Continuous Auditing

Onderdeel van een volwaarde beveiligingsorganisatie

8 maart 2006

Matthijs Koot, Jonel Spellen, Fangbin Liu

Universiteit van Amsterdam
Master Systeem en NetwerkBeheer
2005-2006
Large Installation Administration

Opzet

- **Waarom** te auditen? (Matthijs)
- **Wat** te auditen? (Jonel)
- **Hoe** te auditen? (Fangbin)

Opzet

- **Waarom** te auditen? (Matthijs)
- **Wat** te auditen? (Jonel)
- **Hoe** te auditen? (Fangbin)

Noot: ons verhaal gaat NIET over (EDP-)auditing in formele zin!

Waarom te auditen?
Rode draad:

- Begripsdefinitie + rechtvaardiging
- Verbanden met:
  - systeemontwikkeling
  - systeembeheer

Continuous Auditing

- Wat is "auditing"?
  - Systematisch onderzoek naar organisatie, werkwijzen en procedures
  - Controle op naleving van normen(kaders)
  - De rest volgt op 17 maart (gastcollege KPMG)
- Wat is "continuous auditing"?
  - écht continu
  - perodiek

- Ad 2.1: echt continu="in-band"-verankerde controles (vgl. halt-on-audit-failure Grid)
- Ad 2.2: periodiek="out-of-band" controleprocessen

Continuous Auditing (2)

- "Continuous auditing" in verschillende betekenissen:
  - Kern: financiën
    - Vanwege Ahold, Enron
  - Ondersteunend: ICT
    - Vanwege Ahold, Enron :-)

Waarom dit alles?

- “Goed huisvaderschap”
- Nederlandse corporate governance code
- SOx, HIPAA, NEN7510, ...
- Common sense?

Beginselen

- Informatie is een productiemiddel (geworden)
- Kwaliteit van informatievoorziening is belangrijk voor bedrijfsvoering
  - Schaalbaarheid is een kwaliteitsaspect...
  - Uitbreidbaarheid is een kwaliteitsaspect...
  - Maar beveiliging ook!

- in accountancy ligt de nadruk op "kwaliteit van informatie", niet zozeer van de "informatievoorziening"

Beveiliging door maatregelen?

- Maatregelen om kwaliteit te vergroten?
  - Organisatorische/procedurele maatregelen
  - Technische maatregelen
  - Voorbeelden staan in CvIB (ISO/IEC 17799), Common Criteria, enz.

Om een informatievoorziening te beveiligen worden maatregelen genomen (kort door de bocht)

Beveiliging door maatregelen? (2)

- Selectie van maatregelen volgt na risicoanalyse en wordt vastgelegd in een beleidsplan
- **Algemene regel: beleid moet controleerbaar zijn!**
- **Dus: (technische) beveiligingsmaatregelen moeten ook controleerbaar zijn**
  - Zijn de gastaccounts uitgeschakeld?
  - Staat accounting aan? (success/failure)

Beveiliging van informatievoorziening

- Aandacht nodig tijdens systeem*ontwikkeling*
  - Best practices: secure coding, software testing, enz.
  - Incl. voorzien in controleerbaarheid!
  - *SSE-CMM als procesmodel?*

