Securing the Data Center

Andrew Benhase
Consulting Systems Engineer – Security

Rich Campbell
Consulting Systems Engineer – Data Center
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
Data Centers Are Under Increasing Pressure

New Business Pressures

Operational Limitations

Collaboration  Empowered User  SLA Metrics  Global Availability  Reg. Compliance

Power and Cooling  Asset Utilization  Provisioning  Security Threats  Bus. Continuance
The “Accidental Architecture”

- Siloed
- Complex, heterogeneous infrastructure
- New developments and applications
- Fragmented Security
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
SO, WHY DO WE EVEN NEED SECURITY?
Because of guys like this...

March 4, 2008 - 1:28PM

Hack into a Windows PC - no password needed

A security consultant based in New Zealand has released a tool that can unlock Windows computers in seconds without the need for a password.

Adam Boileau first demonstrated the hack, which affects Windows XP computers but has not yet been tested with Windows Vista, at a security conference in Sydney in 2006, but Microsoft has yet to develop a fix.

Conficker worm infects more than a million PCs

The $250,000 bounty Microsoft has put up for information on the controllers of the globe-spanning Conficker worm seems about right. Conficker has now infected the German military, along with networks in the British and French Air Forces and England’s Sheffield Teaching Hospitals. After several weeks of informal collaborations, the world’s top virus hunters have formed an official posse to hunt down these very slick bad guys.

At least one million PCs, perhaps as many as 10 million have been infected, says Eric Sites, a researcher at Sunbelt Software. (The numbers vary because security researchers differ on how to extrapolate some of the numbers intercepted from a counting mechanism that’s part of the worm.) By comparison, the Storm worm that spread via viral spam messages in 2007 is believed to have peaked at about 1 million botted PCs.

Conficker thus far is a two-trick pony: it spreads itself and then it prevents infected PCs from being cleaned up. Once implanted, the worm searches out nearby servers and executes a brute force password breaking program. It also spreads itself to any shared hard drives.

What’s more, it makes a copy of itself on any device plugged into a USB port, such as any thumb drives, music players, or digital cameras. When that infected device is later plugged into another PC, it infects that machine, which then begins to similarly spread more infections. This is reportedly how the French Navy got infected.
Ex-Fannie Mae employee accused of planting computer time bomb

A computer-engineering employee fired from troubled mortgage giant Fannie Mae is accused of preparing a malware computer time bomb, which had not been detected, might have destroyed millions of files, according to reports.

Rajendrasinh Makwana, the computer contract employee in question, was indicted earlier this week on computer intrusion charges, according to the "DC Examiner" report citing court documents. Makwana, said to be an Indian citizen and former contract employee at Fannie Mae for three years, was terminated Oct. 24 for changing computer settings without permission from his employer and allegedly hiding malware code in a server that was programmed to become active Jan. 31.

"reduced if not shut down operations" at Fannie Mae for at least a week. "The total damage would include cleaning out and restoring of 4,000 servers, restoring and securing the automation of mortgages, and restoring all data that was erased."
CLEAR AND PRESENT DANGERS

Andrew Benhase
Cisco
Real World Threats

- Highly Targeted electronic espionage
  - Spear fishing directed at Senior Leadership
  - Social Engineering of Leadership
- Prolonged Service Disruption to Leadership
- Direct funding of highly distributed Organized Crime in Russia, former Soviet block countries and China
- Aggregation of vast quantities of unclassified data to create an elaborate intelligence mosaic for foreign Intelligence services
NEW WORLD REALITIES
New Realities
New World Reality

- Endpoint Security
  - AV, Malware, Behavioral
- Patch Management
- Admission Controls
“OUR ENEMIES ARE OPERATING WITHIN OUR CERTIFICATION, ACCREDITATION AND ACQUISITION CYCLES”
Technology Circumference vs Acquisition Cycles

Decision and Use

Installation
Govt Lab Testing
Equipment Purchase
Approved Products List
Who is within the Small Circle?

