THE 7 DIRTY WORDS OF CLOUD SECURITY

R.I.P.

GEORGE

...An Equal Opportunity Offender

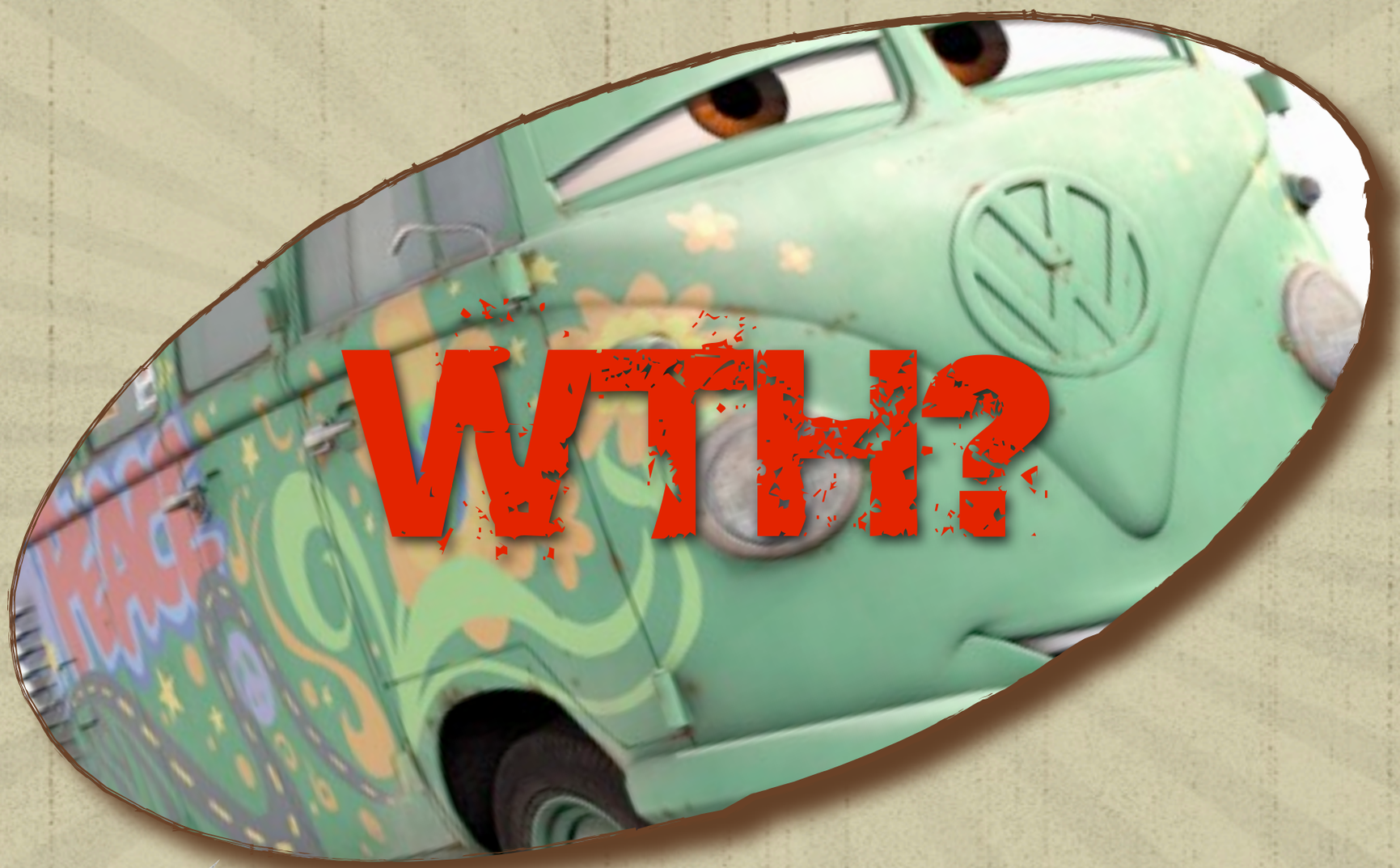
BE EXCELLENT...

