Vulnerability Assessment: Viewing Your Network From a Hacker's Perspective

State of Illinois

Central Management Services

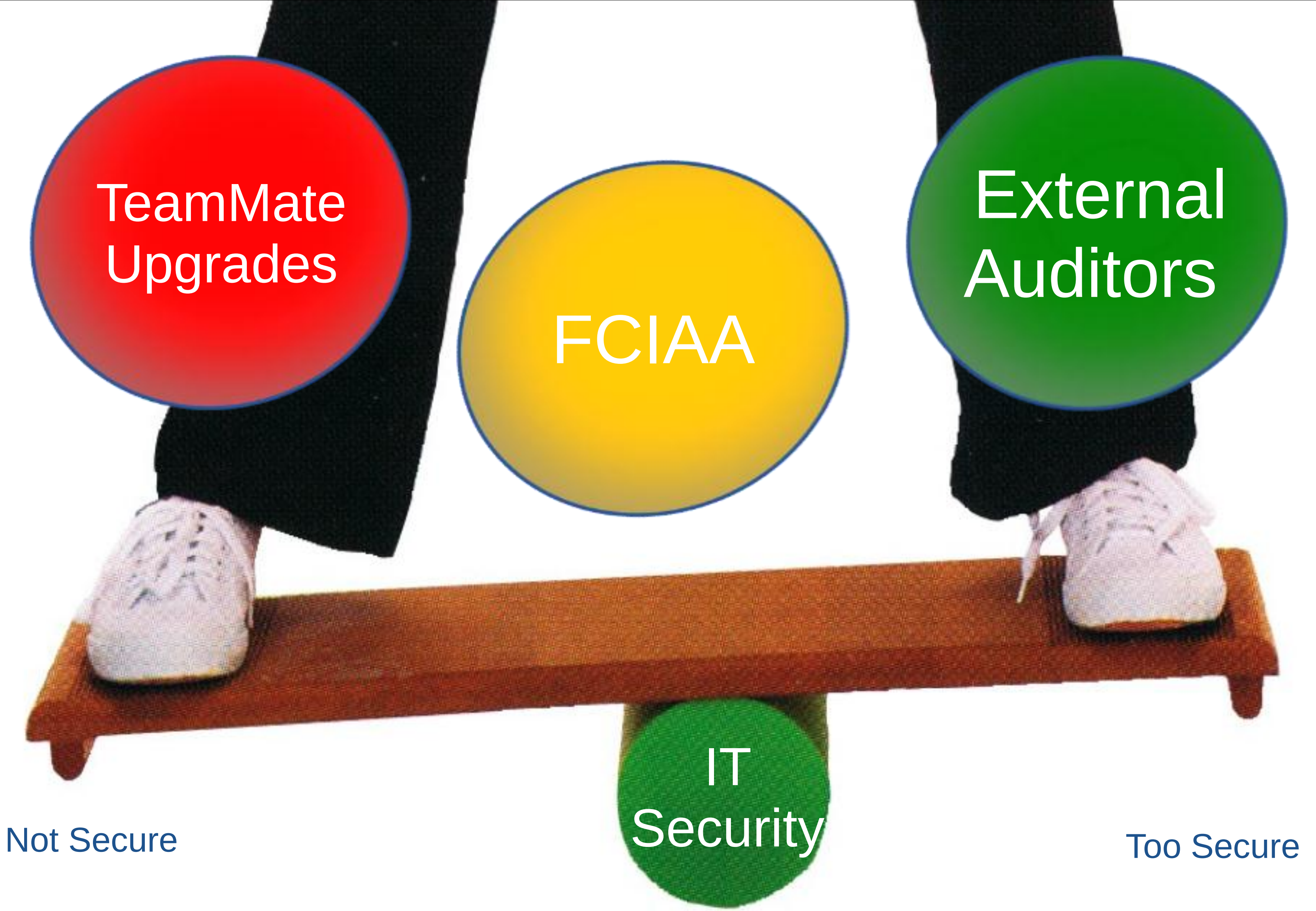
Purpose and Scope

- To present a best practice approach to auditing your servers
- To present real life examples of vulnerability assessment successes
- To present hacker techniques in plain terms

