COS30015 – Lab 9

Authentication & Encryption

Presented by Jamie Ooi

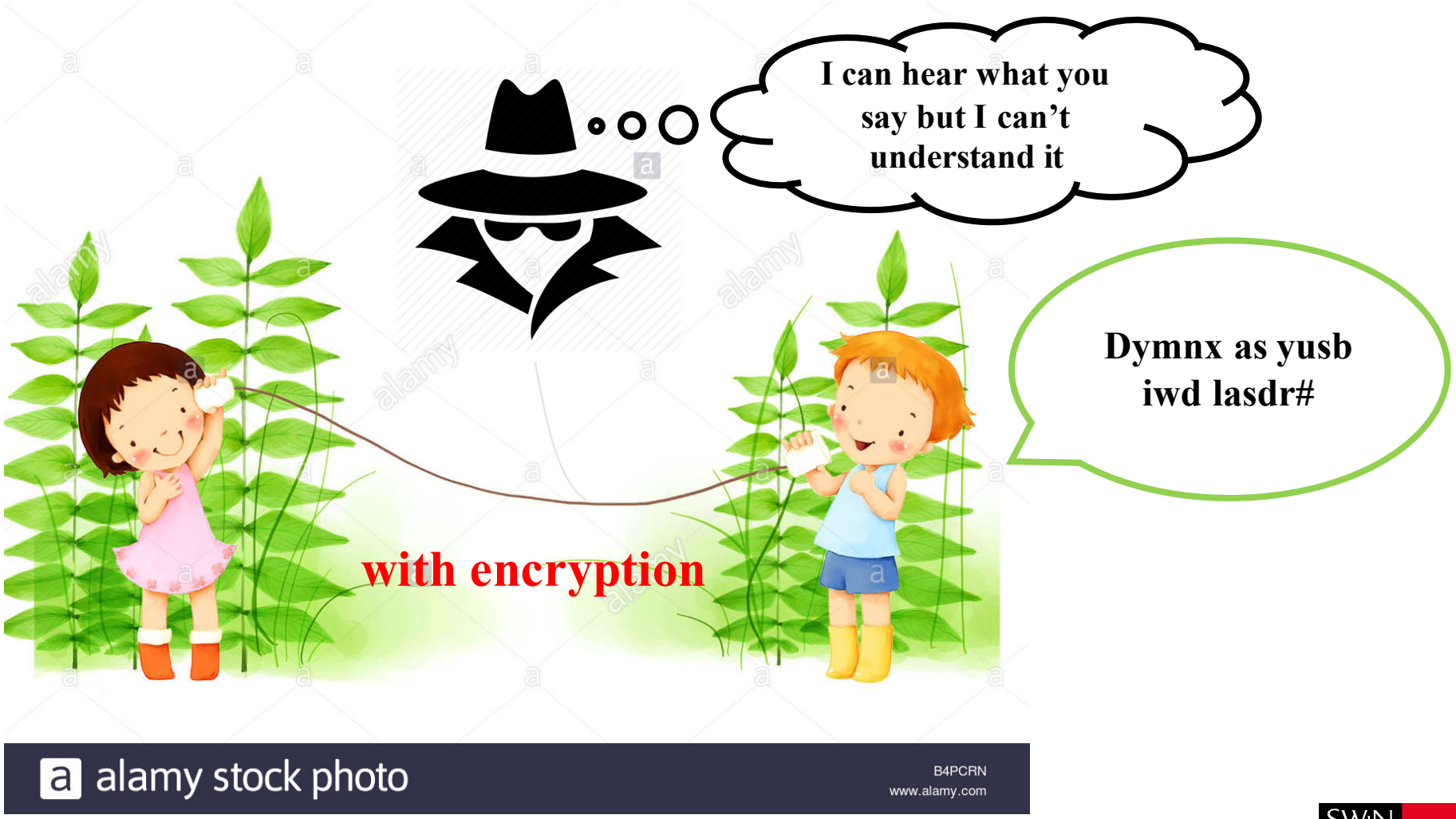
jooi@swin.edu.au

Thursday 6 October, 2022

SWINBURNE UNIVERSITY OF TECHNOLOGY

Man-in-The-Middle Attack (MiTM) Explained

Man-in-The-Middle Attack (MiTM) Explained



Common Types of MiTM Attacks

- **ARP (Address Resolution Protocol) Spoofing**
  Fundamental to networking – MAC Address to IPv4 Address

- **DNS (Domain Name System) Spoofing**
  Internet phone book – hostname to IP address

- **LLMNR (Link-Local Multicast Name Resolution) Poisoning**
  Domain name to IPv4 or IPv6 when DNS isn't available

- **NBT-NS (NetBIOS Name Service) Poisoning**
  NetBIOS name to IP address when DNS isn't available

ARP Poisoning Explained

ARP Poisoning

Useful Tools for MiTM Attacks

- **Responder (made by Trustwave SpiderLabs)**
  https://github.com/SpiderLabs/Responder
  LLMNR, NBT-NS, MDNS Poisoning
  CLI tool

- **Cain and Abel**
  https://en.wikipedia.org/wiki/Cain_and_Abel_(software)
  More commonly known for it password recovery functionality
  Performs MiTM attack and then cracks passwords
  Has a graphical user interface

- **Ettercap (available in Kali)**
  https://github.com/Ettercap/ettercap
  Able to perform various MiTM poisoning attacks
  CLI tool

COS30015 IT Security – Lab 9 Background

Four Virtual Machines

CySCA2014InABox (VM)
Kali (VM)
RedHat Linux (VM)
Windows XP Control (VM)
A computer with internet access

SWINBURNE UNIVERSITY OF TECHNOLOGY

Questions ?

Email: jooi@swin.edu.au
Linkedin: https://www.linkedin.com/in/jamie-ooi-15297b98/

Thursday 6 October, 2022