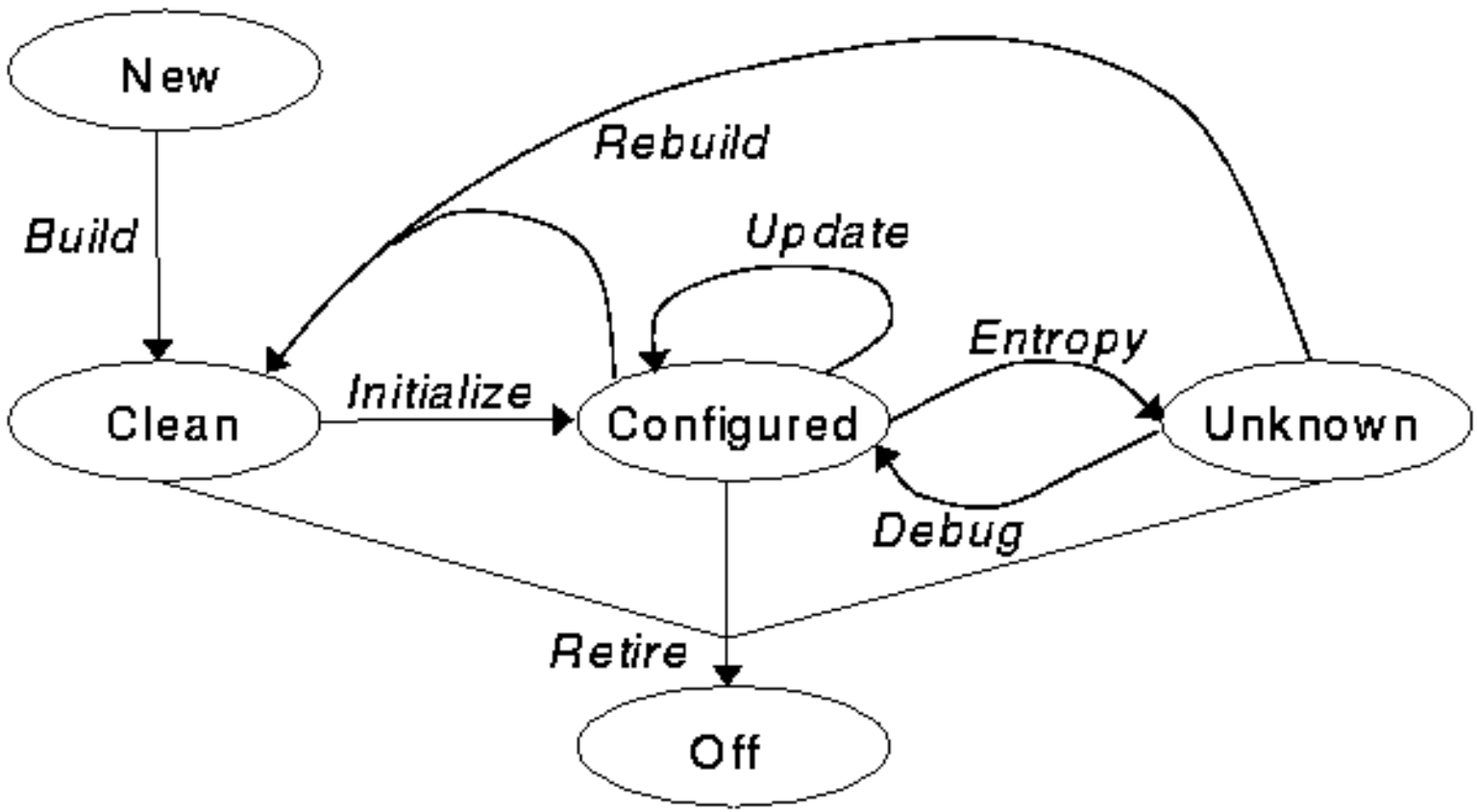
- (security) requirements engineering
- security in analysis/design
- security in implementation
- enz.
- Jaap's voorbeeld van promiscue backupschermen

Beveiliging van informatievoorziening

- Aandacht nodig tijdens systeem*beheer*
  - Best practices: segmentation, least privilege, enz.
  - Incl. uitvoeren van controles!
  - *SSE-CMM als procesmodel?*

- (security) requirements engineering (!)
- security in deployment (secure unattended install)
- security in maintenance (versleuteling in remote admin; anonimisatie)
- enz.

Beveiliging van informatievoorziening



Bron: http://www.usenix.org

Wat is SSE-CMM?