Taliban using Skype phones to dodge MI6

By GLEN OWEN
Last updated at 11:10 PM on 13th September 2008
Comments (0) | Add to My Stories

Taliban fighters targeting British troops in Afghanistan are using the latest internet phones to evade detection by MI6, security sources said last night.

Skype, a popular piece of consumer software that allows free calls to be made over the web, has been adopted by insurgents to communicate with cells strung out across the country.

Unlike traditional mobile calls, which can be monitored by RAF Nimrod spy planes, Skype calls – the commercial application of a technology called Voice Over Internet Protocol (VOIP) – are heavily encrypted.
Who is within the Small Circle?

April 20, 2008

July 16, 2008

In Colombia, they call him Captain Ratacarrero was the inspiration for theQuebecois submarine that was used by cocaine traffickers.

Squat, bearded, and sporting a dashing character, the submarine's character is unique.

Cocaine traffickers here have dubbed the Quebecker "Sous-marin de la mer des Caraïbes." The submarine is made from a fibreglass submarine and is crewed by traffickers to haul cocaine from Colombia.

September 12, 2008

Colombia's FBI equivalent, the Department of Administrative Security.

In Colombia, paramilitary groups are spreading terror.

Figure in alleged Colombia scam extradited.
Who else?

How Gadgets Helped Mumbai Attackers

By Noah Shachtman  
December 01, 2008 | 9:39:23 AM  
Categories: Gadgets And Gear, T Is For Terror

The Mumbai terrorists used an array of commercial technologies -- from Blackberries to GPS navigators to anonymous e-mail accounts -- to pull off their heinous attacks.

For years, terrorists and insurgents around the world have used off-the-shelf hardware and software to stay ahead of bigger, better-funded authorities. In 2007, former U.S. Central Command chief Gen. John Abizaid complained that, with their Radio Shack stockpile of communications gear, "this enemy is better networked than we are." The strikes that killed at least 174 appears to be another example of how wired today's "global guerrillas" can be.

As they approached Mumbai by boat, the terrorists "steered the vessel using GPS equipment," according to the Daily Mail. A satellite phone was later found aboard.

Once the coordinated attacks began, the terrorists were on their cell phones constantly. They used BlackBerries "to monitor international reaction to the atrocities, and to check on the police response via the internet," the Courier Mail reports.
Asymmetric Warfare

Defining the system as the mobile and the platform and unfolding...

We have used our special satellite phone, used several different SIM cards, and events as the siege of BlackBerry web browsers.

“The system as the mobile and the platform and unfolding...”
Approved Product Listings

- Limit rapid deployment of innovative products
- Based largely on completely arbitrary security requirements
- NIAP generally required for compliance with NSTISSP#11 and DoDI 8500
- No intrinsic security value provided through current requirements for CC Evaluations

  Protection Profiles are not well maintained, very static in nature
  Customers are not knowledge about product purchase decisions based on criteria derived and tested in Vendor Security Target
Response: modern day sigint and propaganda

- Taliban and al-Qaeda use handheld radios on military frequencies to overload SIGINT platforms with random noise and propaganda
- Openly use military bands to antagonize troops and then use encrypted IP over higher frequency radio channels to communicate
- Supports IP packet service
Facebook- friend or foe?

- Rogue, unsigned applications running on your machine inside browser space
- You authorize applications to access your profile- which can include personal information
- Similar to opening an email attachment from your friend that says “Happy Birthday Present”
5 December, 2008

Facebook Virus Turns Your Computer into a Zombie
Brennon Slattery, PC World
Dec 5, 2008 11:02 am

- prompts you to update your Flash player before the video can be displayed. Therein lies the virus, cloaked in a "flash_player.exe" file

- Koobface" infects your computer, it prompts a downloaded service named Security Accounts Manager (SamSs) to load on start-up. SamSs then proxies all HTTP traffic, stealing results from popular search engines and hijacking them to lesser-known search sites

- Why? $$$
TOOLS FOR TERRORISTS
MS v2.0
Mujahedeen Secrets
Capabilities

- Primary use is for Messaging Confidentiality
- AES-256 2048bit keys
  - SuiteA equivalency
- Peer2Peer encryption for Chat, File Transfer, Email
(نظام إعلامي وביטريفيت ومشتتة وتأشيرة رقمية في عام 2024).