Legal Disclaimer

- Don’t try this at home
- Get written permission before trying any of these techniques
  - The main difference between a security admin and a hacker is permission

Juggling Tasks



TeamMate Upgrades

FCIAA

External Auditors

IT Security

Not Secure

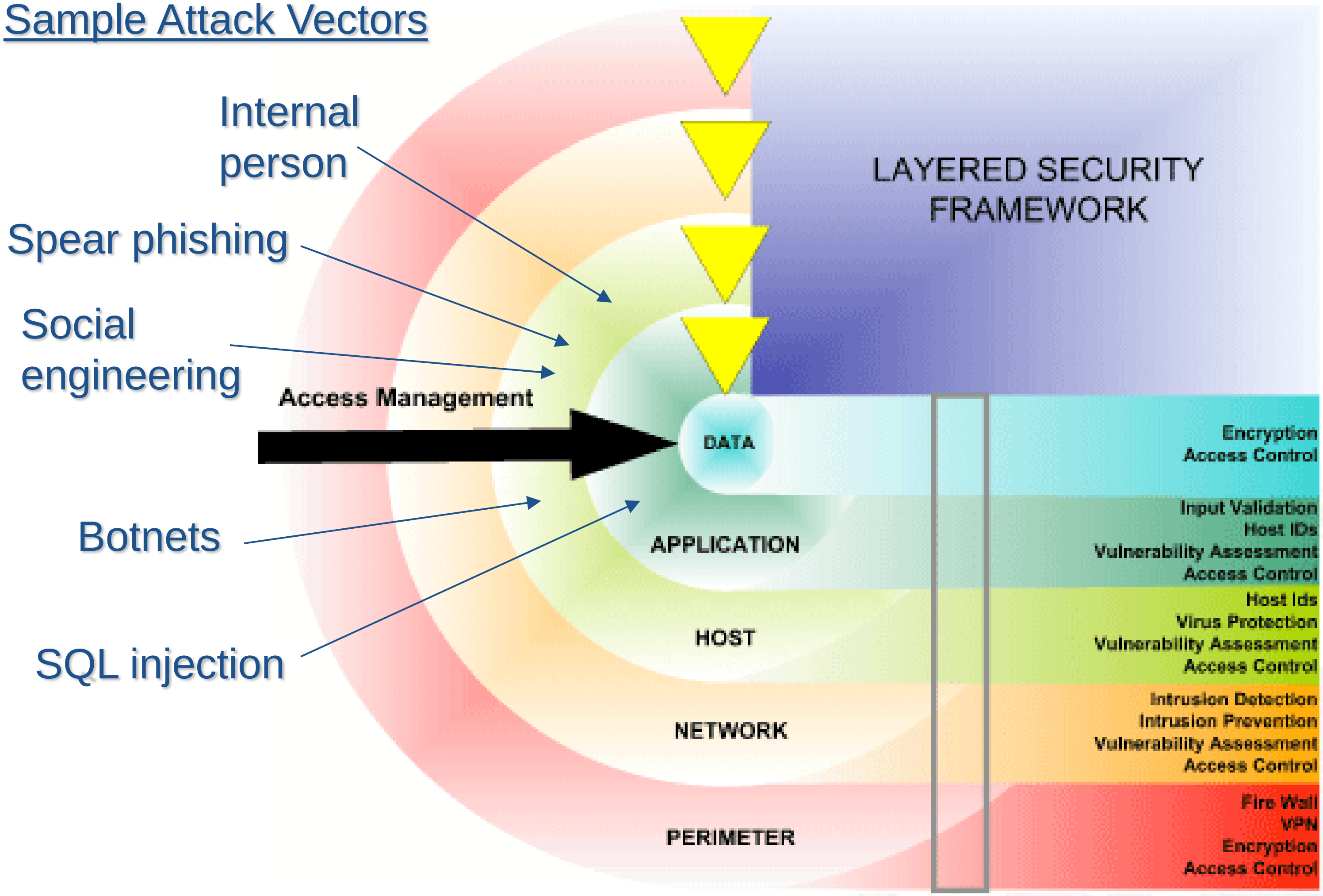
Too Secure

Owasp Top Threats 2013

1. Injection: SQL, OS & LDAP
2. Authentication
3. Cross-Site Scripting
4. Insecure Direct object references
5. Misconfiguration
6. Sensitive Data Exposure
7. Cross-Site Request Forgery
8. Components with Known Vuln’s
9. Unvalidated Redirects