- Referentiemodel voor "security engineering" processen
- Best practices zijn nu meetbaar! (KPIs)
- 22 Process Areas (PAs)
  - 6 organisatie PAs
  - 5 project PAs
  - 11 "security engineering" PAs

- Ad. 1: Compilatie van best-practices (veelal common sense, ervaringskennis)
- Ad. 1: Losjes gebaseerd op SE-CMM van SEI
- Ad. 2: meetbaar = goed :-) (zelfreflectie)
- Ad. 3: org/project PAs zijn algemeen CMM
- Let wel: dit is LARGE Installation Administration

Wat is SSE-CMM? (2)

- Security Engineering Process Areas:
  - PA 01 - Administer Security Controls
  - PA 02 - Assess Impact
  - PA 03 - Assess Security Risk
  - PA 04 - Assess Threat
  - PA 05 - Assess Vulnerability
  - PA 06 - Build Assurance Argument

Wat is SSE-CMM? (3)

- Security Engineering Process Areas (vervolg):
  - PA 07 - Coordinate Security
  - PA 08 - Monitor Security Posture
  - PA 09 - Provide Security Input
  - PA 10 - Specify Security Needs
  - PA 11 - Verify and Validate Security

Wat is SSE-CMM? (4)

- Process Areas: 5+1 niveaus van volwassenheid
  - 0=initial
  - 1=performed informally
  - 2=planned & tracked
  - 3=well-defined
  - 4=quantitatively controlled
  - 5=continuously improving

Wat is SSE-CMM? (5)

Bron: http://www.cetic.be

Wat is SSE-CMM? (6)

- Een middel voor zelfevaluatie
- Een selectiecriterium
- Transitieve vertrouwensrelaties in procesketens

- Ad. 2: vgl. ISO-17799 certificering; selectiecriterium voor klanten
- Ad. 3: if A>=B and C>=B, dan C>=A

Echter: vgl. ISO 9000 doet SSE-CMM geen uitspraak over de kwaliteit van de geimplementeerde maatregelen... that's up to the SSE-CMM taxateur!

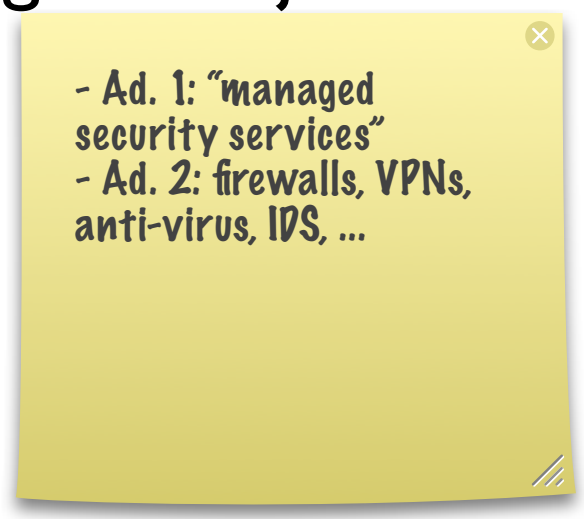
Wat is SSE-CMM? (7)

- Ad. 1: sinds oktober 2002
- Ad. 2: doch niet zo technisch als Common Criteria
- Ad. 3: OMB Circulars (white house), Security Process Framework, ISO/IEC 13335 (GMITS), NIST Handbook, ...

- SSE-CMM = ISO/IEC 21827
- "17799 beschrijft wàt, 21827 beschrijft hoe
- Raakvlak/overlap met andere methoden/ raamwerken
  - zie http://www.issea.org/docs/sse-guides_2001.pdf

Voor wie is SSE-CMM bedoeld?

- Leveranciers van beveiligingsdiensten
- Ontwikkelaars van beveiligingsproducten
- Secure system developers/integrators/jouw-functie-hier



Voor wie is SSE-CMM bedoeld?

- Leveranciers van beveiligingsdiensten
- Ontwikkelaars van beveiligingsproducten
- Secure system developers/integrators/jouw-functie-hier

Dus: voor ons allemaal!

- Ad. 1: "managed security services"
- Ad. 2: firewalls, VPNs, anti-virus, IDS, ...

Says who?

