Security Awareness
For Server Administrators

State of Illinois
Central Management Services
Security and Compliance Solutions

BCCS
Keeping You Connected

Purpose and Scope

- To present a best practice approach to securing your servers
- To present real life examples of vulnerability assessment successes
- To present hacker techniques but not specific tools

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

Physical Security

- Locks keep honest people honest

BCCS
Keeping You Connected

SANS Top Threats 2008

1. Website attacks: exploiting browser holes
2. Botnets
3. Cyber espionage
4. Mobile phone threats
5. Insider attacks
   - 70% of hacks are from in house
6. Malicious spyware
7. Web application security exploits
8. Social engineering through phishing

BCCS
Keeping You Connected

Layered Security

Sample Attack Vectors

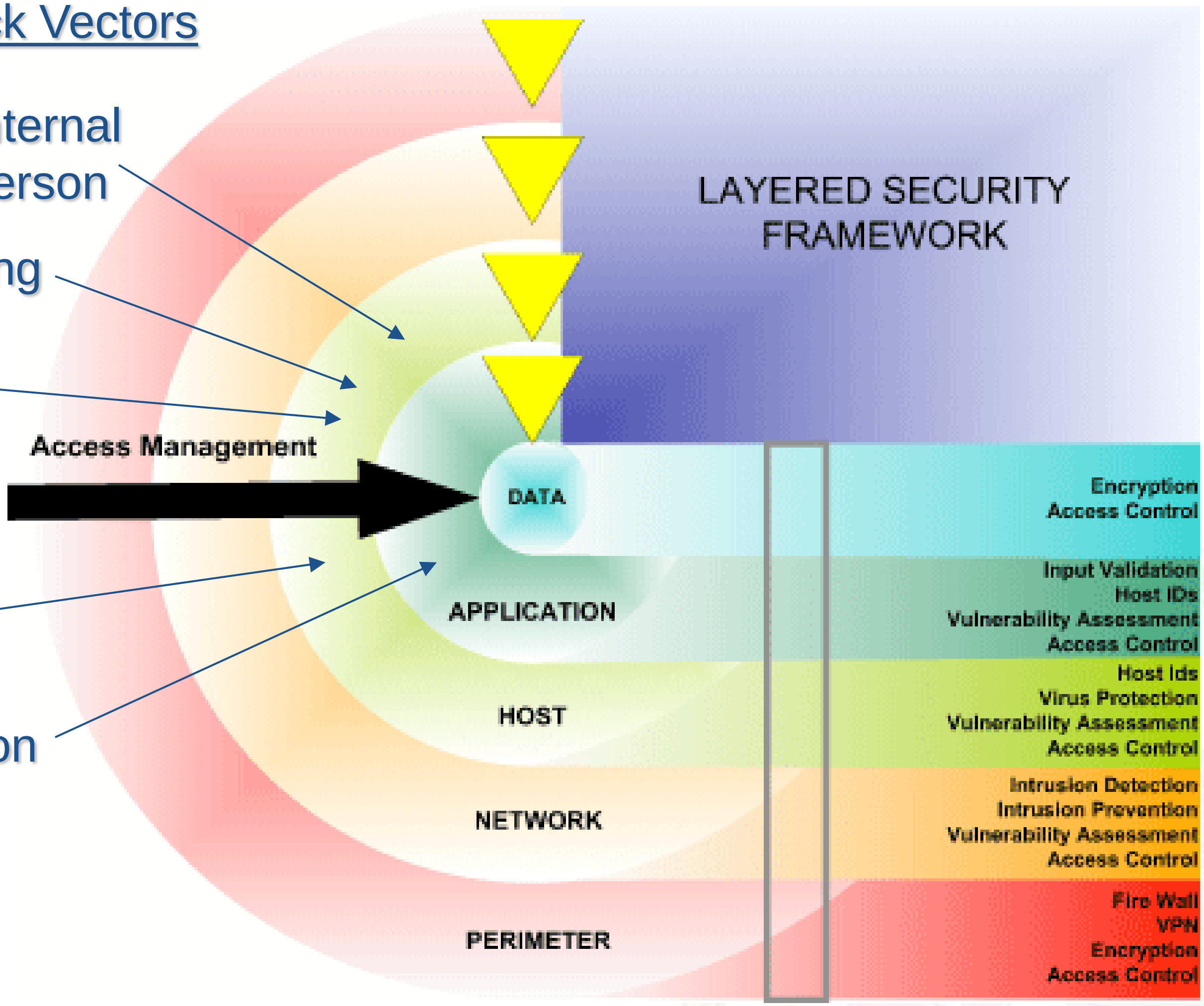
Internal person

Spear phishing

Social engineering

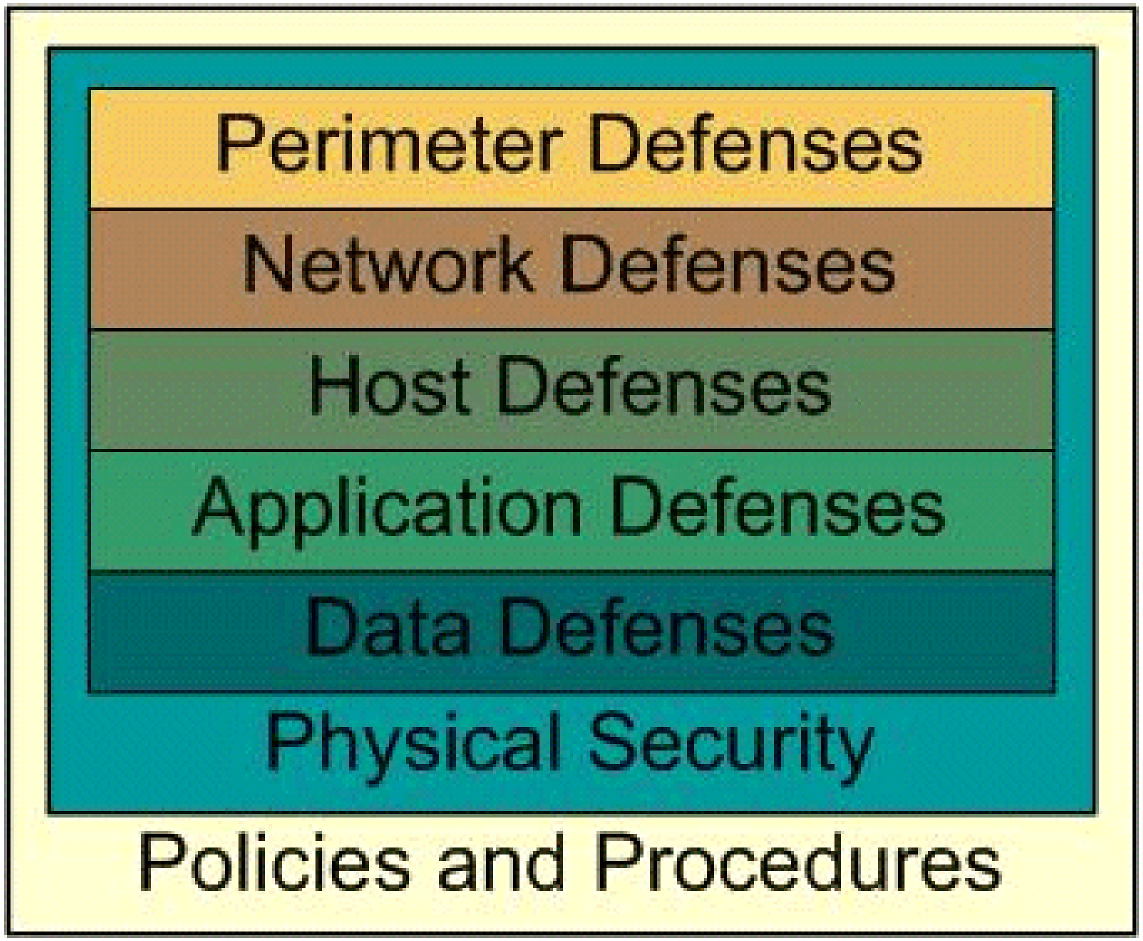
Botnets

SQL injection



BCCS
Keeping You Connected

Security In-Depth



Perimeter Defenses

Network Defenses

Host Defenses

Application Defenses

Data Defenses

Physical Security

Policies and Procedures

Return on Investment

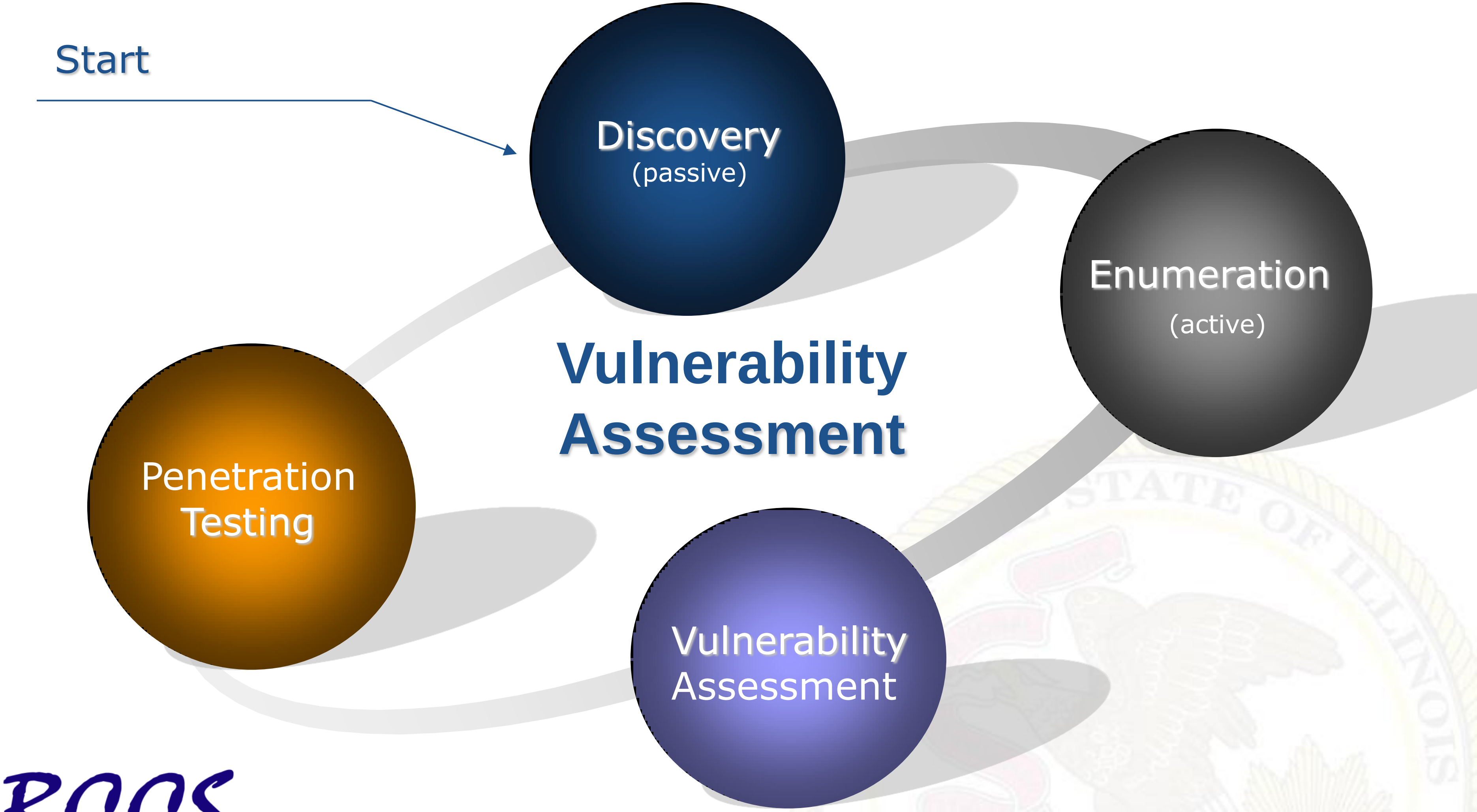
- 2006 Illinois breach notification law
- Average cost to notify per identity compromised?

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