Rufus - Bill & Ted's Excellent Adventure

CATHOLICISM, WOW!

Cardinal Glick - Dogma

RESPECT THE CLASSICS, MAN!



Disney presents a PIXAR film

Cars

Fillmore - Cars

LET'S BACK UP A SECOND...

LENNY BRUCE IS NOT AFRAID

- Actually existed prior to REM's lyrics
- An amazing comic; father of modern-day stand-up
- Was arrested during one of his performances for saying nine so-called "dirty words"
- He was the Mike Rothman of Comedy...

DON'T FORK WITH THE FCC

- 7 of Bruce's 9 original Dirty Words became...
- ...Carlin's "7 Words You Can Never Say On Television"
- ...which became "Filthy Words" that setup a battle with the FCC that went to the Supreme Court
- Carlin was also arrested for saying these words during a live performance

THE WORDS

THE 7 DIRTY WORDS

CENSORED

QUALYS®

On-Demand

Vulgarity Management

THE 7 DIRTY WORDS

1. **S**calability
2. **P**ortability
3. **F**ungibility
4. **C**ompliance
5. **C**ost
6. **M**anageability
7. **T**rust

...Of Cloud Security

WHY WE'RE AFRAID OF THE 7 DIRTY WORDS

- Every computing paradigm transition and disruption has instilled fear in incumbents and those that utilize their solutions

- Lack of mature tools, organizational shift of operational ownership, subverted control, lack of visibility, audit pain, highly dynamic environments...don't help

- Differences in delivery and deployment models means it's a multi-dimensional problem

- The velocity of disruption is unequivocally disturbing...we can't absorb change quickly

SOME PERSPECTIVE

- Who you are matters greatly to how sensitive you are to these Dirty Words - Service Providers vs. Consumers vs. Auditors...
- Enterprises own two of everything, some have mainframes and call them clouds... (Thank you, Mr. Reilly)
- “Pure” cloud (heh) is a reasonably recent phenomenon as are the stacks that power them and they are rapidly evolving
- The Public vs. Private cloud debacle highlights the “security problem”
- Let’s see why...

