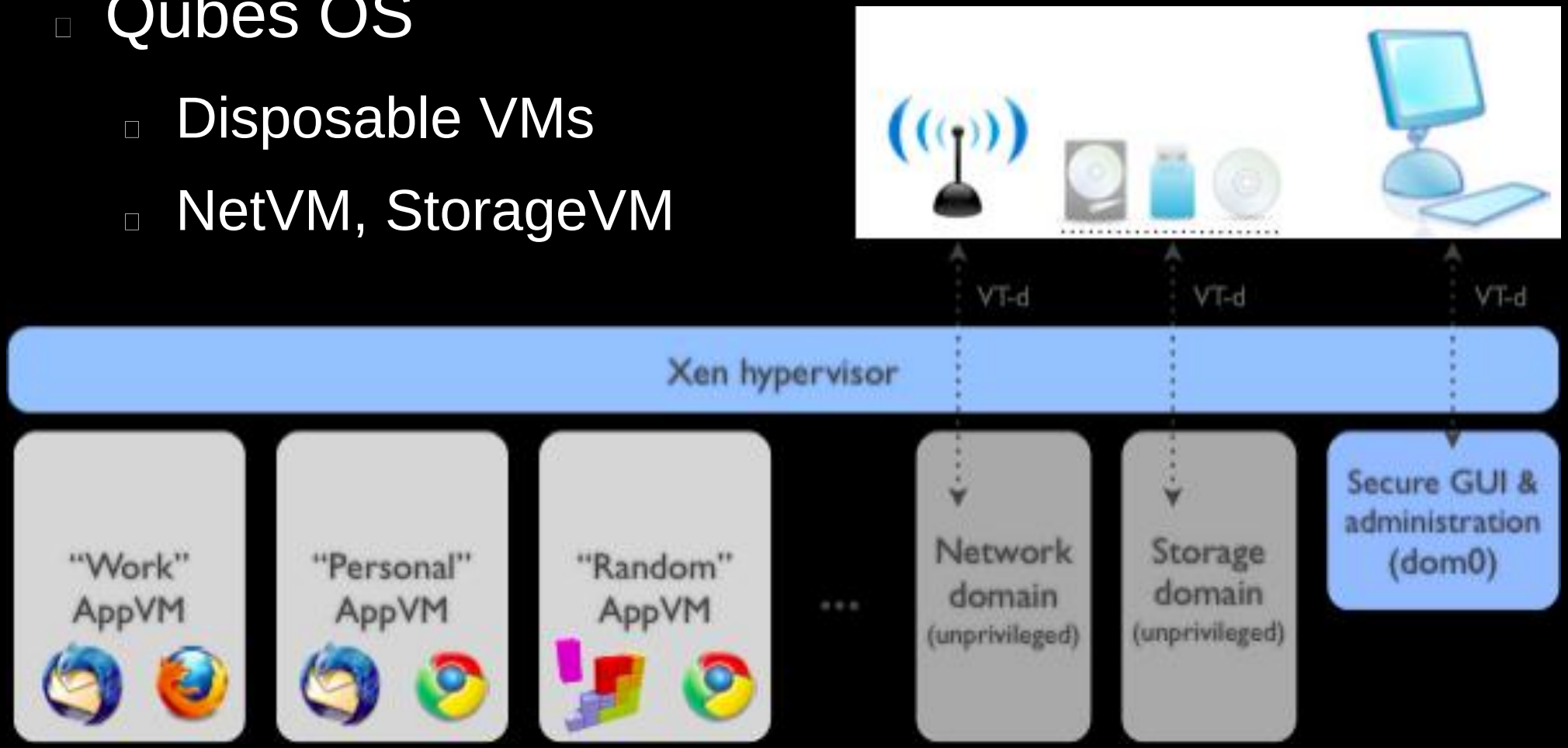
- Why does my network card has complete memory access?