Layered Security

Sample Attack Vectors



Internal person

Spear phishing

Social engineering

Botnets

SQL injection

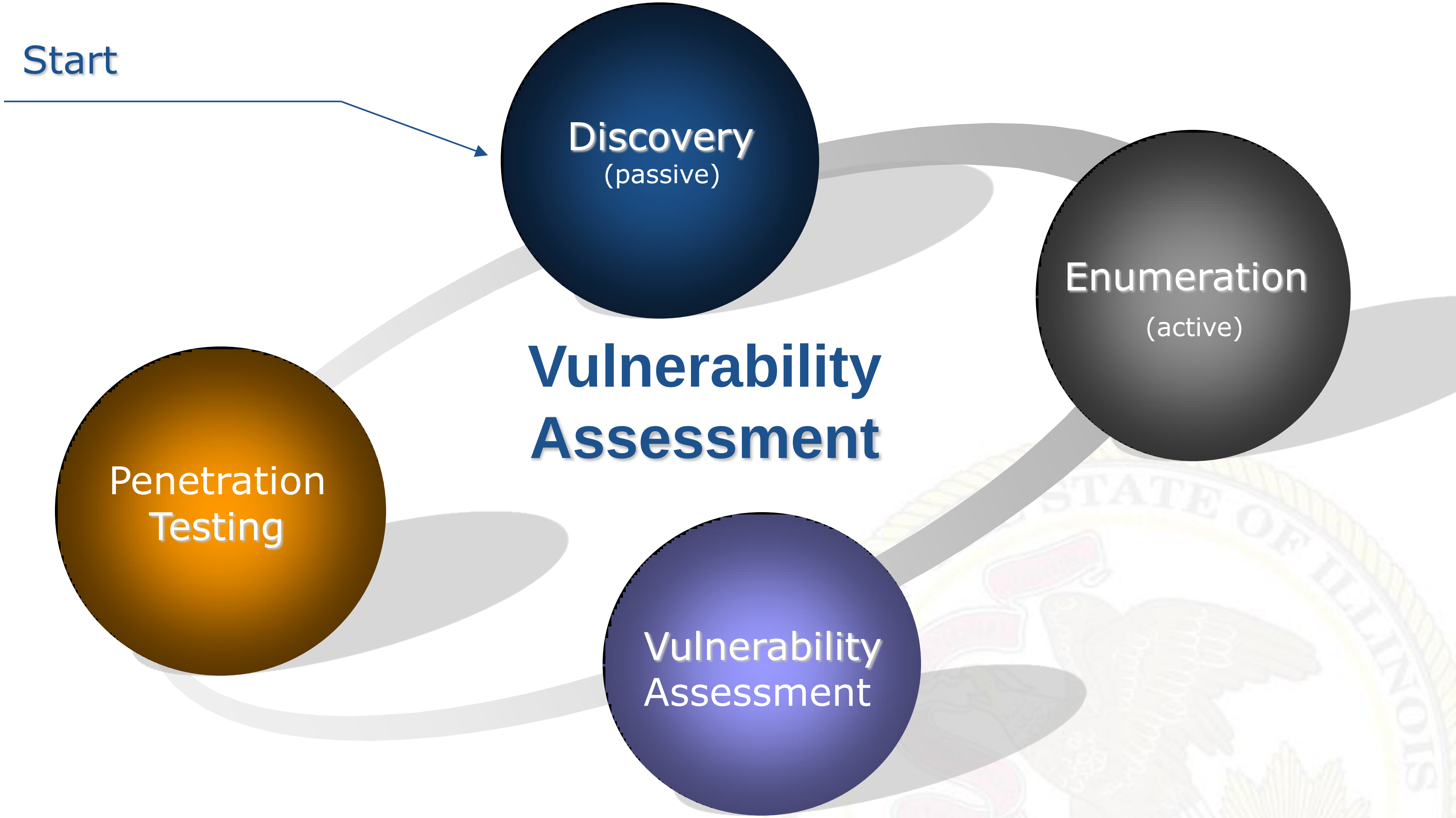
Return on Investment

- 2006 Illinois breach notification law
- Average cost to notify per identity compromised?

  $14 - 90
- Black market value of your identity?

  $2
- What is the return on investment for proactive security?
  - ROI spreadsheet

Testing Methodology



Discovery

- Internet registrar search (http://whois.net)
- General company research (Google, etc.)
- Dumpster diving
- Archive.org
- Newsgroups
  - Techs posting questions
- Job postings
  - Specific software used

Discovery – Google hacking

- Password site:yoursite.com
- Filetype:doc site:yoursite.com classified
- Robots.txt site:yoursite.com
- Intitle:index.of “parent directory” site:yoursite.com

Enumeration

- Ping sweeps / port scanning
- Banner grabbing (telnet ip port)
- Fingerprinting
- MSN virtual hosts search (ip:address)
- Directory Structure
  - Default directories: /admin /secure /adm
  - Backup files: /.bak /backup /back /log /archive
  - Include files: /include /inc /js /global /local

Enumeration

- Common files
  - Ws_ftp.log
  - Install.txt
  - ToDo
- HTML source code
  - Password, select, insert, #include, #exec, connect, //
  - Comments

Enumeration

- Hidden fields
- Query strings
  - User ID (/login?userID=558253)
  - Session ID (/menu.asp?sid=69jt7b9329kuy)
  - Database queries (/dbsumit.php?sTitle=ms&iphone=5551212)

Video (Terminal Services)

Corrective Actions

- Investigate and disconnect unauthorized hosts
- Disable or remove unnecessary or vulnerable services

Vulnerability Assessment

- Proactive
- Validate policy compliance
- ID vulnerabilities
- Fast and easy
- MS08-067 is the current litmus test

Video (MS06-040 proof of concept)

Vulnerability Assessment Weaknesses

- False positives
- Requires high expertise in networking and OS security

Corrective Actions

- Upgrade or patch vulnerable devices
- Improve setup procedures and security baseline steps
- Assign a staff member to monitor alerts and mailing lists
- Modify the organization's security policies
- Implement and monitor Intrusion Detection

Example (DoD calls)

Passwords

- Password Cracking
  - Identify weak or default passwords
  - Verify the use of complex passwords
  - Brute force attack estimator

Video (Lock your PC)

Characters (complex)	Estimated time to crack
7	.009 hours
8	2.34 hours
14	9 hours
15	209 days

24 most-used passwords

1. 123456
2. password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123
11. 123123
12. admin
13. 1234567890
14. letmein
15. photoshop
16. 1234
17. monkey
18. shadow
19. sunshine
20. 12345
21. password1
22. princess
23. azerty
24. trustno1

Pick The Best Password

password

Summer13

P@swordCompl3x

juggle13 google

Password Challenge

- Remove any non-complex passwords at your agency.
- Contact TSU for a password recheck
- Certificate for the winners
- Admiration of all your friends and auditors

Passwords

- A strong password is:
  - 8 or more characters
  - Uppercase and lowercase
  - Alpha-numeric
  - Odd character(s)
  - Non-dictionary
  - Non-pronounceable
  - 15 or more characters for admin passwords (recommended)

