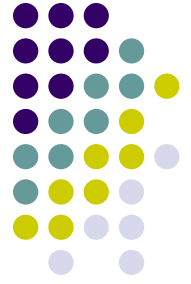




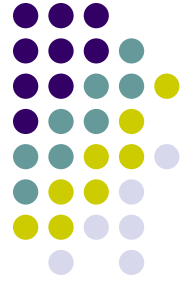
# IT Security: Protecting Data & Systems against the Realities of a Global Society



# Topics

- Quick description of PHFE-WIC
- Do I need security? I am just WIC!
- Overall Security Design Philosophy
- Two examples

# PHFE WIC



- California Local Agency
- 700 employees, 63 locations – Los Angeles area
- 330,000 enrolled individuals in our local agency
  
- 46 Servers, 74 firewalls/routers, 750 workstations
- Software development, 15 systems developed
  - Support several multi-agency applications
  - Support a state wide grocer application



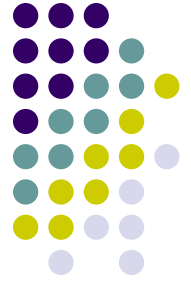
# How bad is the threat?

- Automated attacks are COMMON
- Threats
  - Use your system to attack others
  - Porn storage
  - Identity theft
  - Vandalize (for fun)

**16 days shown in log,  
11 had attack  
6/13 attack lasted an hour**

Name	Size	Date Modified
ex090612.log	28,841 KB	6/13/2009 12:01 AM
ex090611.log	2,319 KB	5/12/2009 12:00 AM
ex090610.log	320 KB	6/11/2009 12:02 AM
ex090609.log	1 KB	6/10/2009 12:02 AM
ex090603.log	320 KB	6/4/2009 12:02 AM
ex090602.log	6 KB	6/3/2009 12:02 AM
ex090601.log	1 KB	6/2/2009 12:02 AM
ex090529.log	322 KB	5/30/2009 12:02 AM
ex090528.log	2 KB	5/29/2009 12:01 AM
ex090527.log	13 KB	5/28/2009 12:02 AM
ex090526.log	214 KB	5/27/2009 12:00 AM
ex090525.log	1 KB	5/25/2009 10:24 AM
ex090524.log	1,058 KB	5/25/2009 12:03 AM
ex090523.log	13,130 KB	5/24/2009 12:00 AM
ex090522.log	1 KB	5/23/2009 12:02 AM
ex090521.log	4 KB	5/22/2009 12:01 AM

# Top 20 Internet Security Problems



## Client-side Vulnerabilities in:

- C1. Web Browsers
- C2. Office Software
- C3. Email Clients
- C4. Media Players

## Server-side Vulnerabilities in:

- S1. Web Applications
- S2. Windows Services
- S3. Unix and Mac OS Services
- S4. Backup Software
- S5. Anti-virus Software
- S6. Management Servers
- S7. Database Software

## Security Policy and Personnel:

- H1. Excessive User Rights and Unauthorized Devices

- H2. Phishing/Spear Phishing

- H3. Removable Media

## Application Abuse:

- A1. Instant Messaging

- A2. Peer-to-Peer Programs

## Network Devices:

- N1. VoIP Servers and Phones

## Zero Day Attacks:

- Z1. Zero Day Attacks

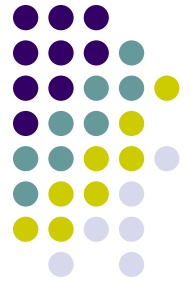
Slide 5

---

m1

mikew, 10/31/2009

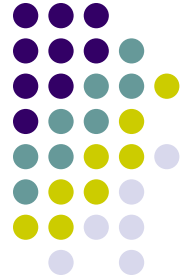
# Example 1: Minimize PCs



- PCs are very exposed
- Need virus checkers and updates
- Have personal information on them
  - Usually not backed up, may be stolen
- Can become infected and used as a basis for other attacks
  