إيرادات الأداء الأولية:
- (AES finalist algorithms).
- (Ultra Strong Symmetric Encryption).
- (طريق 2048 بت) (زوج مفاهيم مبتكر).
- (رمز 256 بت).
- (Collisions Auto-detection).
- (Files Shredder).

إيرادات الأداء الثاني:
- (هيرالد الفضائي).
- (Files to Text Encoding).
- (إرسال من المستخدم للملفات).
- (إنهاء الاتصال لهذه البيانات مع وسائل الإعلام).
Islamic Emirate of the Caucasuses
Primary Author
US Shutting down Al-Ansar

- Intelligence value rapidly declining
- US pushes to shutdown the two primary websites
- Media distribution is immediately affected
- New Video distribution method being used: YouTube
الجبهة الإعلامية الإسلامية العالمية: سار بسلام وحيدًا

From: abuharbj
Joined: 2 months ago
Videos: 1

Added: July 06, 2008

More From: abuharbj

Related Videos

السؤال في القرآن الكريم
04:37 From: Ansar/Ansasheed
Views: 847

لا يلائم جهاده رأله إلا بالحريبي
08:41 From: oovOvoo
Views: 1,541

لا يلائم جهاده رأله إلا بالحريبي
08:09 From: CheChiLa
Views: 6,689

لا يلائم جهاده رأله إلا بالحريبي
04:10 From: oovOvoo
Views: 2,427
New Realizations

- Virtualization
  - Is changing the security model
- Perimeter security
  - Does not secure the data center
- SOA interoperability
  - Adds new vulnerabilities
Cisco Security in the Data Center

Data Protection
- Security automatically associated with VM instances
- Layered prevention
- Standard security practices operationalized and automated within the data center

DR/COOP
- High-speed encryption to parallel data center sites
- Secure data at rest and in-flight via access control and encryption
- SSL VPN for secure connections from anywhere

Preventing Insider Threat
- Secure virtual resource segmentation
- Automated monitoring/control of access
- Incremental buildout to meet current and future requirements
- Protect reputation and avoid liability

Virtualization Security
- Virtual context-aware security policy
- Platform agnostic
- Prevents breaches and Insider threat
- Allows for VM portability
- Protects both the Hypervisor, and guest OS
Steps to Securing the Data Center

- Secure the network
- Secure the applications
- Secure the virtualized environment
- Ensure system performance, and optimization with detailed security policies
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
Comments and Caveats

- There is no “single correct design”
- Location and scale of network
- Co-location variables
  - Internet gateway connections
  - Corporate LAN
- Equipment choices
  - Through-put requirements
  - Scalability
  - Blades vs. appliances
Architecture Overview

- Wan Edge Layer
- Firewall and DMZ Layer
- High Speed Campus Core Layer
- Data Center Security Layer
- DC Core
- Application/Server Layer
- SAN Fabric Layer
Firewall and DMZ Layer

- **Perimeter Security**
  Intrusion prevention, DDoS, DNS attacks

- **Controlling access to public resources**
  Load balancing, global load balancing, global site selection

- **Preventing access to private resource**
  Web application firewall
  XML gateway
  Application security at the edge
Data Center Sub-Perimeter

- **First line of defense for Application Security**
  - Insider threat
  - Policy enforcement
- **Improves data center performance**
  - Load balancing
  - Segments application
  - Virtualizes server farms

![Diagram of data center sub-perimeter with ASA, Cat6k ACE, and Internal NIDS connections.]

