

Security Threats to Schools IT Systems & Long term solution



Mr. Albert Wong
Chairman, Association of IT Leaders in Education (AiTLE)
IT Coordinator & Computer Subject Panel, Lee Kau Yan Memorial School (LKYMS)

Email : albertwong@aitle.org.hk



My background



- A School Teacher (~ 25 years)
- Major : Biology
- Teaching Math, Biol & IS at the first 9 years
- Change to the IT in Education field then
 - School IT Infrastructure
 - Computer subject teaching




My background



- IT Coordinator / Head of IT ... of
 - Kiangsu-Chekiang College
 - Victoria Shanghai Academy
 - Law Ting Pong Secondary School
 - Lee Kau Yan Memorial School
 - serving now
 - School type : Aided, DSS, PIS

My background



- Chairman  **AiTLE**
 - Association of IT Leaders in Education (AiTLE)
 - formed by a group of school IT Coordinators in 2002/2003
 - to promote quality of education through the use of IT
 - in form of peer-sharings, seminars and workshops
 - Now has 1117 members
 - In frequent contact of schools & teachers
 - Through activities
 - Different formats of free consultancy services
 - In frequent contact with vendors/SI & professionals

Security Threats to Schools IT Systems & Long term solution



What schools' IT Systems now commonly have

- Server Room
- IT Office (Technician Room)
- Staff Room
- General Office
- Classroom & Special Room
- Open Area

Schools' IT Systems @ Server Rm

- Domain Controller
 - PDC, BDC
- WebSAMS
 - HTTP Server
- File Server
- Web Server
 - Apache, IIS
 - HTML based ?
 - Package (WP, J) ?
- Intranet Server
- Email Server
- ESDA Server
- Library Server
- Inventory Server
- OMR Server
- Print Server
 - Centralized printing
- Fax Server
- Proxy Server

Schools' IT Systems @ Server Rm

- IP Phone Server
- Octopus Server
- Servers related to school-based project
- Routers
- Switches

Schools' IT Systems @ Server Rm

- Server OS
 - Windows
 - Linux
 - Mac

Security Threats to Schools IT Systems

- Server Room — External Hacking
- IT Office (Technician Room) — 無間道
- Staff Room — 唔
- General Office — 唔
- Classroom & Special Room — Internal Hacking
- Open Area — Internal Hacking

Security Threats to Schools IT Systems : Server Room

External Hacking

- Server Room

- Technologies moving too fast
- Many need on phishing agent




- Experience sharing

- Server response slow
 - Call to support :
 - Checked
 - Frequent communication with 120.209.156.170



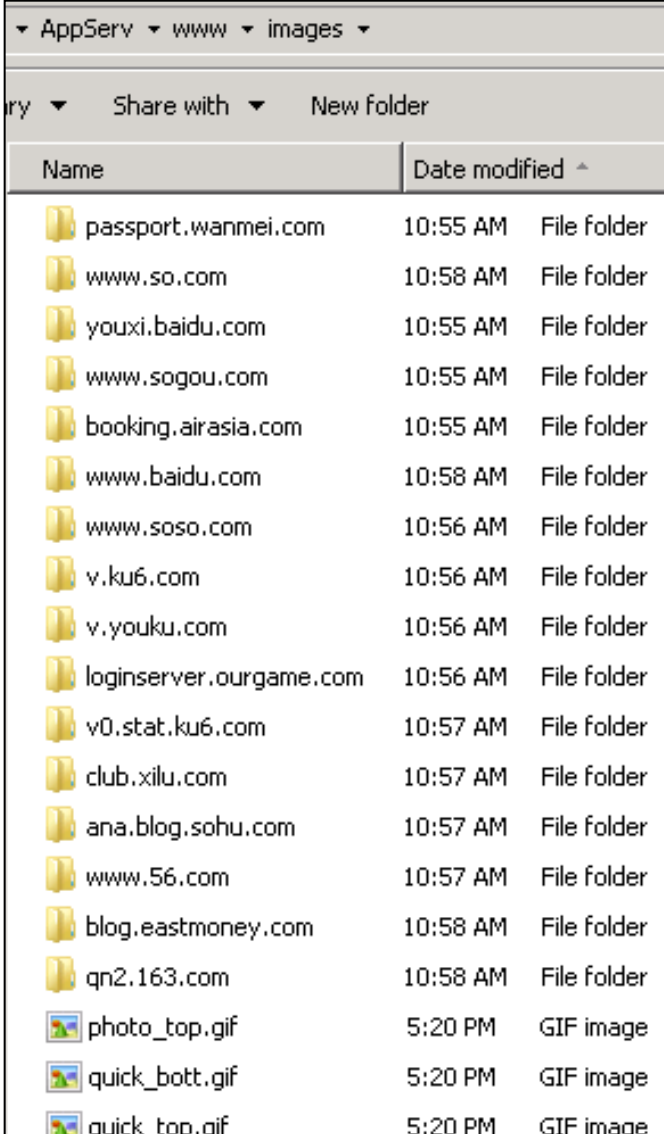
Security Threats to Schools IT Systems : Server Room

- Experience sharing
 - Once you are being infected
 - How to solve ???

