ห้องทดสอบไวรัสคอมพิวเตอร์สำหรับประเทศไทย

โดย

นาย กิติศักดิ์ จิรวรรณกูล

ศูนย์ประสานงานการรักษาความปลอดภัย
คอมพิวเตอร์ ประเทศไทย (ThaiCERT)

หัวข้อในการบรรยาย

- เหตุผลและความจำเป็น
- วัตถุประสงค์
- โครงสร้างของห้องทดสอบ
- การทดสอบ

เหตุผลและความจำเป็น

- ปัจจุบันมีไวรัสคอมพิวเตอร์ > 70,000 ชนิด
- ผู้ใช้งานมีความรู้และความตระหนักลดลง
- โปรแกรมป้องกันไวรัสของต่างประเทศ
- อาจมีไวรัสในประเทศไทย
- ไม่ทราบวิธีการแก้ไขที่เหมาะสม

วัตถุประสงค์

- เพื่อนำความรู้ที่ได้ประกาศแจ้งเตือนได้ทัน
- เพื่อเป็นศูนย์กลางข้อมูลไวรัสของประเทศ
- เพื่อกระตุ้นให้มีผู้เชี่ยวชาญด้านไวรัสเพิ่มขึ้น
- เพื่อนำความรู้ไปพัฒนาโปรแกรมป้องกันไวรัสของประเทศไทย
- เพื่อจัดตั้งเป็นศูนย์รับแจ้งเหตุร้องเรียนต่อไป

โครงสร้างของห้องทดสอบ

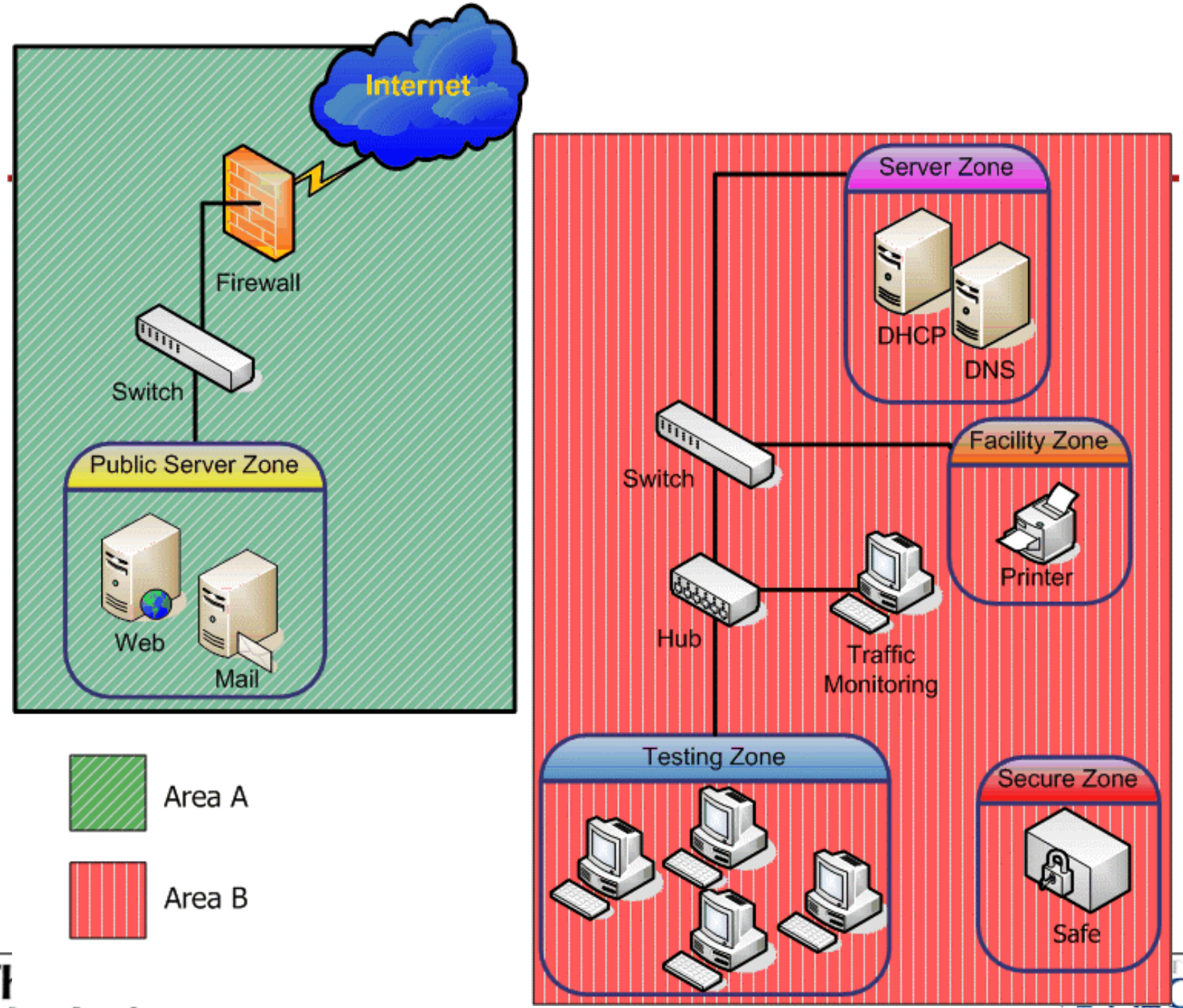
- นโยบายการรักษาความปลอดภัย
- ระบบเครือข่าย
- ระบบทางกายภาพ