---

**Layer Breakdown**
- Wan Edge Layer
- Firewall and DMZ Layer
- High Speed Campus Core Layer
- Data Center Security Layer
- DC Core
- Application/Server Layer
- SAN Fabric Layer
Data Center Switching

- High speed core switching
- Virtual switching: Unified Fabric
- The future in data center switching
  - Linking role-based access control with virtualization
  - Cisco TrustSec and Unified Fabric
Application Server Layer

- Switch and virtual switch port level security
- Physical machine security policy
- Virtual machine security policy
- Preventing insider threat
- Preventing root kits
- Securing VM portability
SAN Fabric Layer

- **Fabric scalability and performance**
  Resilient, high performance fabric to support large, dense VM environments

- **VSANs isolate fault domains**
  Increase availability, simplify troubleshooting, improve security and compliance

- **Mobility with security**
  Wire-speed encryption protects data in transit and VMs during migration

- **Enabling secure DR/COOP operations**
  Continuous data protection and continuous remote replication with encryption and security profiles
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
Secure Campus Access Control:
Role Based Access Control Deployment

Legend

<table>
<thead>
<tr>
<th>Link/Port Status</th>
<th>Security Group Classifications</th>
</tr>
</thead>
<tbody>
<tr>
<td>-</td>
<td>Ingress Tagging</td>
</tr>
<tr>
<td>Unauthenticated</td>
<td>E Employee Group</td>
</tr>
<tr>
<td>F Authentication</td>
<td>Confidential Group</td>
</tr>
<tr>
<td>A Authentication</td>
<td>Partner Group</td>
</tr>
<tr>
<td>A Authentication</td>
<td>Unrestricted Group</td>
</tr>
<tr>
<td>A Authentication</td>
<td>Guest Group</td>
</tr>
<tr>
<td>A Authentication</td>
<td>Internet Group</td>
</tr>
</tbody>
</table>

Source Groups

Destination Groups

- E Employee Group
- P Partner Group
- G Guest Group
- I Internet Group

SGACL Matrix

- C Confidential Group
- U Unrestricted Group
- I Internet Group

Access Denied

Internet

General

CRM

Employee

Partner

Guest
End-to-End Deployment
Delivers Investment Protection

Access Control
- Identity-based Networking
- Role-based Access Control
- Network Admission Control

Policy Enforcement
- Firewall
- Intrusion Prevention
- Switch Policy Engine

Pervasive Confidentiality
- LAN Confidentiality
- Device Integrity
- WAN Confidentiality
Mapping Physical to Virtual Data Center Security

- As workloads migrate to Virtual Machines, security policies must be maintained
  
  Same Application and OS executes within a VM requiring the security policy to be applied to the VM

- Hypervisor abstracts Application and OS from hardware
  
  Schedules and controls access to all system resources requiring a different security policy from the VM

- Enables multiple guest OS and Applications on the same physical server requiring more detailed security policy for the Virtualized environment

- Provides resource segmentation and VM mobility requiring Security policy to follow the individual VM
VM security policies are the same as physical server policies

Apply existing security policy to VM environments
  - Extend policies to virtual environments for LAN and SAN
  - Requires coordination between IA, Server, LAN and SAN teams

VN-Link services will extend per-VM allowing detailed visibility and security control over VMs

VN-Link services allow security policy to follow the VM
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
Data Center Services

- Data Center Assessment
- DCAAL
Agenda

- Accidental Architecture
- Why Cisco Security in the Data Center
- Layered Architecture Solution
- Cisco’s Solution Summary
- Data Center Services
- Why Cisco?
Setting Cisco Apart from the Rest

- Technical thought leadership
  22-year track record as industry leader
  Decades of enterprise expertise and best practices
  Human network for Enterprise

- Commitment to security
  1500+ security engineers
  $500M in security R&D
  Security partnerships/acquisitions

- Secure network as platform
  Collaborative, integrated approach to securing the federal enterprise

- Cisco® Consulting Services

- Cisco Capital finance programs

“Because the network is a strategic customer asset, the protection of its business-critical applications and resources is a top priority.”

John Chambers, Chairman and CEO, Cisco
Q&A