IP Address:	 [IP Lookup]
Hostname:	
IP Location:	Central District - Hong Kong (HK) 
ISP:	Hutchison Global Communications
Organization:	Hutchison Global Communications
IP Blacklist Check:	<div style="border: 1px solid black; padding: 5px;"><p>Status: Suspicious Threat Level Score: 36 (on the scale from 0 - 255) Last Known Activity: 3 days ago</p></div>

Security Threats to Schools IT Systems : Server Room

- Experience sharing
 - A web server with ‘auto’ folders creation
 - Once you are being infected
 - How to solve ???



Name	Date modified	Type
passport.wanmei.com	10:55 AM	File folder
www.so.com	10:58 AM	File folder
youxi.baidu.com	10:55 AM	File folder
www.sogou.com	10:55 AM	File folder
booking.airasia.com	10:55 AM	File folder
www.baidu.com	10:58 AM	File folder
www.soso.com	10:56 AM	File folder
v.ku6.com	10:56 AM	File folder
v.youku.com	10:56 AM	File folder
loginserver.ourgame.com	10:56 AM	File folder
v0.stat.ku6.com	10:57 AM	File folder
club.xilu.com	10:57 AM	File folder
ana.blog.sohu.com	10:57 AM	File folder
www.56.com	10:57 AM	File folder
blog.eastmoney.com	10:58 AM	File folder
qn2.163.com	10:58 AM	File folder
photo_top.gif	5:20 PM	GIF image
quick_bott.gif	5:20 PM	GIF image
quick_top.gif	5:20 PM	GIF image

Security Threats to Schools IT Systems : Server Room

- It is lucky that if the hacking make your system (you) alert !
- How about if it is not !!!

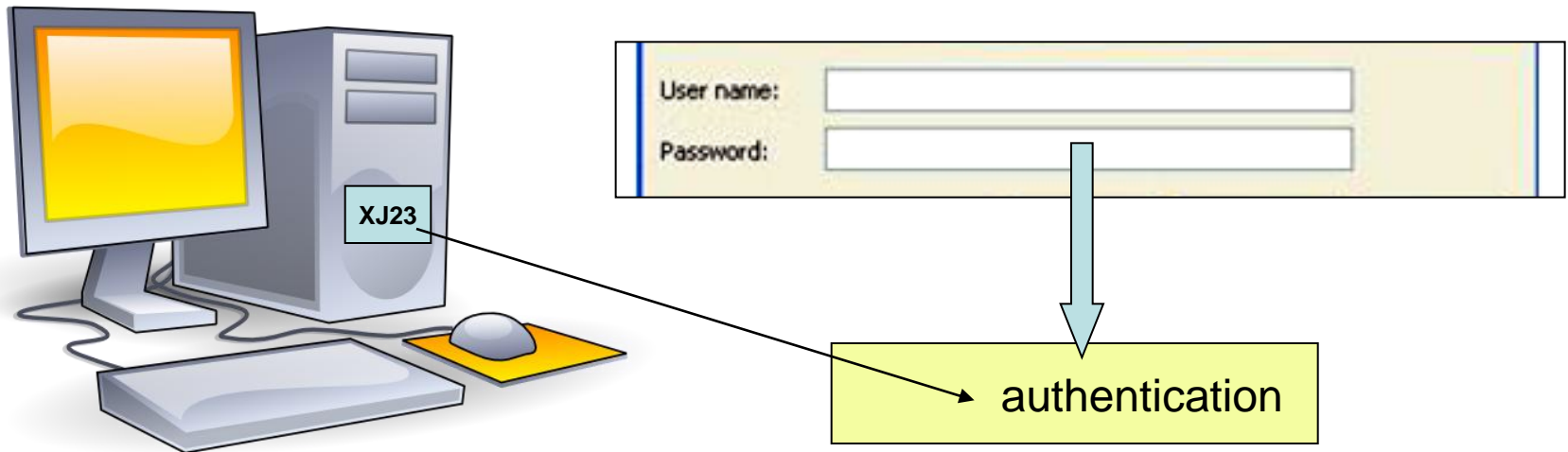


Security Threats to Schools IT Systems : Classrooms / Special Rooms / Open Area

- Can your school domain access password be kept securely ?
- Can your school WiFi key be kept securely ?
- Can kept securely for ?? hour(s) ???