Passwords

- Prevention
  - Set minimum length and complexity through group policies
  - Disable LM hashing
  - Don’t store passwords in plain text
    - Password Safe (recommended)
  - Educate the users
  - Change defaults

Example (Router and password)

Auditor’s Perspective

- Who to get access from
- One-Off audits
- Full audit
- Jack’s Testimonial
- How to read an Audit report

Demo (Sample audit report)

Post Testing Actions

- Remediate vulnerabilities
- Update policies
- Security awareness
- Legal notice
- Patch, patch, patch
- Change passwords

Demo’s

- Video (Client side scripting)
- Video (Path traversal attack)
- Video (SQL injection)
- Video (Cross-site scripting)
- Video (Information Security)

Penetration Testing

- Identify methods of gaining access to a system by using common tools and techniques used by attackers
- Should be performed after careful consideration, notification, and planning
- Perform during off hours to prevent unplanned outages

Penetration Testing

- Rules of engagement
  - Specific IP addresses/ranges to be tested
  - Any restricted hosts
  - A list of acceptable testing techniques
  - Times when testing is to be conducted
  - Identify period for testing
  - IP addresses of the tester’s machines
  - Points of contact for the penetration testing team, the targeted systems, and the networks

(Example) (Example)

Penetration Testing

- Blue teaming
  - Testing *with* the knowledge and consent of the organization's IT staff
  - Least expensive and most frequently used

Penetration Testing

- Red teaming
  - Testing *without* the knowledge of the organization's IT staff but with full permission of upper management
  - Useful for testing the IT staff's response to perceived security incidents
  - May be conducted with or without warning
  - More expensive and time consuming
  - Better indication of everyday security

Penetration Testing

- Outside attack
  - Usually performed first
  - Usually limited by firewall
  - Focus on commonly used ports
  - Done with very little inside information
  - Testers are not provided with any real information about the target environment
  - Leverages minimal access to gain greater access