- *Move back to paper and pencil?*

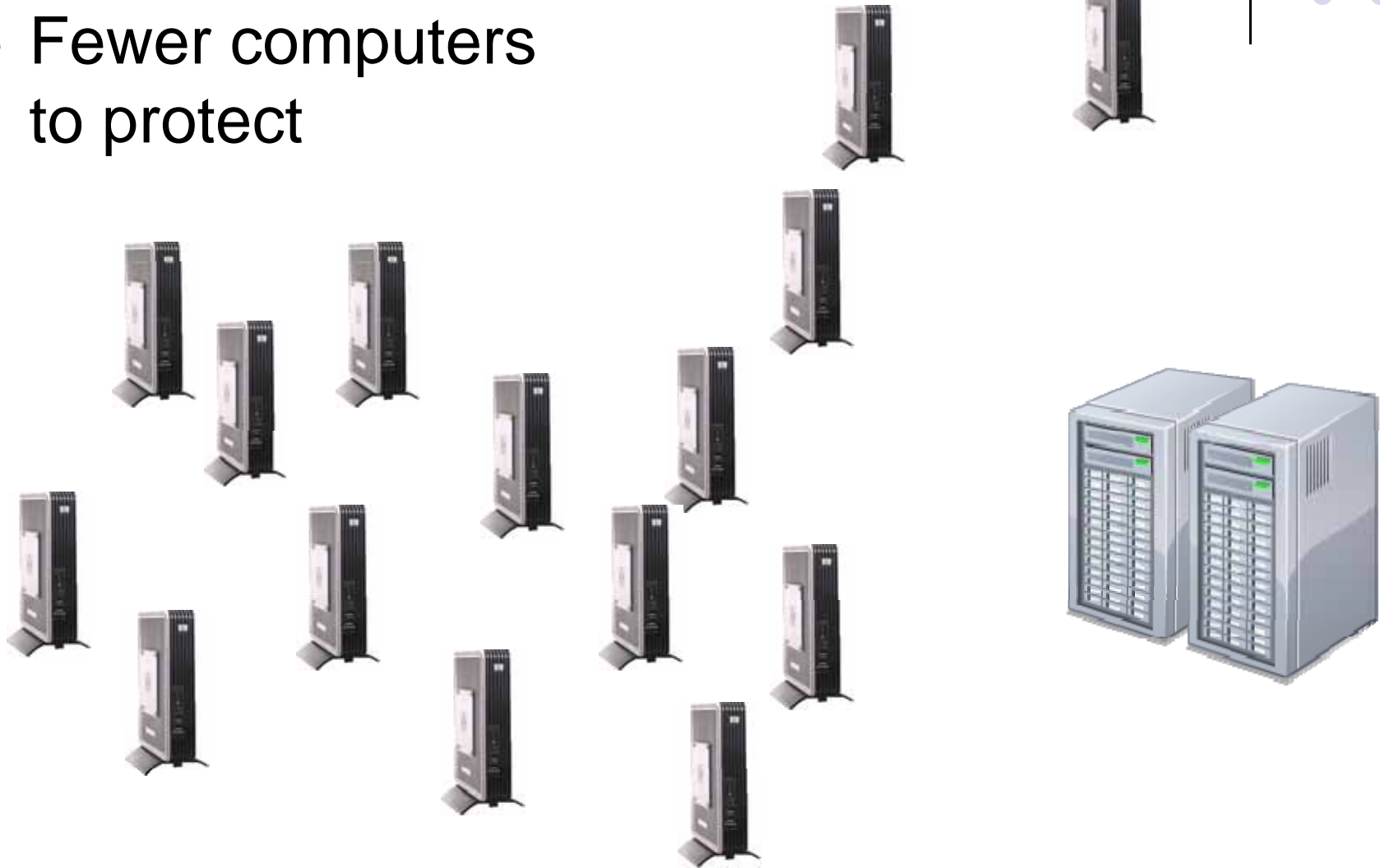
# How to avoid PCs

- Of 700 employees only 6 have PCs
  - Tremendous lines!
- Thin Client technology (modern “dumb terminal”)
  - “PC” with write protected memory
  - No hard drive
  - No Word, no Excel, few local products
    - No installing security patches and updates
  - No virus checkers - TC’s can’t be infected
  - No registry corruption
  - *Employees have access to all the software they need*
- with Citrix: benefits
  - Install and protect Microsoft Office just on servers
    - *Protect 10 servers VS 700 PCs?*
    - *Maintain 10 virus checkers*
    - *Install / patch MS Office 10 times*