- DISA, NSA
- NCSA, NIST
- MITRE
- Software Engineering Institute (Carnegie Mellon)
- Electronic Warfare Associates
- Cisco
- *Onderhoud/ontwikkeling SSE-CMM is sinds 1999 belegd bij ISSEA*

Wat is de scope van SSE-CMM?

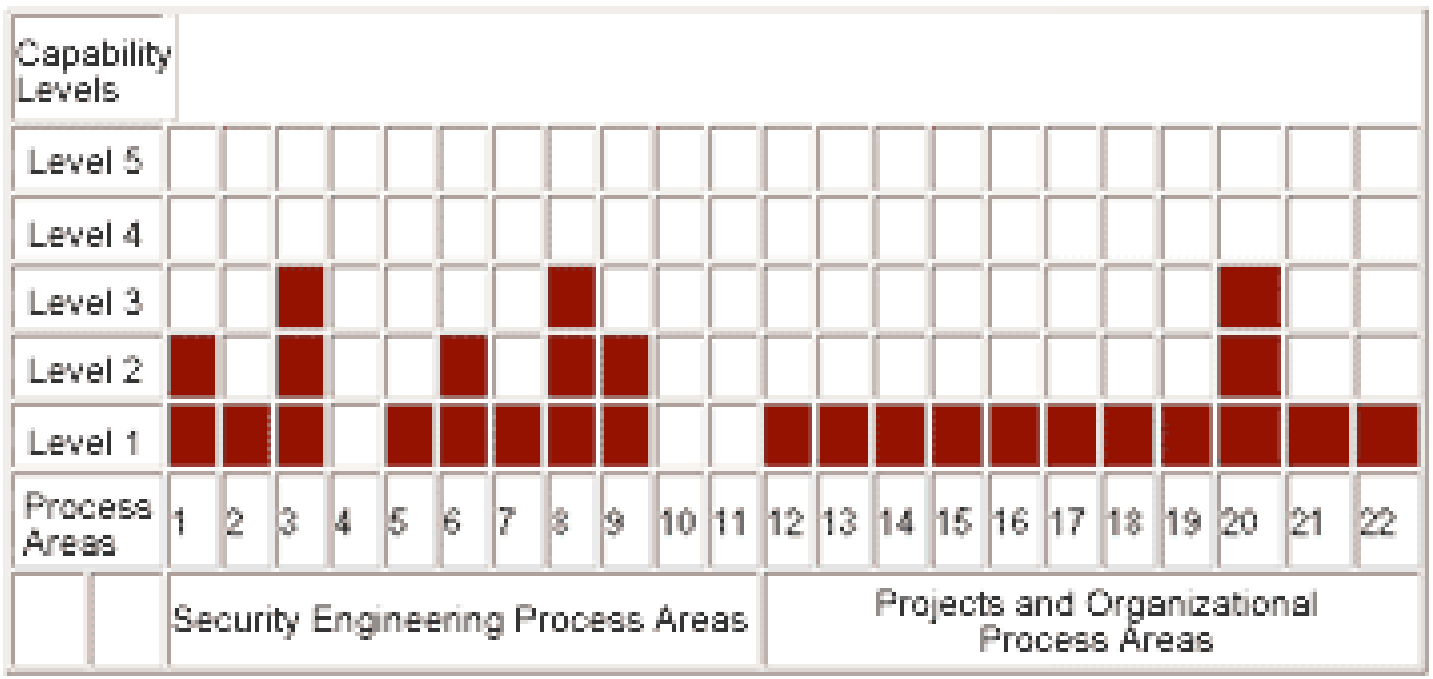
- De gehele "trusted product or secure system life cycle”
- Alle sectoren

- Ad. 1: van concept tot uitfasering (ref. ISO 15288 voor "system life cycle")
- Ad. 2: overheid, finance, retail, onderwijs, ...

Hoe wordt het SSE-CMM niveau bepaald?