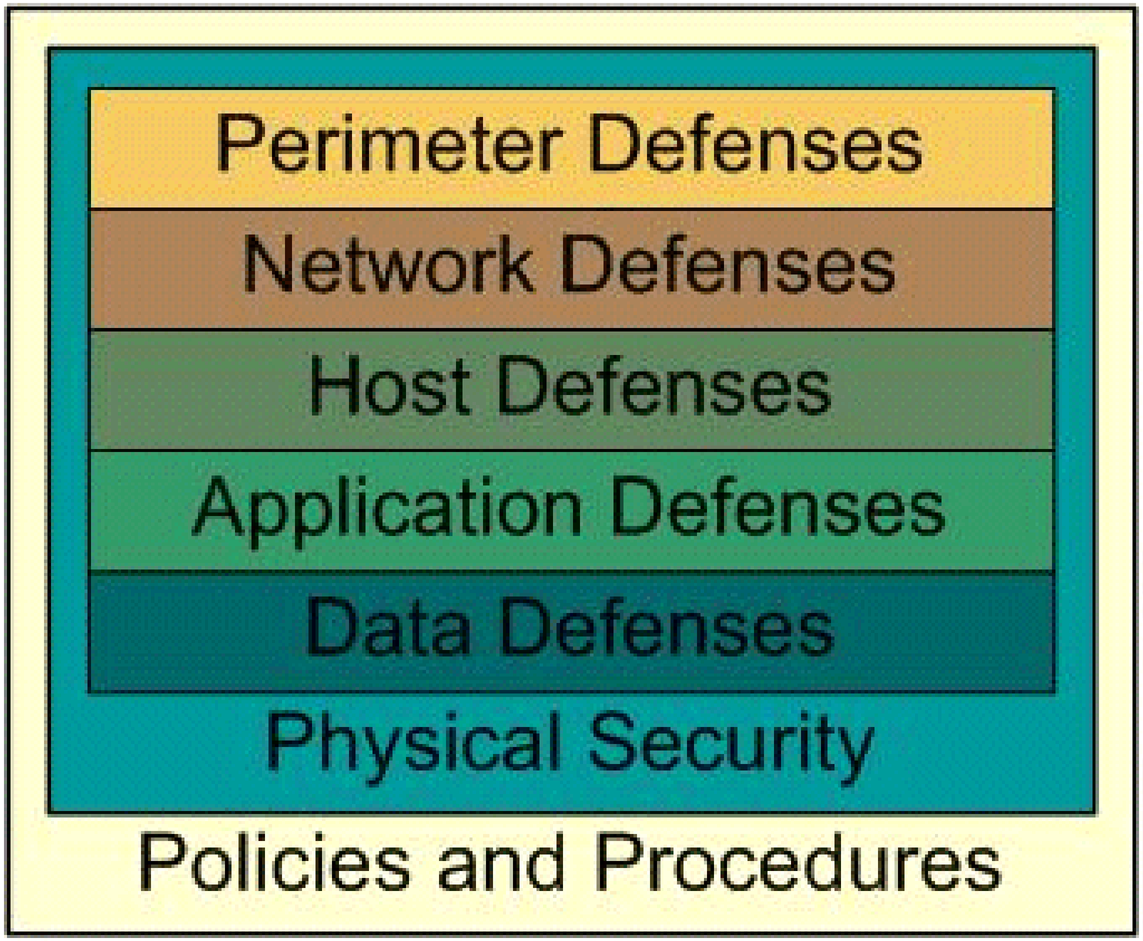
Penetration Testing

- Inside attack
  - Testers are on the internal network
  - Granted some level of access to the network (generally a user)
  - Attempts privilege escalation
  - Provided with commonly known network information

Roles and Responsibilities

- Only designated individuals should conduct the tests
- Alert appropriate staff that network mapping is taking place

Security In-Depth