# Thin Client Architecture

- Fewer computers to protect

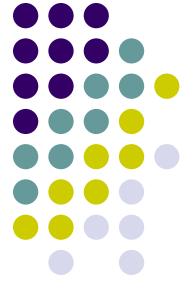


# User Experience?

- Users have Word, Excel, Outlook just like PC users
  - Desktop icons or Start button
  - Applications faster
- No C: drive
  - So files are always backed up and secure
- Do have speakers, can watch video
- Thin Clients are more reliable than PCs
  - If something fails just swap the box
- Get new versions of software and fixes faster
  - We install on 10 servers and everyone has the new software

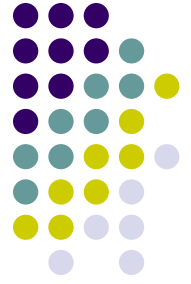


# Example 2: Protect Your Web Applications!

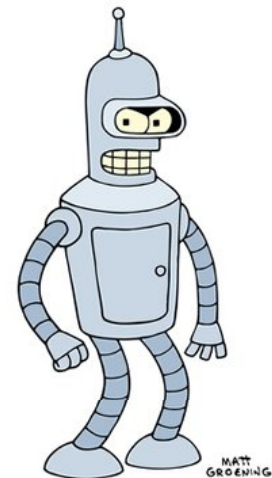
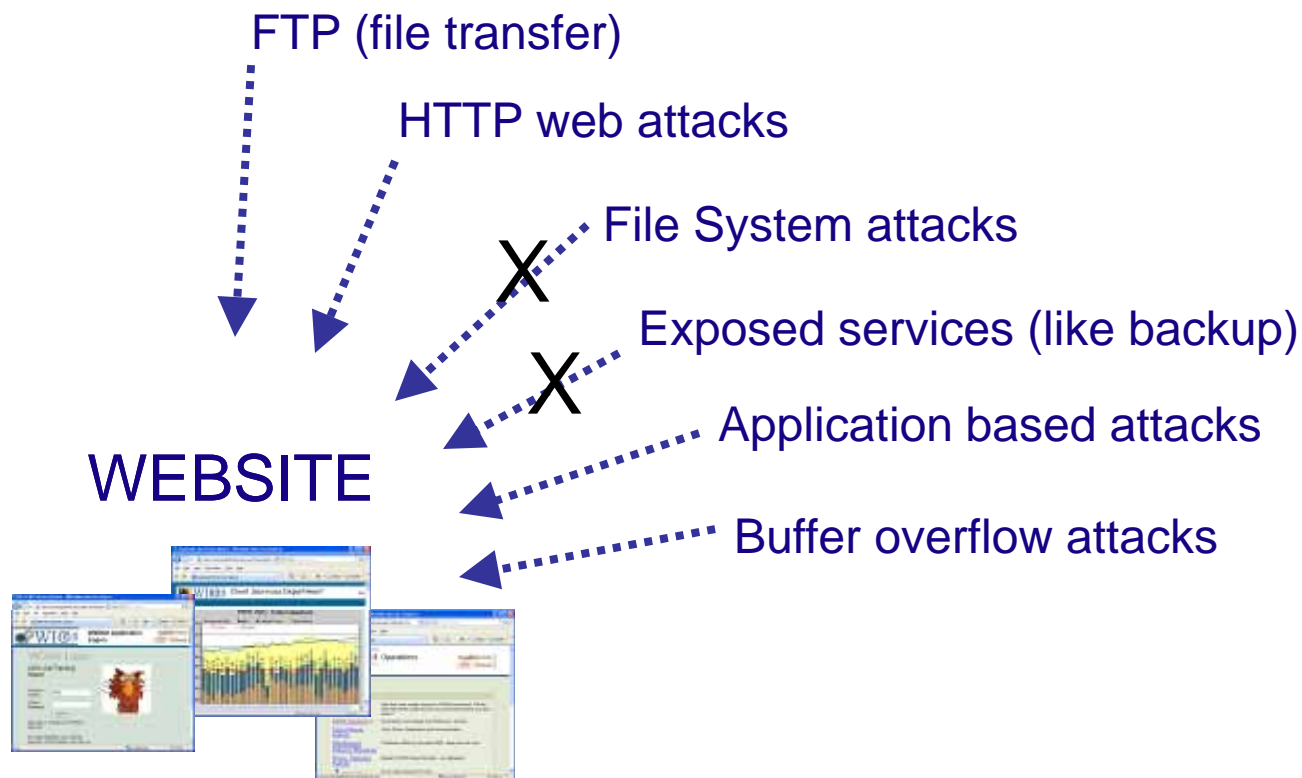