- Taxatie via SSAM "Appraisal Method"
  - intern (zelfevaluatie)
  - extern (klantrelaties, overnames, ...)
- Projectmatig
  - preparation phase
  - on-site phase
  - post-appraisal phase

Hoe wordt het SSE-CMM niveau bepaald?



Bron: http://sse-cmm.org

Pff, en nou concreet

- Onder PA-05 (Assess Vulnerability) kan NSA beslag leggen op belastinggeld om 1337 security/scanning tools te kunnen gebruiken:
  - CORE IMPACT, Nessus, nmap, metasploit, ...
- Onder PA-08 (Monitor Security Posture) kan NSA beslag leggen op belastinggeld om hun NT/UNIX/etc. systemen fatsoenlijk te configureren (voorbeelden uit NT checklist):
  - "1.5 GUEST accounts are disabled or removed?"
  - "1.14 Unnecessary Services are disabled?"
  - "4.1 Auditing is Enabled For Logon and Logoff (Success and Failure)?"
- Ons praatje gaat vooral over PA-08

Ten slotte

- MBAs denken in processen
- MSc's denken in techniek
- HRMs denken in mensen
- Beveiliging = MBA + MSc + HRM

Bronnen

- “Handboek EDP-Auditing”, Kluwer, 2003
- SSE-CMM.org
- netcentrum.nl/ea/
- GvIB.nl :-)

Vragen?

>> Next in line-up: Jonel

What to audit? Red Wire:

- Introduction
- Internal and External Auditing
- Security Policies
- Continuous System Auditing
- Summary
- Questions

Introduction

- Ways to audit
  - External audit
  - Internal audit

Internal auditing

- Checking whether security environment are in compliance with policy and design criteria
- Employee and contractor list against AA database
- Physical checking
- Machine checking up-to-date
- Scanning relevant machines to verify services
- Launching sophisticated in-depth attacks particular area in the infrastructure.

External auditing

- Examining security of a company from outside
  - Scanning networks
  - Remote access point
  - Penetration tests
  - In-dept attacks
  - Social engineering

Policies

- Acceptable Use Policy
- Monitoring and Privacy Policy
- Remote Accessing Policy
- Network Connectivity Policy
- Log Retention Policy