นโยบายในห้องทดสอบ

- นโยบายการเข้าถึง
- นโยบายการทดสอบไวรัส
- นโยบายการจัดการกับเอกสาร
- นโยบายการจัดการกับบุคลากร

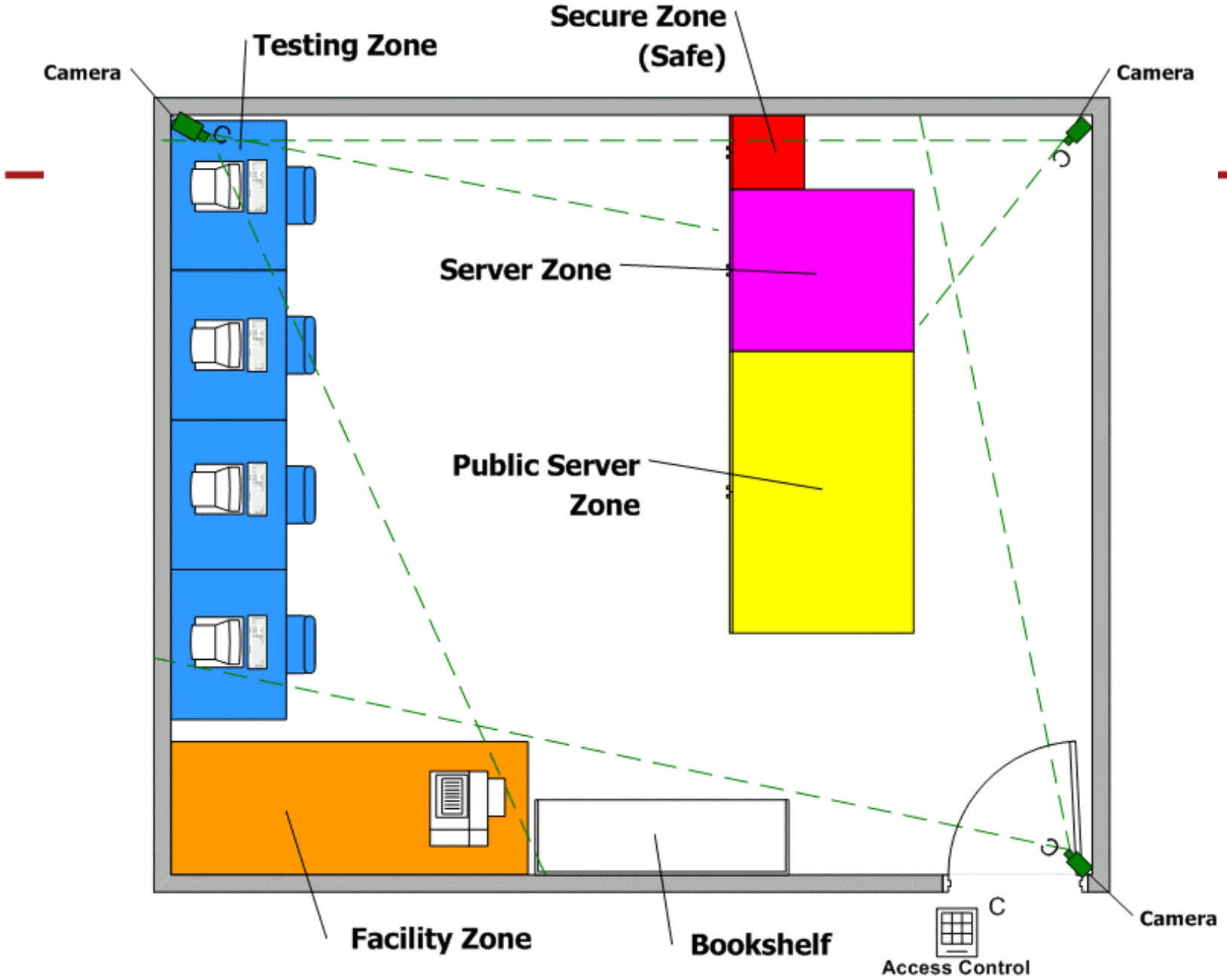
ระบบคอมพิวเตอร์

- Internet Area => พื้นที่สีเขียว
  - Public Server Zone
- Intranet Area => พื้นที่สีแดง
  - Server Zone
  - Facility Zone
  - Secure Zone
  - Testing Zone


Internet
Firewall
Switch
Public Server Zone
Web
Mail
Server Zone
DHCP
DNS
Switch
Facility Zone
Printer
Hub
Traffic
Monitoring
Testing Zone
Secure Zone
Safe
Area A
Area B

ระบบทางกายภาพ

- เข้าออกทางเดียว
- มีคีย์การ์ด
- ระบบสัญญาณไฟเตือน
- ติดตั้งกล้องวงจรปิด
- เครื่องทำลายเอกสาร
- ตู้นิรภัย