Perimeter Defenses

Network Defenses

Host Defenses

Application Defenses

Data Defenses

Physical Security

Policies and Procedures

Wireless Security

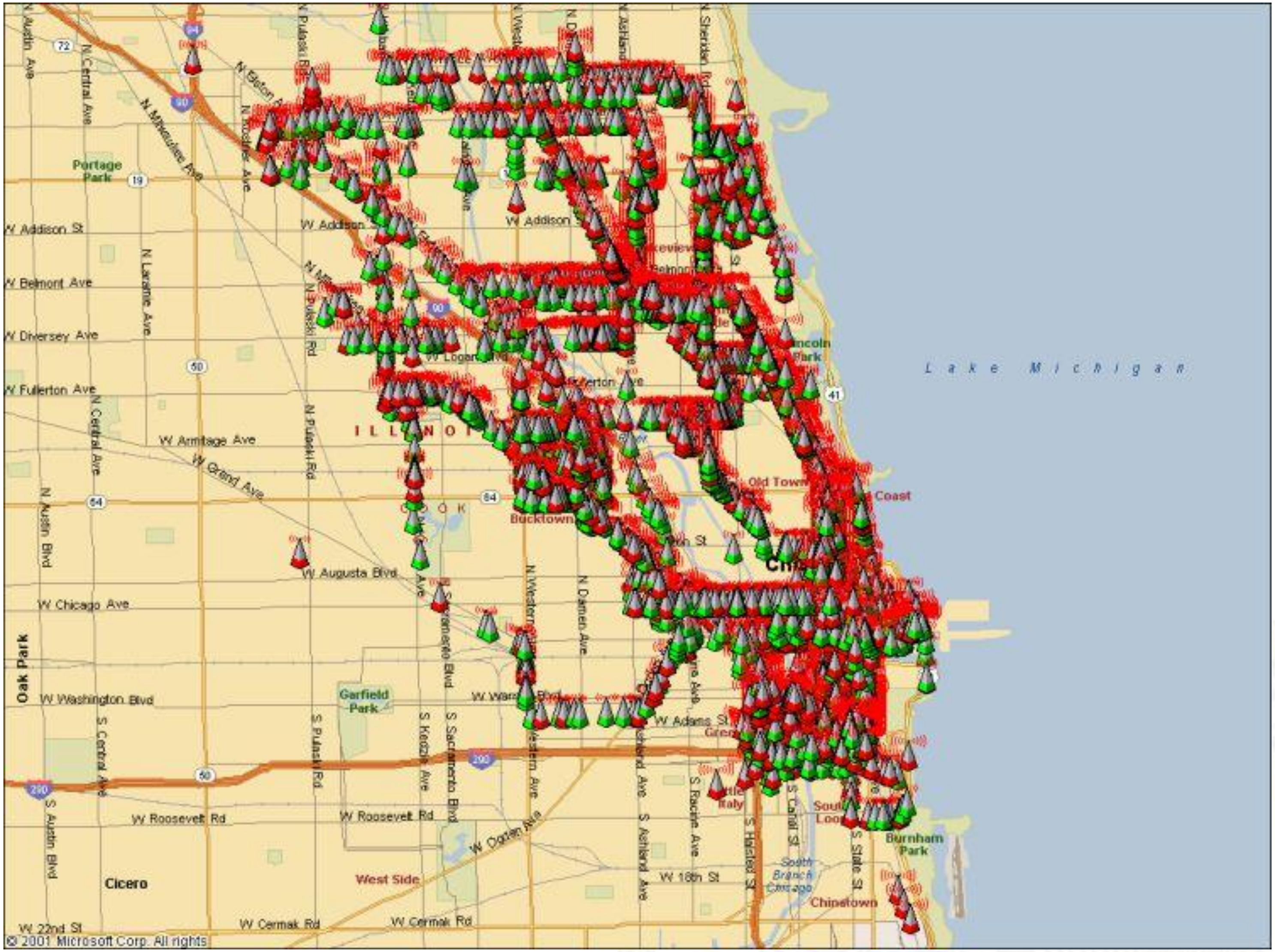
- 802.11b has serious flaws in its current implementation of WEP
- AP's often set to default configuration
- 300-600 feet range (more with an antenna)
- WPA 2 or above for encryption
  - WEP 128 bit encryption can be cracked in 1 to 6 minutes