Platform/OS Design

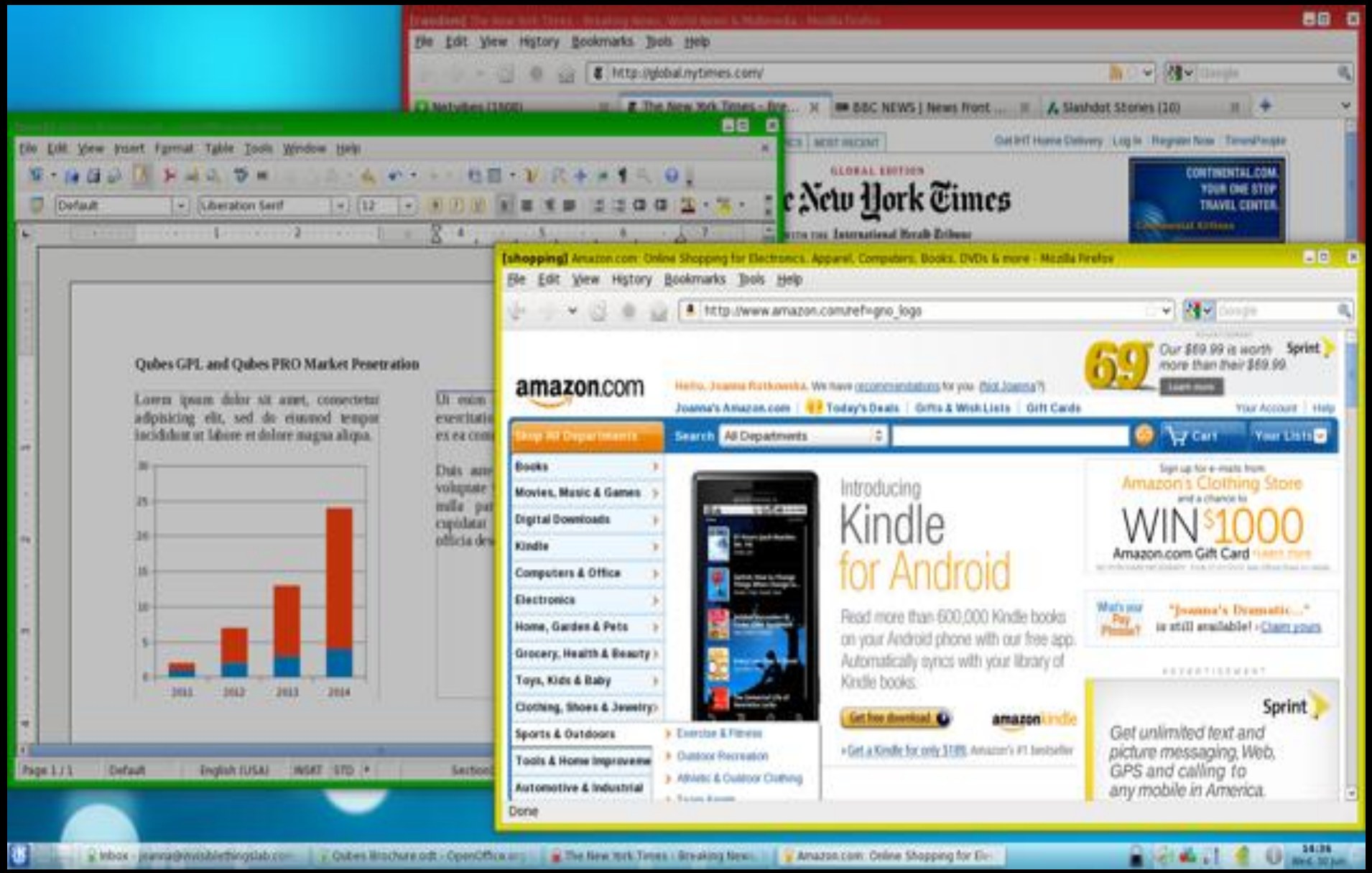
Broken by Design!

Security by Isolation– Qubes OS

- Virtual Machine Monitor / Hypervisor
  - Virtual Machine
- Qubes OS
  - Disposable VMs
  - NetVM, StorageVM



Security by Isolation– Qubes-OS



Trusted Computing – Very brief overview

- Trusted eXecution Technology (TXT)
  - Trusted Platform Module (TPM)
  - Can fix the DMA problem
- Protection
  - Software based attack
  - Unsophisticated local hardware attack
  - Protect user's data from outsiders
    - Sealed storage
  - Attestation