Secure Zone
(Safe)
Testing Zone
Camera
Camera
Server Zone
Public Server
Zone
Facility Zone
Bookshelf
Access Control
Camera

แผนดำเนินการ

- วางแผนและร่างนโยบาย
- ติดตั้งระบบ
- ตรวจสอบระบบ
- เขียนคู่มือและจัดอบรม

การทดสอบ

- หนอน W32.Sasser.E.Worm
- เพนเทียม 4 ความเร็ว 2.4 GHz.
- ฮาร์ดดิสก์ SCSI 38 GB
- RAM 1 GB
- ระบบปฏิบัติการวินโดวส์ XP
- โปรแกรมที่ใช้ทดสอบค่าต่างๆ ของเครื่อง

วิธีการทดสอบ

- ศึกษาข้อมูลของหนอน
- เก็บค่าสถานะตั้งต้นของเครื่อง
- รันไฟล์หนอน และเก็บค่าสถานะต่างๆ
- สรุปผลและเขียนรายงาน

สรุปผลการทดสอบ

- ผลการทดสอบที่ได้นั้นค่อนข้างถูก
- แต่ไม่ค่อยปลอดภัยเท่าที่ควร
- ประสิทธิภาพจะเพิ่มขึ้นถ้ามีห้องทดสอบ

คำถาม?