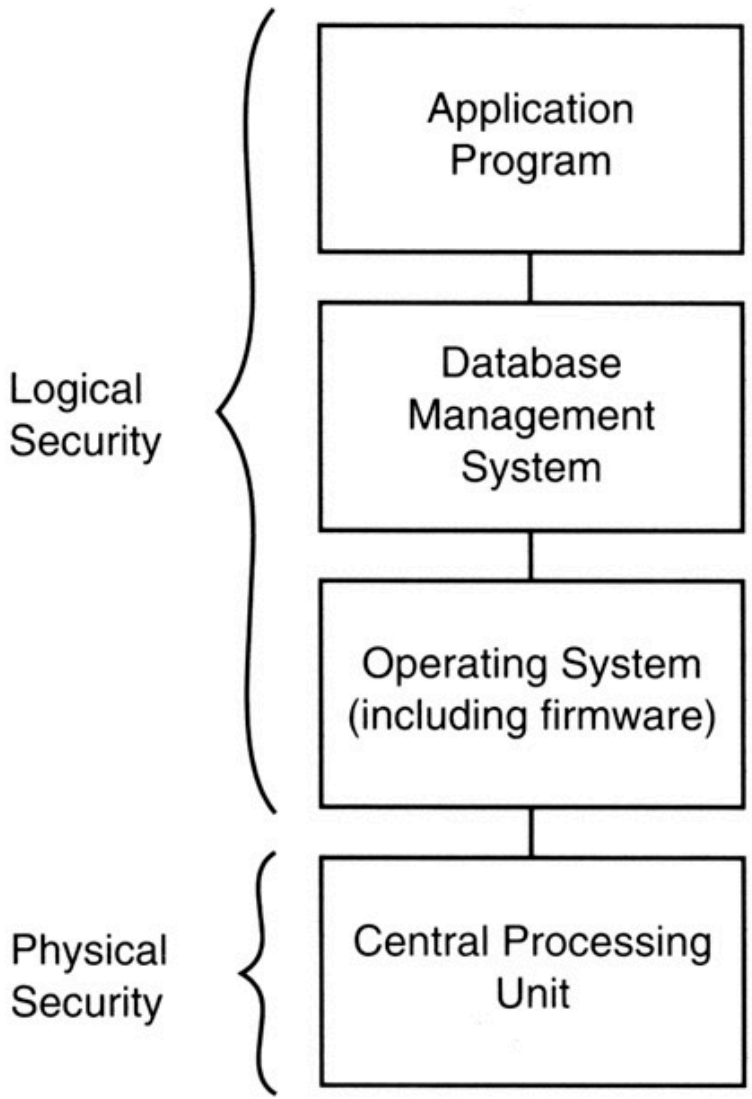
Continuous System Auditing

- What is Internal Continuous System Auditing
- System en network policies
- Checklist to audit

