RSA®CONFERENCE2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Oh the PaaSabilities

SESSION ID: CSV-R01

David Mortman

Chief Security Architect
Dell
@mortman

Why PaaS?

- **Fast easy deployment**
  - **Drop The Code And Go**
  - **ZOMG Separation of Duties!$&(!!)!$ (also see DevOps)**
  - **Automation FTW**

Why PaaS?

- Consistent deployment
  - From Dev to Test to Prod
  - Who doesn’t like this?
  - Huge security and operations benefits

Why PaaS?

- Hides the complexity
  - From Ops
  - From Dev
  - Freaks out the Security Folks

Why Not PaaS?

- **Policy Concerns**
  - **Especially in Public PaaS**
  - **Compliance**
  - **Regulatory**
  - **Legal**
  - **Privacy**
  - **Auditors don’t understand**
  - **Incident Response**

Oh The PaaSabilities: Product Dev → Ops

Oh The PaaSabilities: Product Dev

- Containers
  - LXC
  - Warden
  - Docker
- Whitelisting
- Blacklisting

Oh The PaaSabilities: Ops → Security

Oh The PaaSabilities: Security

- 3rd Party Security Tools?
  - What tools?
  - Especially in Public PaaS
- Crypto behind the webserver?
- Encrypted File Systems?
- Logging/Auditing
- Compliance?!!?!?

Oh The PaaSabilities: Security→ App Dev

Oh The PaaSabilities: App Dev

- Secure Coding
  - JAVA -- FindBugs, Checkstyle and PMD
  - Ruby – Saikuro, Roodi, Dust and Flog
  - Write your own unit tests
  - Jenkins
  - https://buildsecurityin.us-cert.gov/bsi/home.html
  - Threat modeling

Speaking of Threat Modeling

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

Speaking of Threat Modeling

- Elevation of Privilege
  - Gamification of Security
  - Help communicate about security design in applications
  - Analyze designs for potential security issues
  - Suggest and manage mitigations
  - Creative Commons

Speaking of Threat Modeling

- Elevation of Privilege
  - Adam Shostack
  - http://www.microsoft.com/security/sdl/adopt/eop.aspx

Elevation of Privilege card game easily and simply helps you define and examine possible threats to software or computer systems.

Until now, considering a bunch of possible attacks may have seemed hard to wrap your head around. But through 6 threat groups, EoP keeps you focused on identifying attacks: Spoofing, Tampering, Repudiation, Denial of Service and Elevation of Privilege.

And because EoP incorporates a simple point system, you can challenge other developers and become your opponent's biggest threat.

Includes 84 cards

© 2008 Microsoft Corporation

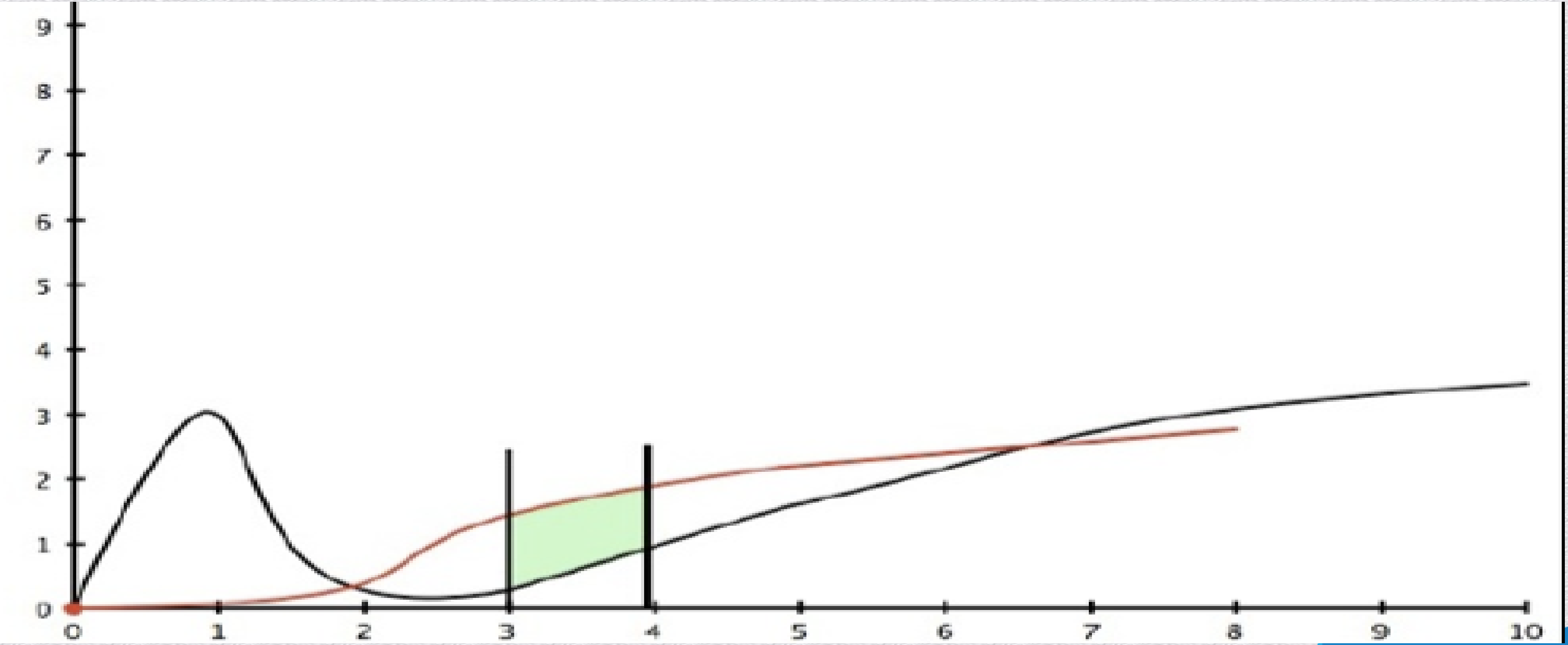
Oh The PaaSabilities: App Dev

- Embrace DevOps/CI/CD
  - Woodward: Code Changes & Complexity, 1979
  - Clark: Forthcoming
  - Build at every commit
  - Test at every commit
  - OSS and Commercial Options

Oh The PaaSabilities: App Dev

- Vulnerabilities
  - Ozment & Schechter: Milk vs Wine, 2006
    - 60% of vulnerable code was foundational
    - Security issues are intrinsic
  - Blaze, Clark, Frei, Smith: The Honeymoon Effect..., 2010
    - Largest vuln gap is from first release
    - Security is really an extrinsic property
  - Mortman-Hutton Model, 2009

The Mortman-Hutton Model



Oh The PaaSabilities: Final Thoughts

- Platform isolation looks pretty good
- Side effects of PaaS are compelling
- Some concerns w/Compliance etc.
- Limits to use case for 3rd Party Tools
- Highlights that security is code issue
- DevOps/CI/CD helps

RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Oh The PaaSabilities

CSV-R01

David Mortman

@mortman