Wireless Security

- Don’t use hotel or coffee shop wireless for anything requiring authentication or confidentiality (treat them like a postcard)
- Don’t jump on “free_internet”
- Avoid theft of service

HACKERS AHEAD
DO NOT PICK UP VIRUSES

War Driving


N Austin Ave
N Central Ave
N Milwaukee Ave
N Elston Ave
N Pulaski Rd
N Western Ave
N Ashland Ave
N Sheridan Rd
Portage Park
W Addison St
W Belmont Ave
W Diversey Ave
W Fullerton Ave
N Laramie Ave
W Armitage Ave
W Grand Ave
W Augusta Blvd
W Chicago Ave
Oak Park
W Washington Blvd
S Central Ave
S Austin Blvd
W Roosevelt Rd
Cicero
W 22nd St
W Cermak Rd
Garfield Park
S Pulaski Rd
S Kedzie Ave
S Sacramento Blvd
West Side
W Ogden Ave
N Damen Ave
Bucktown
Lincoln Park
Old Town
Coast
W Adams St
S Racine Ave
S Ashland Ave
W 18th St
S Halsted St
S Canal St
S State St
South Branch Chicago
Burnham Park
Chinatown
ILLINOIS
COOK
Lake Michigan
© 2001 Microsoft Corp. All rights

Corrective Actions

- Create and communicate a wireless policy
- Search for (and remove) rogue AP’s and misconfigured wireless LANs

Conclusion

- Security is a journey, not a destination.
- Keep informed
  - Newsgroups
  - Constant research
  - Books, etc.
- Request access to your agencies audits

Resources

- Security e-mail notifications
  - www.securiteam.com
- US-CERT bulletins
  - www.us-cert.gov/cas/bulletins/
- National Vulnerability Database
  - http://nvd.nist.gov/

Physical Security

- Locks keep honest people honest

(720 ILCS 5/19-2) (from Ch. 38, par. 19-2)