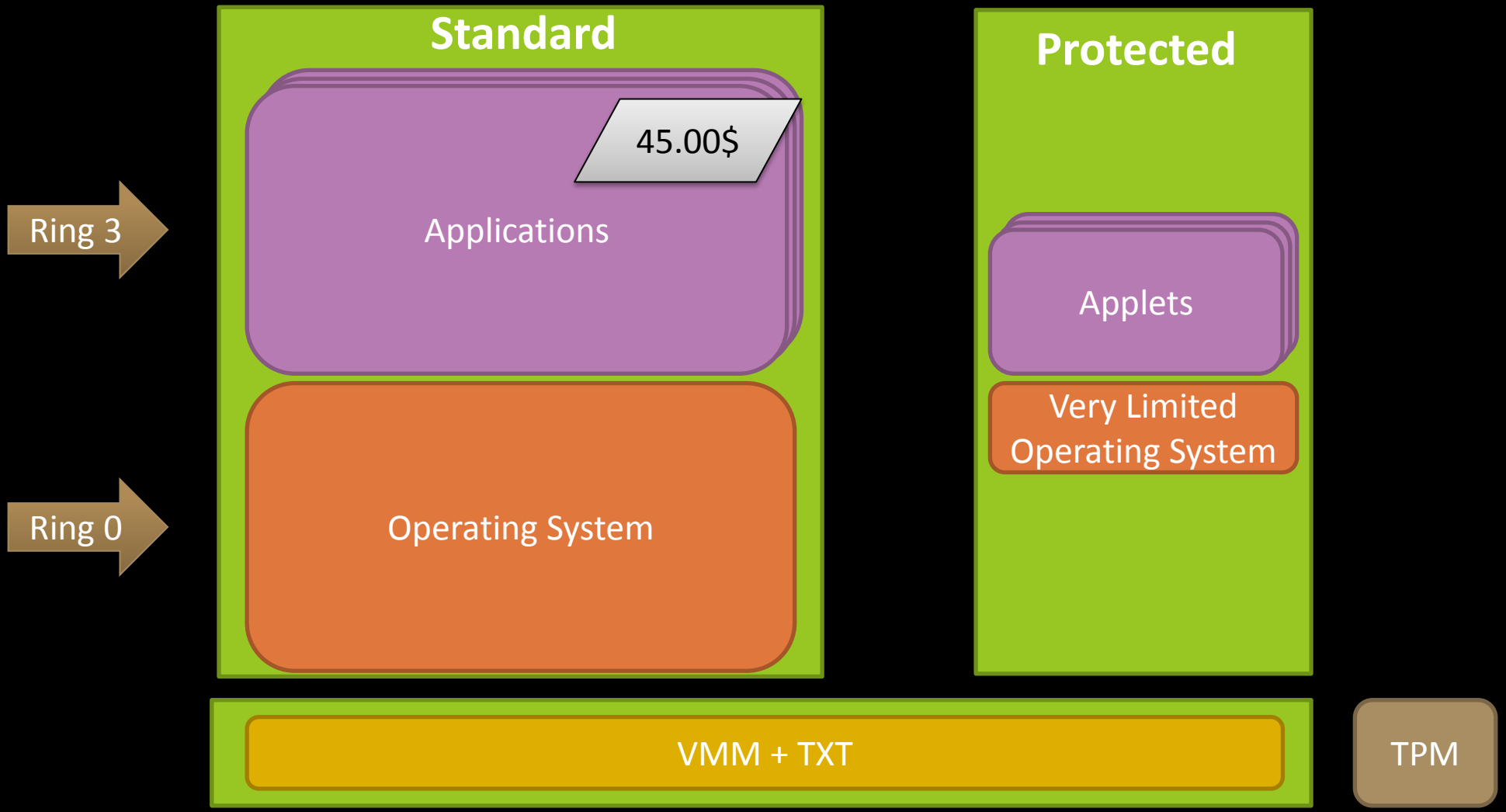
Trusted Computing – Quick Example

- How would we secure a 45$ Ebay transaction?

