Cisco Security Agent (CSA)
Network Admission Control (NAC)

Pascal Delprat
Security Consultant
Cisco France

Vincent Bieri
Marketing Manager, Security
EMEA Technology Marketing Organisation
Agenda

- CSA and NAC Presentation (30’) – vincent bieri
- CSA Demo (20’) – pascal delprat
- Q&A / Discussions (10’) – all
Cisco Security Agent (CSA)
Agenda – CSA

• Overview of Cisco Security Agent
• Management Model
• CSA Implementation and Architecture
• Security Functions
• Performance Impact
• Integration with Other Security Technologies
• Roadmap CSA 4.5
What is Cisco Security Agent?

• A security software for desktop, laptop, & server computers that minimizes patch and security problems with behavior-based OS kernel wrappers

• Centrally administered, with distributed, autonomous policy enforcement
  
  Scales well & also works with intermittently connected hosts
  
  Can also adapt defenses based upon correlation of events from different hosts

• Effective against existing & previously unseen attacks
  
  Stopped nimda, code red, slammer, blaster with out-of-the-box policies
JPEG (GDI+) OVERFLOW

The process 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to accept a TCP connection from 172.20.12.1 on port 4444 and this was prevented.

The critical system application 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to call the function CreateProcessA("CMD") from a buffer (the return address was 0x19163cb). The code at this address is "515351ff 75006872 1e6316ff 5504f0d0 89e5f775 00631ad9 05e0ff53 0460c35a" This either happens when a program uses self-modifying code or when a program has been subverted by a buffer overflow attack. The user chose 'Yes'.

The process 'C:\WINDOWS\Explorer.EXE' (as user XP-PRO-SP1A\Administrator) tried to accept a TCP connection from 172.20.12.1 on port 4444 and this was prevented.

Default action will be taken in 4 minutes:57 seconds

Cisco Security Agent: A problem was detected, press one of the action buttons below.

The network application 'C:\WINDOWS\Explorer.EXE' (which is an important system process) tried to make a system call from self-modifying code. This normally happens when a program has been subverted by a buffer overflow attack. If you want to prevent further execution of the specific thread, choose 'Terminate' below. Your system may need to be rebooted in any case.

Yes  Yes to All  Terminate
Cisco Security Agent (CSA) Components

**Management Server**—deploys Security Policies, Receives and Stores Events in SQL Database, Alerts Administrators, Deploys Software, Part of Cisco VPN and Security Management System

**Cisco Security Agents**—Enforce Security Policy Received from Management Server, Sends Events Immediately, Interacts with User (If Necessary), Protects Itself, Poll for Policy Updates, Run on Windows and Solaris

**CSA Management Console**—Web Browser Interface, Policy Configuration Tool, Event Views
Management Architecture

Remote Users or Branch Offices

- Events are pushed to it
- Configuration is pulled from it

DMZ

Management Server
- Events are pushed to it
- Configuration is pulled from it

Campus
Hosts are Attached to a Group that includes a set of Policies defined by Rules

GROUP
Web Servers

HOSTS
Web1.cisco.com
Web2.cisco.com

POLICIES
IIS Module
Windows Module
Groups

- Used to Organize Logical Collections of Hosts
  e.g. “IIS Servers”, “Executive Desktops”, or “SQL Servers”

- Default Desktops: Default group for systems that install the Desktop agent kit
- Default Remote Laptops: Default group for systems that install the Remote Laptop agent kit
- Default Servers: Default group for systems that install the Server agent kit
- DHCP and DNS Servers - Dedicated: DHCP and DNS servers that are not running any other server applications
Policies

- Are attached to zero or more groups
- Are composed of logical collections of rules
Rules

- Are attached to policies
- Are where security functions are specified
- May enable specific heuristics

### Rules Table

<table>
<thead>
<tr>
<th>ID</th>
<th>Type</th>
<th>Events</th>
<th>Status</th>
<th>Action</th>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>336</td>
<td>File access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Email applications, read/write dynamically quarantined files</td>
</tr>
<tr>
<td>340</td>
<td>File access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Email applications, user initiated applications and command shells</td>
</tr>
<tr>
<td>334</td>
<td>File access control</td>
<td>Disabled</td>
<td></td>
<td>Disable</td>
<td></td>
<td>Backup applications, read all files</td>
</tr>
<tr>
<td>337</td>
<td>COM component access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>PDA applications, access outlook</td>
</tr>
<tr>
<td>242</td>
<td>File access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Initializing local applications, read/write registry files types (which are considered vulnerable to virus)</td>
</tr>
<tr>
<td>343</td>
<td>File access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>All applications, write PDA applications</td>
</tr>
<tr>
<td>339</td>
<td>File access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Email applications, write Suspicious or Dangerous Email files</td>
</tr>
<tr>
<td>200</td>
<td>COM component access control</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Vulnerable applications and Windows Scripting Host, accessing outlook</td>
</tr>
<tr>
<td>222</td>
<td>Network worm protection</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Detect and protect against network worms</td>
</tr>
<tr>
<td>220</td>
<td>Trojan detection</td>
<td>Enabled</td>
<td></td>
<td>Enable</td>
<td></td>
<td>Detect and terminate potential application trojans</td>
</tr>
</tbody>
</table>