- Public websites, especially your web applications
  - Company email
  - Company applications over the Internet
    - For your customers or employees
    - Online WIC education will be coming
- WIC MIS System over the internet?

# Public Web Applications are a Risk



- Misconfigured servers and applications coding errors
- Firewalls help, but you let some of this traffic through!

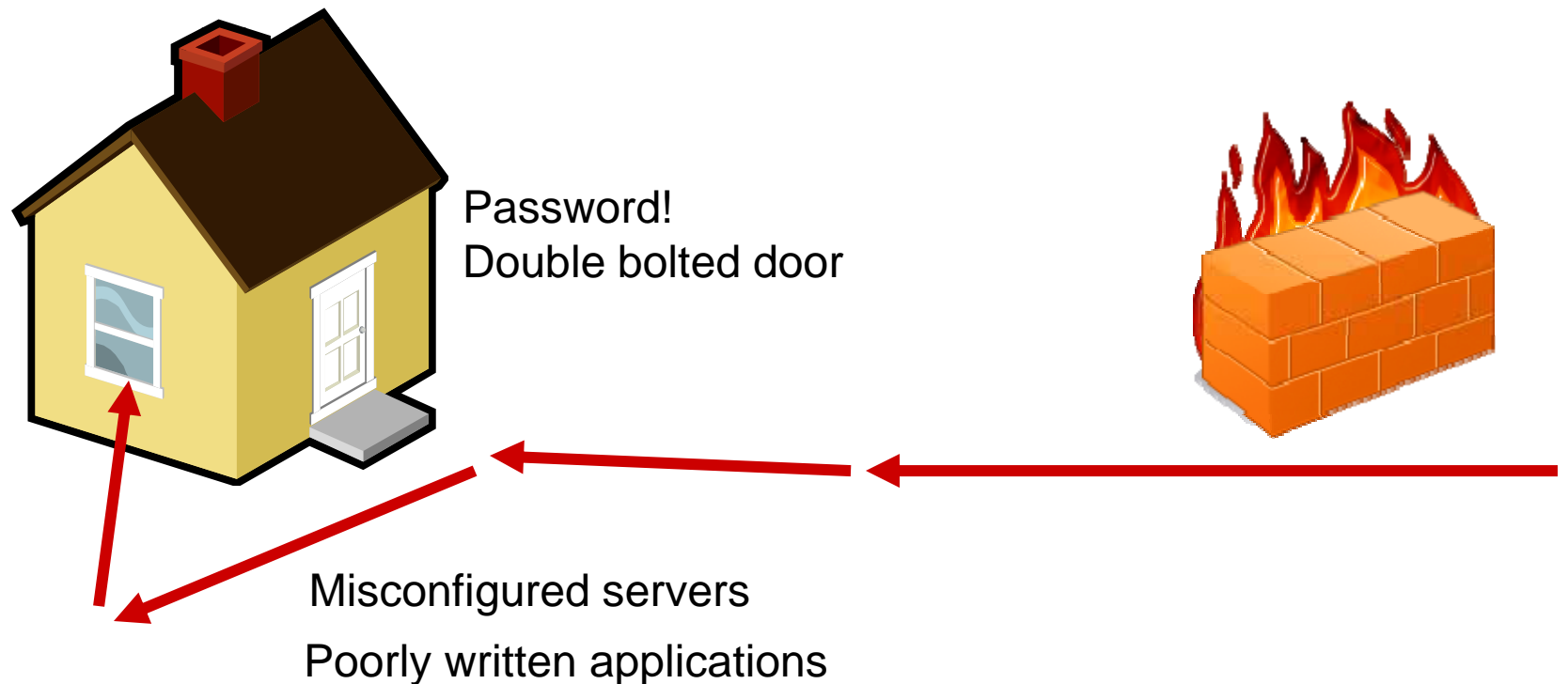


*Apollo astronaut story*

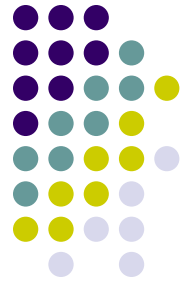


# Protecting your web applications

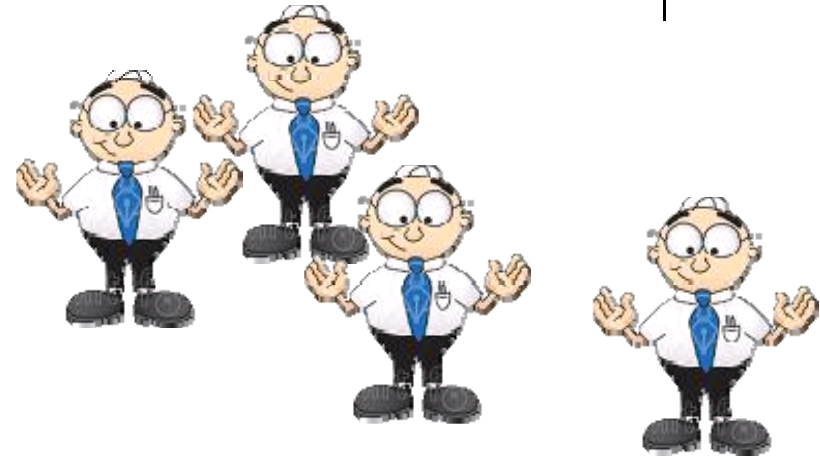
- You have a logon required and firewall



# How to protect your website?

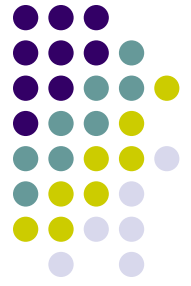


- Hire lots of security professionals to keep up with things
- Frequently patch your servers/firewalls...
- Review all your web application code with experts
- Read security problem flashes from vendors ...