- What if we could use a trusted environment to confirm the transactions?
  - Secure code: small and simple to verify
  - Trusted by both parties (Ebay and You)
  - External entities must not be able to interfere

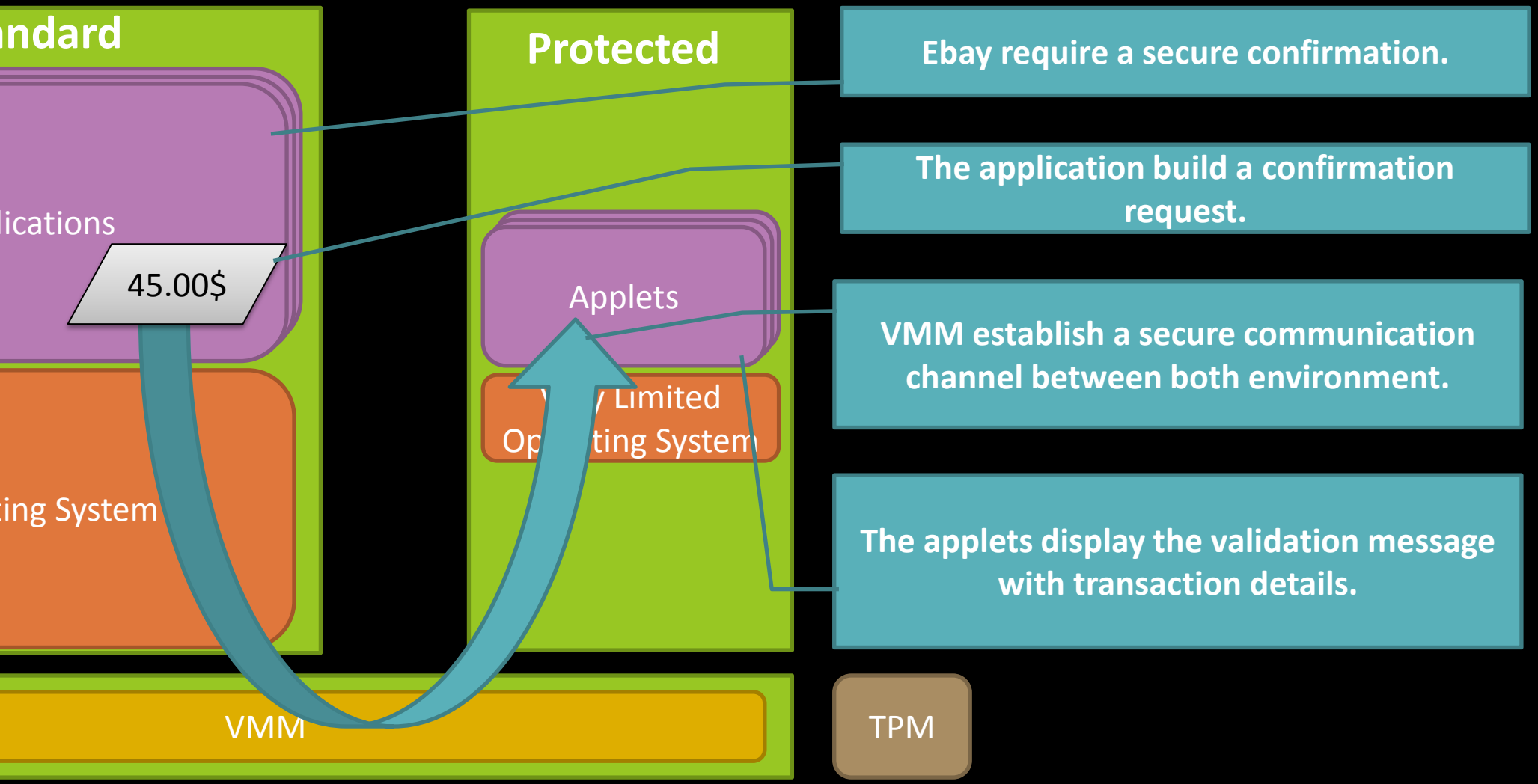
Trusted Computing – Quick Example

- The architecture



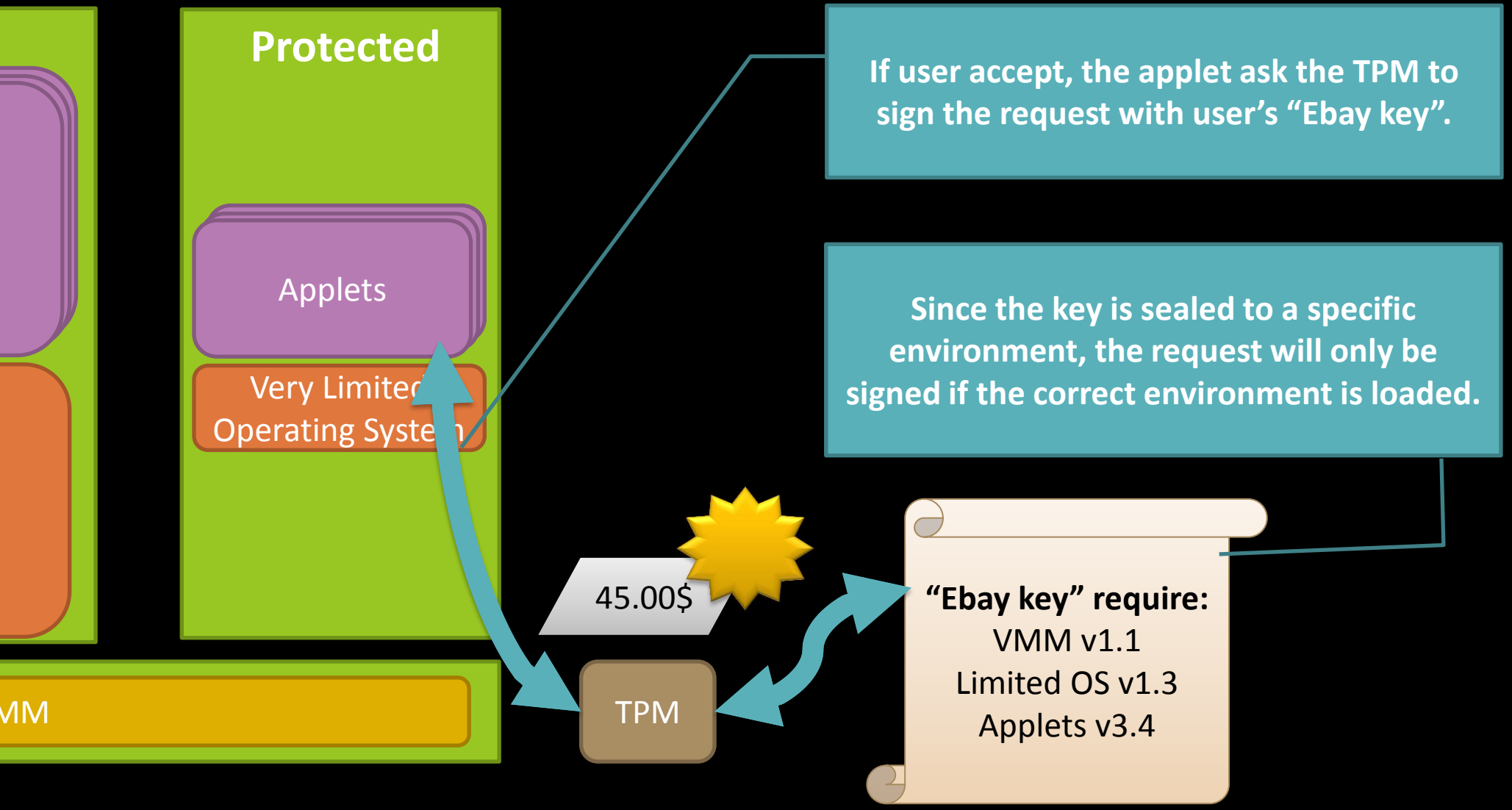
Trusted Computing – Quick Example

Validation 1/2



Trusted Computing – Quick Example

Validation 2/2



Security Processes

Current State

Security Processes – How?

- Industry Security Standard are audit oriented
  - ISO/NIST/etc don't define how to implement security!
- Security is not implemented as it should
- Almost no metrics
  - Hard to identify our success/failure
  - Hard to get better
  - Hard to justify
  - Inconsistent security measure

Security Processes – How to evaluate 3rd parties?

Any hesitation?