Security With CSA and NAC © 2004 Cisco Systems, Inc. All rights reserved.
CSA Security Functions

- **System hardening**
  - Syn-flood protection
  - Malformed packet protection
  - Restart of failed services

- **Resource protection**
  - File access control
  - Network access control
  - Registry access control
  - COM component access control

- **Control of executable content**
  - Protection against email worms
  - Protection against automatic execution of downloaded files or ActiveX controls

- **Application-related**
  - Application run control
  - Executable file version control
  - Protection against code injection
  - Protection of process memory
  - Protection against buffer overflows
  - Protection against keystroke logging

- **Detection**
  - Packet sniffers and unauthorized protocols
  - Network scans
  - Monitoring of OS event logs

- **Network firewalling**
CSA Implementation Approaches

- **Call Interception**
  Intercept system calls between applications and the operating system

- **Security policy**
  - Pre-defined rules
  - Heuristics
  - Combination of methods

- **System “state” monitoring**
  Application behavior—What are the running applications doing?
CSA Architecture Overview

Application

File system interceptor
Network interceptor
Configuration interceptor
Execution space interceptor

Rules engine
State
Correlation engine
Rules & policies

Kernel
Allowed request
Blocked request
Performance Impact

- Windows CPU usage: 1-5%
- Solaris CPU usage: 3-10%
- Memory usage: 7–10MB, up to 20
- Network impact:
  - Policy download: 35-70k
  - Event: ~3k
  - Poll: ~2.5k
  - Polling interval change: ~3k
  - Software update: Varies
- Transactions per second is a very good way to measure latency
Performance: Transactions per Second

HTTP Requests (W2K)

Note: Performed on W2K SP3 Running IIS 5.0; Single 2Ghz P4 CPU, 1Gbps NIC, Non-hyperthreaded, 533Mhz System Bus
CSA Integration other Security Technologies

• VPN “Are You There”
  Requires version 4.0 of Cisco VPN client and concentrator
  Also supported in Checkpoint VPN-1

• Network Admission Control (NAC)

• Complement NIDS and AV
  Combining signature detection and behavioral protection
  Need AV to eradicate a virus, worm, or trojan

• Log Collectors and Correlators

• Windows Event Viewer and AV logs into CSA events
Cisco Security Agent Roadmap

New Agent Platforms – ver 4.5

- Windows Clusters
- RedHat Enterprise Linux 3.0
  - Enterprise Server, Workstation
  - Advanced Server (Stretch Goal)
- Windows XP Home Edition

New Features – version 4.5

- MC Scalable to 100,000 agents
- Antivirus DAT version checking
- Application/patch tracking
- Location-based policies
- User-based profiles
- Agent Internationalization & Localization
- Policies based on NAC status
- Security Enhancements

New Agent Platforms – ver 4.0.3

- Windows 2003 Server
- Windows XP SP2

New Features

- RTM: 13 Dec 2004
- CCO Download: 13 Dec 2004
- FCS: 22 July 2004

New Agent Platforms

- RTM: 22 July 2004
- CCO Download: 22 July 2004
- FCS: 22 July 2004
Network Admission Control (NAC)
Agenda – NAC

- Overview of Network Admission Control
- NAC Phase 1 (Current) Model and Components
- NAC Credentials
- NAC Phase 2 (Future) Model and Components
Network Admission Control (NAC)
preventing non-compliant host

Client attempts connection

- Access Granted
- Access Denied
- Quarantine Remediation
NAC Phase 1 Logical Components

June 2004

CTA

EAPoUDP

RADIUS

HCAP

Cisco Security Agent
McAfee VirusScan
Symantec SAV & SCS (EDAP customers only)
Trend Micro OfficeScan

Cisco Trust Agent (NT, 2000, XP)

Routers (83x-72xx)

Cisco Secure ACS

Monitoring & Reporting
CiscoWorks SIMS

Trend Micro Control Manager
Credentials Available

- NAC credentials characterize the state of an asset, and compliment ID credentials for the asset and user
- Credentials form the basis for policy expressions for network admission control
- Below are most of the initial credentials available at NAC phase 1 ship
- Vendors will add new credentials often and at any time

FROM CISCO AGENTS
- CTA 1.0
  - CTA version
  - Operating system name
  - Operating system version
- CSA 4.0.2
  - Installed Service Packs
  - Installed hotfixes
  - CSA version
  - CSA enabled or disabled
  - FQDN of CSA-MC (VMS)
  - CSA status
  - Last poll of CSA-MC (VMS)

FROM VENDORS
- Anti-Virus
  - AV software name or identifier
  - Software version
  - Scan engine version
  - DAT/pattern file version
  - AV enabled or not
  - On-access scan enabled
  - DAT/pattern file release date
- Other Software
  - Varies by vendor
    - E.g. SYMC SCS 2.0 includes FW and HIDS