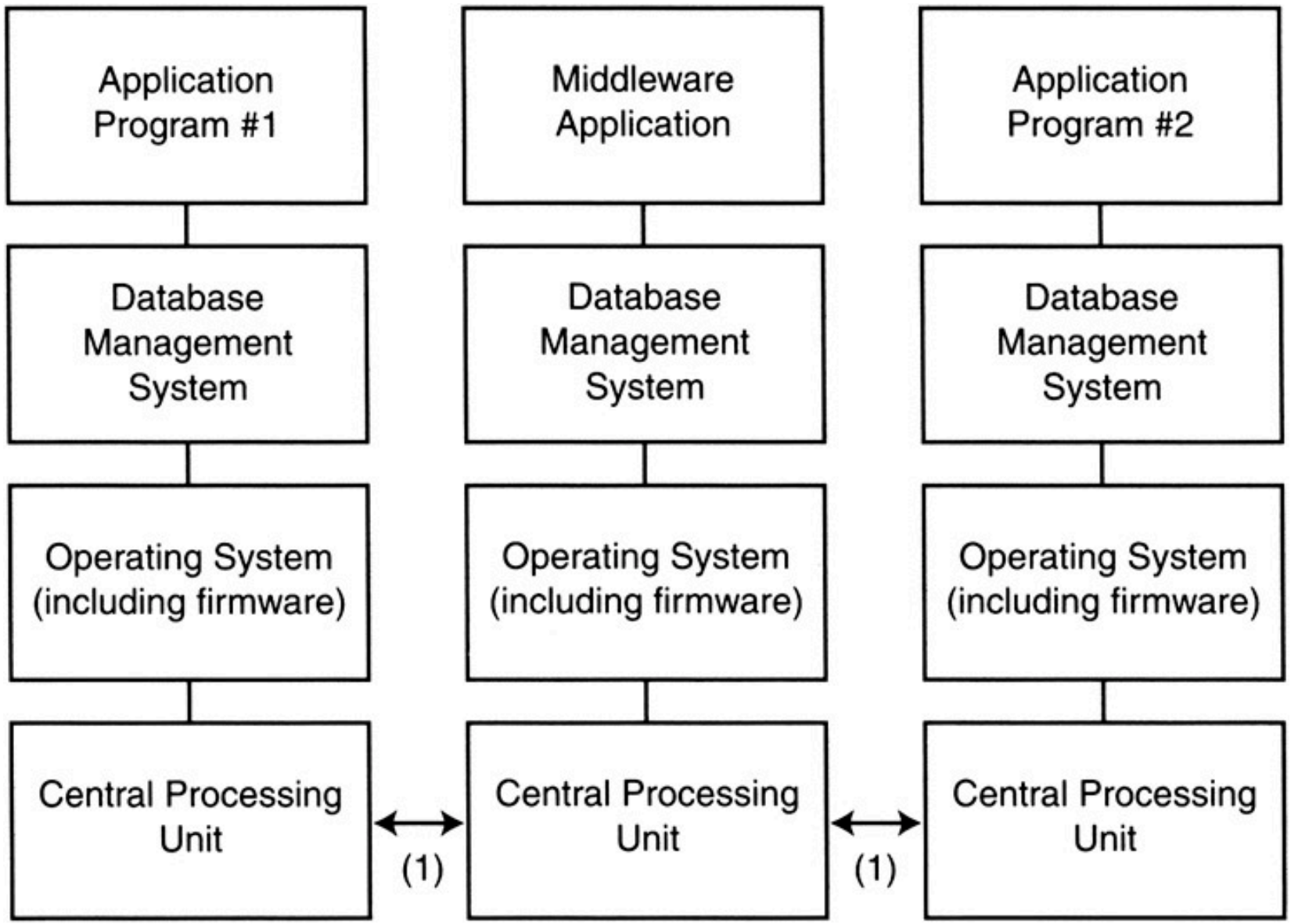
Continuous System Auditing

- Central Processing Unit
- Operator System
- Application Programs
- Database Management System
- Physical Security Control
- Logical Security Control

Model #1


Application Program
Database Management System
Operating System (including firmware)
Central Processing Unit
Logical Security
Physical Security

Model #2


Application Program #1
Middleware Application
Application Program #2
Database Management System
Database Management System
Database Management System
Operating System (including firmware)
Operating System (including firmware)
Operating System (including firmware)
Central Processing Unit
(1)
Central Processing Unit
(1)
Central Processing Unit

Checklist

- How much systems on the network
- What type of systems
- Check amount Router and Switches on the network
- Default Configurations
- Check if systems are patched or not patched
- Services running on the hosts
- Resources in use
- etc?

What we want to audit

- Operating System
- Application Programs
- Logical Security Control

Operating System Audit

- Antivirus
- Firewall
- Security updates
- Status of the default configuration
- File systems

Application Programs

- Services running
- Open ports
- User policies
- Backups
- Log files

Logical Security Control

- Changes Network Infrastructure (without change procedure)
- Network configurations
  - Routers
  - Log files

Summary system auditing

- Knowing the environment
- Company policy
- Make checklist
- Find the appropriate tools

References

- "The Practice of System and Network Administration", *Thomas A. Limoncelli and Christine Hogan*
- "Auditing Information Systems, Second Edition", *Jack J. Champlain*

Questions?

>> Next in line-up: Fangbin

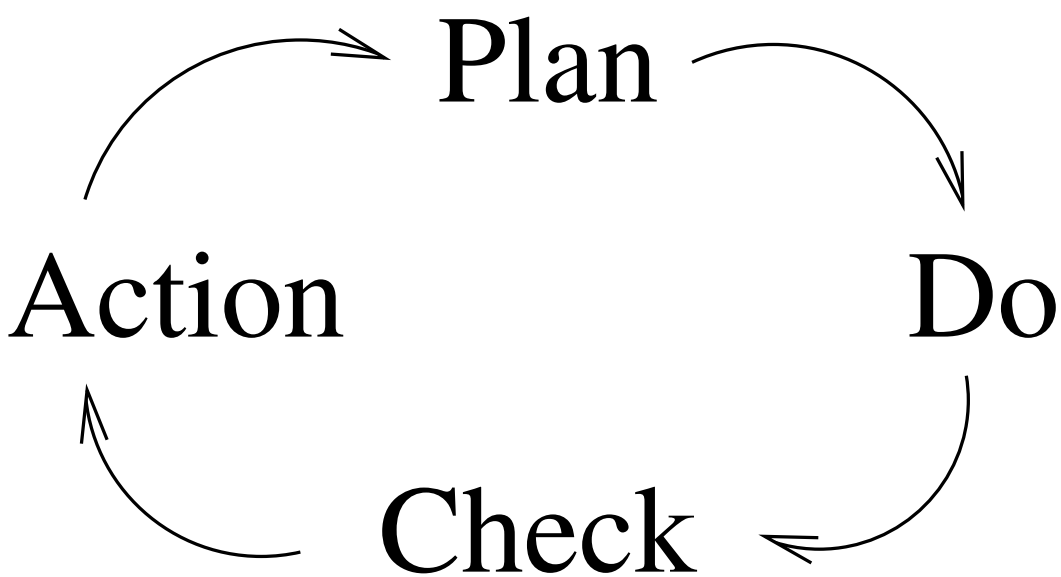
How to audit?
Red wire:

- Target of Continuous System Auditing (CSA) Tools
- Characters of CSA Tools
- Utilization of CSA Tools
- Evaluation of CSA Tools

Target of CSA tools

- Internal Applications
  - Intranet systems
  - Database management
- External Services
  - E-commerce
  - Database management
- Cross-LAN Systems
  - Communication with partners LAN
  - VLANS, C-level domains, ...

Characters of CSA tools



Continuous Auditing as a PDCA-cycle

Utilization of CSA tools

- Available Tools for CSA applications:
  - Nessus (Vulnerability Scan);
  - Snare (Events-driven Auditing);
  - YouRen (Penetration Tests).

Utilization of CSA tools (2)

- Nessus:
  - Structure of Nessus system:
    - Lighting Console
    - Remote scanners
  - Deployment of Nessus:
    - Achieving the system and network information
    - Scanning the system and network vulnerabilities
  - "Duister Corner":
    - CGI enabled
    - System crash possibilities

Utilization of CSA tools (3)

- Snare:
  - Structure of Snare event-log system:
    - Snare Server
    - Snare Agent
  - Deployment of Snare system
    - Remote Installation
    - Events Filter
    - No agent cache
    - Analyzing with "Objectives"
  - Vulnerabilities
    - Logs changed
    - Amounts of data logged
      -

Utilization of CSA tools (4)

- YouRen:
  - Vulnerability Database
  - Password test
  - Host configuration test

Utilization of CSA tools (5)

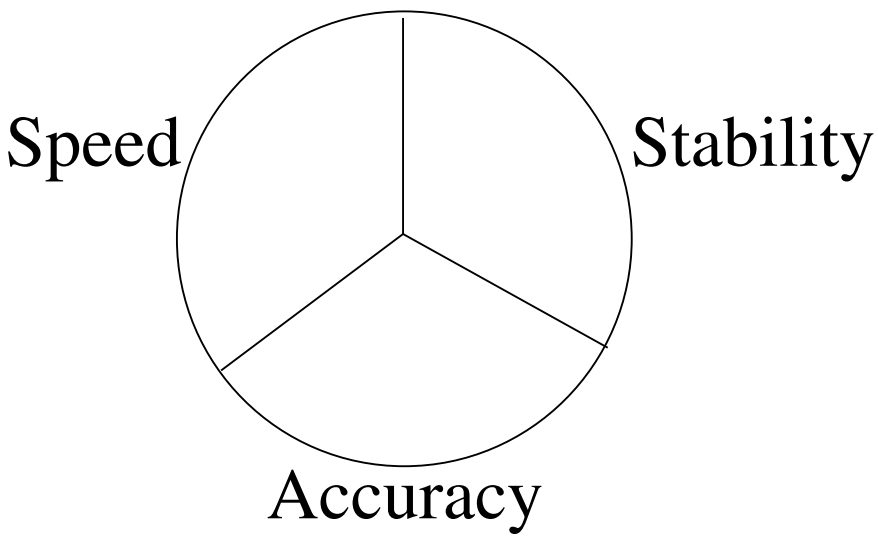
- Main Steps of CSA processes:
  - External network test
    - Remote attack to web servers and so forth
    - Password vulnerability tests
    - Firewall security tests
    - Services vulnerability tests

Utilization of CSA tools (6)

- Main Steps of CSA processes (continued):
  - Internal network test
    - Buffer overflow tests
    - Password security tests
    - Services security tests
  - System optimization through log analysis

Evaluation of CSA tools

- Speed - Accuracy - Stability



Dimensions of Evaluation

Questions?