- External development team
- External business solution
- Cloud computing

Security Processes

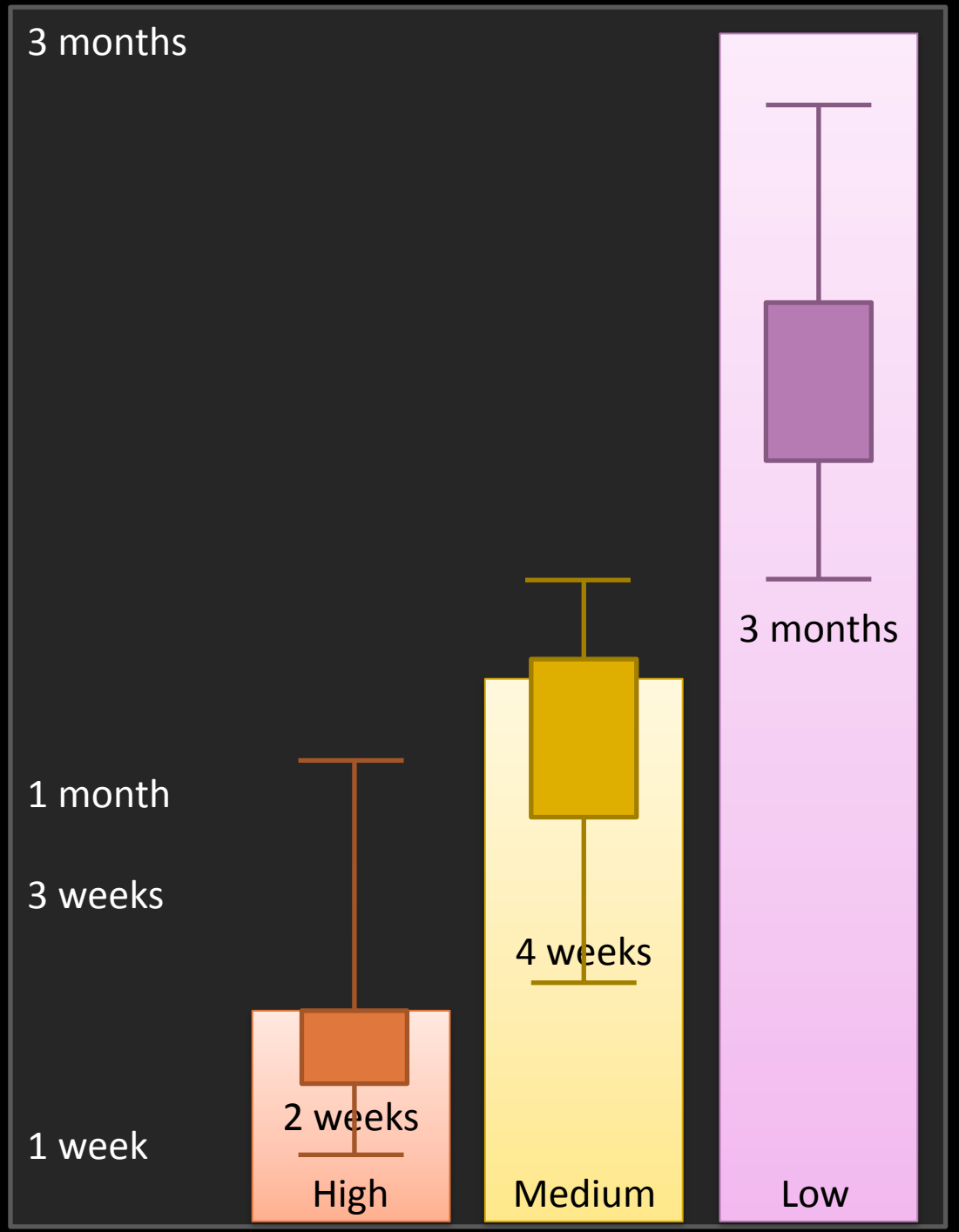
Broken by Design!