Security Threats to Schools IT Systems : Classrooms / Special Rooms / Open Area

- Experience sharing
 - Login password for school computer in Classroom



Security Threats to Schools IT Systems : Classrooms / Special Rooms / Open Area

- Reason behind



Image Source : <http://www.earthbeforeflood.com/images/faces.jpg>; http://s1.hubimg.com/u/6525456_f520.jpg

Security Threats to Schools IT Systems : Classrooms / Special Rooms / Open Area

- Technology advancement and affordable price



Security Threats to Schools IT Systems : Staff Room / General Office

- 一個字開頭：「唔
- Numerous cases
- Numerous types of devices
- Numerous types of systems
- Numerous types of applications
- Numerous types of understandings

Your personal files are encrypted!



Private key will be destroyed on
9/13/2013
5:27 AM

Time left
71 : 19 : 53

Your important files **encryption** produced on this computer: photos, videos, documents, etc. [Here](#) is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a **unique** public key **RSA-2048** generated for this computer. To decrypt files you need to obtain the **private key**.

The **single copy** of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will **destroy** the key after a time specified in this window. After that, **nobody and never will be able** to restore files...

To obtain the private key for this computer, which will automatically decrypt files, you need to pay **300 USD / 300 EUR / similar amount** in another currency.

Click «Next» to select the *method of payment* and the *currency*.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Next >>

Security Threats to Schools IT Systems : Staff Room / General Office

- 小心勒索軟件「**CryptoLocker**」陷阱
 - https://www.hkcert.org/mobile_url/zh/blog/13101102
 - Once infected, the malware encrypts
 - not only the files located in the affected machines,
 - but also the files shared on the network drive connected

Security Threats to Schools IT Systems :

Staff Room / General Office

- After the files are encrypted
- the malware creates a popup to request for ransom money (around 300 USD or 300 EUR or 2 BitCoin)
- It also threaten the victim to pay in a limited time, otherwise the only key used to decrypt the files will be deleted.

Facing these security threat

- Is it the ability / responsibility of
 - A teacher
 - Non computer graduate
 - Or even a computer graduate

Facing these security threat

Curriculum

The curriculum is composed of a set of highly focus core courses and a wide range of electives.

solving and a
communicati
spectrum inc
computer gra
provide broa

The main su

- Comp and c
- Algor skills design
- Softw design and synthesis, database design and management, and understanding of social, ethical and professional issues.
- Seminar Series -- keeps the students abreast of the latest development in technology and market trends and to introduce students to a research culture in the early years of study. Outside scholars, IT professionals, and hardware / software vendors will be invited as guest speakers or honorary lecturers.
- English Communication Skills to enhance language proficiency and presentation skills of the students.

The main subject areas are :

- Computer Systems
- Algorithm Design and Analysis and Mathematics
- Software Engineering
- Seminar Series (latest development in technology and market trends)
- English Communication Skills

BSc in Computer Science

- › Aims
- › Curriculum

Description

Degree/Major Requirements
Study Plan

- › Admissions
Direct/Non-JUPAS
HKDSE
- › Contact Us

Minor in Computing

MSc in Computer Science

MSc in Electronic Commerce

PGC in Information Security

Master of Philosophy / Doctor
of Philosophy

Useful Links

- › [Job Vacancies](#)
- › [Robocode](#)
- › [CityU CS Programming](#)

Info source : <http://www.cs.cityu.edu.hk/academic/bsscs/curriculum/description.html>

Facing these security threat

- Is it the ability / responsibility of
 - A teacher
 - Or a TSS
 - Especially in an era that we need many IT professionals

Solution

- TSS 常規化
 - Providing scaled salary to TSS
- SMTC
 - Server Migration to Cloud

Solution

- TSS 常規化
 - Providing scaled salary to TSS
 - Consider
 - Number of TSS that school can afford
 - Still handling school IT works
 - Plus security issue
 - Effect to TSS
 - Personal development
 - Effect to School
 - TSS Eagerness to work

Solution

- SMTC
 - Server Migration to Cloud
 - Migrating the Servers in Server room to cloud
 - Subscribe Managed IT Services
 - Help to manage PC / equipment status of school
 - Let Teachers back to teaching work
 - Lower TSS loading

Solution

- SMTC
 - Server Migration to Cloud
 - AiTLE is work on this project
 - AiTLE project before
 - WaaSchool (WiFi as a Services ~~ subscription)
 - If you are interested, join as a pilot
 - Discuss specification
 - Recruit interested vendor / SI
 - Provide free trial from vendor / SI
 - Provide feedback from school
 - Calculate budget and discuss with EDB

Thank You !