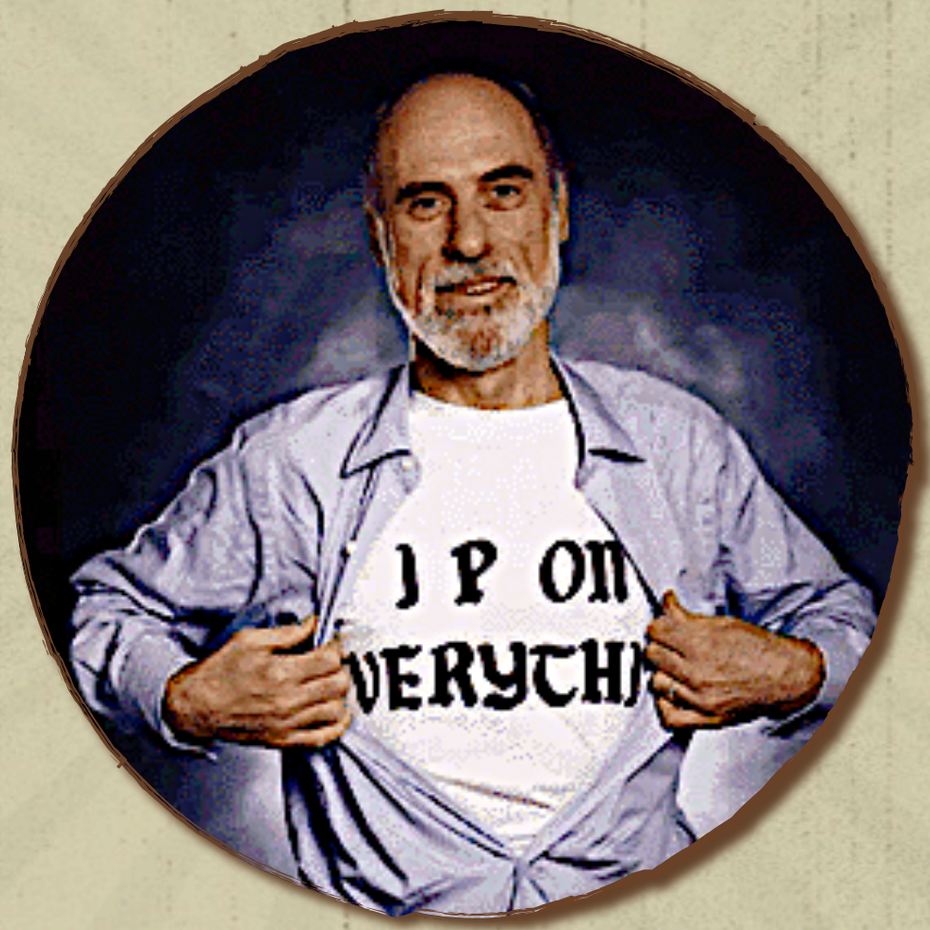
THE WORDS

SCALABILITY*

- Distributed Networked System problems are tough
- “Traditional” security doesn’t scale across distributed architecture
- The Hardware vs software cycle; where and how we invest is changing
- Metcalfe vs. Moore's Law vs. HD Moore’s Law (Thanks, Josh Corman!)
- Good enough vs. Best of breed

**Implies Performance*

HE P'S ON EVERYTHING...



Everything's Connected

DO NOT POKE THE BEAR

If You Think A Noogie Is Bad, Try the Wedgie!

PORTABILITY

- If we don't have consistency in standards/formats for workloads & stack insertion, we're not going to have consistency in security

- Inconsistent policies and network topologies make security service, topology & device-specific

- Abstraction has become a distraction

- Lack of consistent telemetry

- You cannot expect physical-appliance based security alone & virtual solutions are immature

FUNGIBILITY

- What's the difference between a firewall, a router and a switch from the perspective of the cloud?
- Where/What is the network?
- Hardware empowered by software or vice versa?
- Single function vs. programmable and extensible?
- UTM isn't fungibility, it's feature creep & the security equivalent of marrying your sister (See: Scalability)

COMPLIANCE

- Security != Compliance and “security” doesn’t matter
- ...Budget Does : Follow the money
- Compliance doesn’t fool anyone, especially security people...but we’ll gladly flaunt it when we get audited
- Regulatory compliance and frameworks don’t address emerging/disruptive innovation quickly enough
- Lack of automation for gathering audit/compliance artifacts

COST

- Built-in or bolted on? Either way, it ain't free, or when it is, you get what you pay for and when it's not, you often don't
- It's a squeezing the balloon problem depending on where the stack focus is
- Device or service centric - costs shift, but management and quality/stability cost you in the long run
- Operational experience and expertise is expensive

MANAGEABILITY

- This is the single worst dirty word of them all
- Security is everywhere, consistent management isn't
- Device centric vs application/service vs information centric security
- Managed by different tools, different people across discipline slices
- Differences in Deployment & Delivery Models
- APIs & Automation, FTW

MANAGEABILITY

- Here's what security management looks like in the Cloud*:

```
POST /api/1.0/vshield/host-5450 HTTP/1.1
Content-type: application/xml; charset=UTF-8
Authorization: Basic YWRtaW46ZGVmYXVsdA==
Cache-Control: no-cache
Pragma: no-cache
Host: 10.112.196.244
Accept: text/html, image/gif, image/jpeg, *; q=.2, */*; q=.2
Connection: keep-alive
Content-Length: 489

<VshieldConfiguration><VszInstallParams><DatastoreId>datastore-5035</DatastoreId>
                <ManagementPortSwitchId>network-4485</ManagementPortSwitchId><MgmtInterface>
                <IpAddress>10.112.196.245</IpAddress><NetworkMask>255.255.252.0</NetworkMask>
                <DefaultGw>10.112.199.253</DefaultGw></MgmtInterface></VszInstallParams>
                <PortgroupIsolationInstallParams><DatastoreId>datastore-5035</DatastoreId>
                </PortgroupIsolationInstallParams><EpsecInstallParams>true</EpsecInstallParams>
                <InstallAction>install</InstallAction></VshieldConfiguration>
```