Security Processes – Live Security Standard

- Test-Driven Development
- Policy enforcement
- Metrics

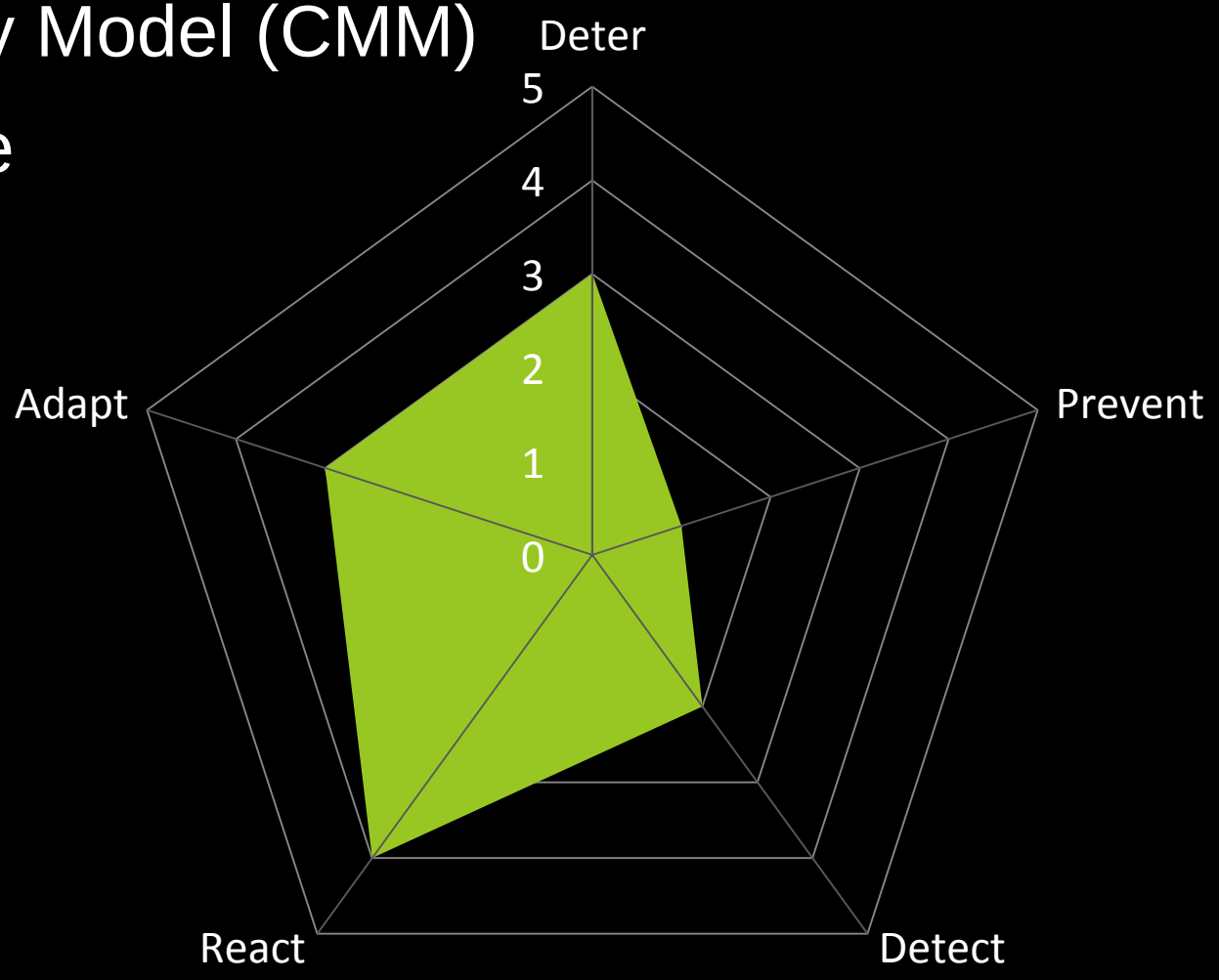
Security Processes

- Vulnerability Scan
- Patch Management
- Issue Management
- SDLC Enforcement



Security Processes – Live Security Standard

- Security Postures
  - Capability Maturity Model (CMM)
  - Process Coverage
  - Domain Coverage
  - Automation Level



Use case – Mantor's dnssec

- DNS -> Domain Name System
  - google.com -> 67.68.33.234
  - Federated
  - Highly Redundant
- DNSSEC
  - DNS + Integrity
  - Can be used to distribute Public keys
    - Servers and Clients Authentication
    - Establish Secure Channels (HTTPS, Emails, etc)
  - Death of PKI/SSL/TLS/PGP ???

The END

Security by Design

Links

- Mantor: www.mantor.org
- Blog: blog.mantor.org
- OpenSec: dev.mantor.org/opensec
- Qubes OS: www.qubes-os.org
- Trusted Computing: www.trustedcomputinggroup.org
- TrouSerS: trousers.sourceforge.net
- Bsssd: bsssd.sourceforge.net
- Firewire attack: www.hermann-uwe.de/blog/physical-memory-attacks-via-firewire-dma-part-1-overview-and-mitigation