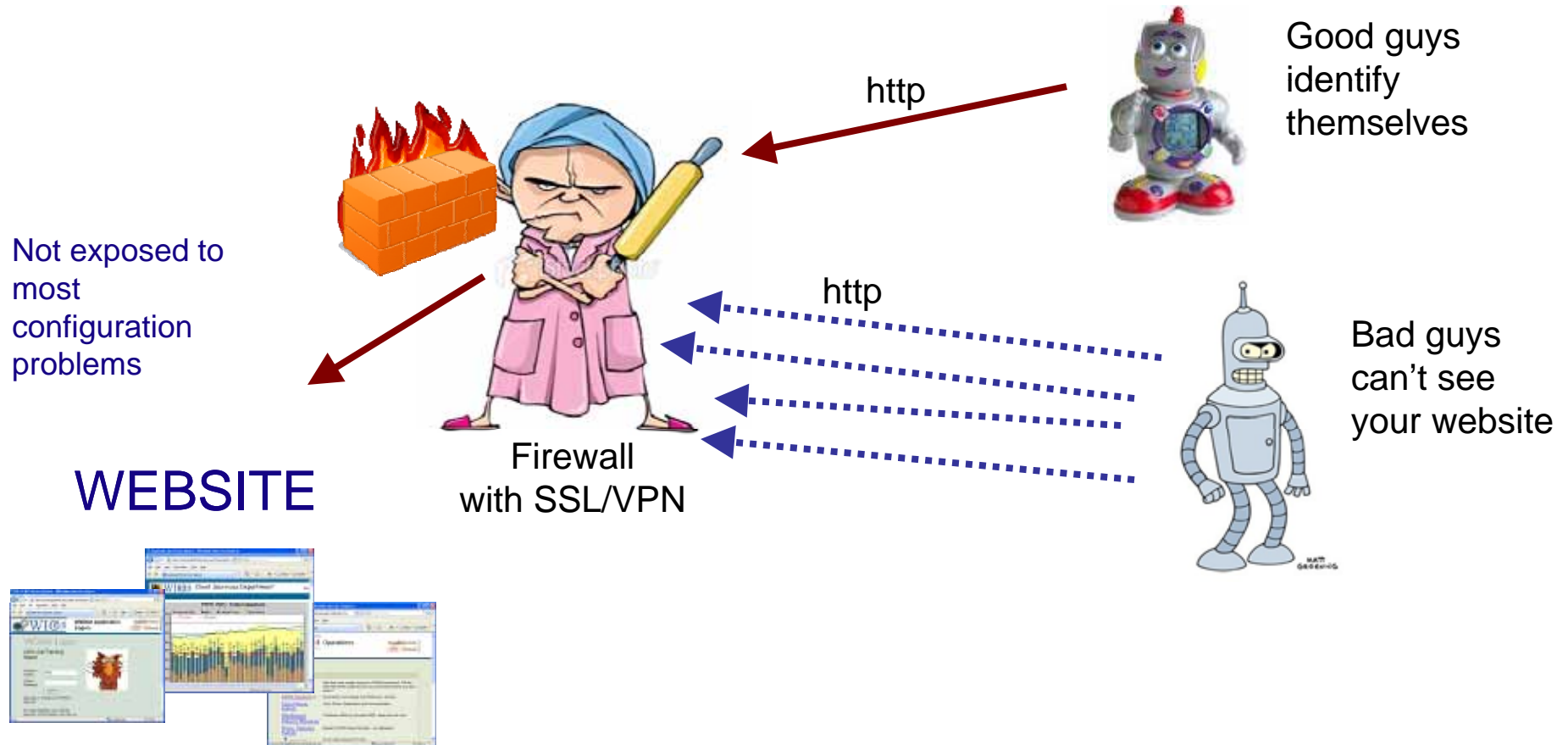


*And hope all your vendors are doing this as well!*

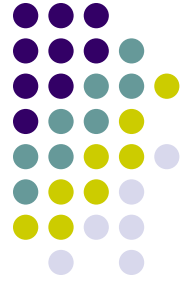
# Don't allow people to access your public web applications!



- SSL/VPN – must logon to firewall BEFORE you can connect to server/applications/website.



# SSL/VPN



- Not as exposed to poorly written applications and misconfigured servers



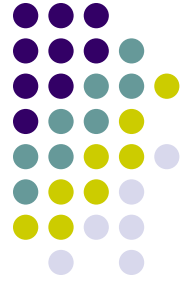
Password!  
Double bolted door



Password!  
Double bolted door



# SSL/VPN - Productivity



- Maintain VPN firewall device
  - Not all servers and web applications
- Reduces exposure to server and application errors



Internet Explorer provided by Dell

Google

File Edit View Favorites Tools Help

https://wicaps.phfewic.org/+CSCO+/logon.html?reason=1

# WiCAPS

PHFE-WIC Applications

**Login**

Please enter your logon id and password.

Logon ID:

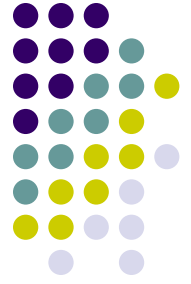
Password:

Done

Internet | Protected Mode: On

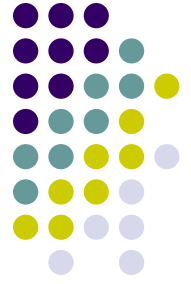
100%





# SSL/VPN is not VPN

- SSL/VPN requires nothing installed on the clients PC or laptop
- No trouble calls to your help desk
- No VPN configuration upgrades
- Lot's of manufacturers sell SSL/VPN
  
- If you roll out an application to 800 users...
  - Nothing for them to install on their PCs
  - VPN requires PC installs and updates



# Summary

- Can't keep up with security.
- Limit the devices which are risky
- Exploit technology to prevent common problems
  - *Dump PCs!*
  - *Implement SSL/VPN*