*Specifically, VMware, vCloud

TRUST

- Trust models in computing are horribly warped
- Adding more abstraction makes the security problem more obtuse
- ...so, we don't "trust" the cloud
- We didn't "trust" client/server or the Internet, either
- We don't have a consistent way to measure and compare trust levels, so we hope instead


SECURITY
YOU'RE DOING IT WRONG

DON'T BE SILENCED

SPEAK THE WORDS

Solve The Problems

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Distributed architectures stretch the network, your security needs to respond in kind
- Host/guest, App, information, physical/logical network, hypervisor and platform-centric architecture is critical
- Service insertion/chaining or both “native” and external security services are required
- Automate!

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- IaaS: most portable security capabilities are those in the guests of VMs or the VMs themselves [See: Scalability] assuming you don't build it into the app layer
- PaaS: nteresting equalizer given where, who and how security is applied; AppSec is highly important
- SaaS: highly proprietary security-wise and you don't control it; leverage (id)entity and "federation"
- We need a common way of describing security requirements at the container, application and information level
- Realize you're going to end up with a hybrid model

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Automation leverages programmability, standardization of interfaces & re-use so choose solutions that enable/are enabled by it
- Learn to script/code and use platforms/tools that can be leveraged across your stacks and your providers'
- Look for software-driven solutions that interoperate with hardware and have SDK's/API's as part of the platform
- Security functions should be API driven and abstracted to allow for interchangeable components

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Leverage a consistent and cross-matrixed set of control objectives normalized across compliance frameworks (CSA CCM)
- Leverage automation (CloudAudit/STAR/CAI/CTP) to scale audit data gathering & presentation
- Check out ENISA Risk Assessment, CSA materials & CAMM
- Integrate vulnerability, threat, topology, control configuration and risk-assessment derived BIA on assets to manage from different PoVs

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Recognize that as we adapt, cloud & virtualization is initially squeezing of the cost balloon
- CapEx vs OpEx seems to forget the ‘Op’ part can cost you more without displacing MeatClouds with automation
- If you have limited visibility and transparency due to platform constraints, focus back on the basics of telemetry, instrumentation and monitoring
- If you’ve got the money, honey, I’ve got the time

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Still the elephant in the room and moose on the table...
- Fractured approach to management yields an unmanageable mess; consolidate, automate and instrument yourself or via a third party
- APIs are your friend
- Get used to crafting your own tools/ interfaces (again)
- Delivery and deployment models matter

SANITIZING THE 7 DIRTY WORDS

1. Scalability
2. Portability
3. Fungibility
4. Compliance
5. Cost
6. Manageability
7. Trust

- Trust is about hedging your bets (which is about managing exposure.) Not sure most have the precision to manage “risk”
- Ultimately how you measure risk determines who/how/why you trust Consistency in approach to measurement and audit
- Standardize on a methodology to link a rationalized “score” to exposure across your assets and your providers’
- Drive/demand better transparency & visibility from providers

ANOTHER 7 WORDS...

1. **S**calability
2. **P**ortability
3. **F**ungibility
4. **C**ompliance
5. **C**ost
6. **M**anageability
7. **T**rust

1. **S**ome
2. **P**eople
3. **F**orget
4. **C**loud
5. **C**oncerns
6. **M**ore (than)
7. **T**echnology...

SRSLY: TL;DR

- There's so much potential for awesomesauce with respect to Cloud and security...

- Cloud, virtualization and automation; you can do things you can't do otherwise and you can also get pwn3d in wonderfully inventive ways! Balance & common sense, FTW!

- If you approach Cloud security like it's 1991 and you think VLANs are still evil, you're responsible for the death of 11 kittens. You should feed badly.

SRSLY: TL;DR

WINNING!

[Christofer] Hoff

choff@packetfilter.com

choff@juniper.net

@beaker

+1.978.631.0302

Other Presentations In The Series...