  $2 - 18
- What is the return on investment for proactive security?

BCCS
Keeping You Connected

Testing Methodology



BCCS
Keeping You Connected

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)

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

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

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)

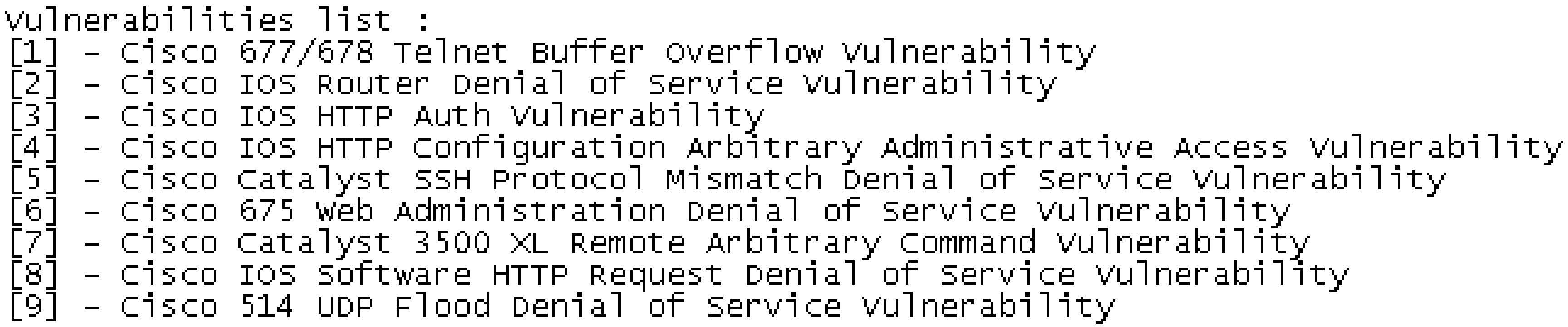
BCCS
Keeping You Connected

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)

Example (Cisco Exploit)



```
Vulnerabilities list :
[1] - Cisco 677/678 Telnet Buffer Overflow Vulnerability
[2] - Cisco IOS Router Denial of Service Vulnerability
[3] - Cisco IOS HTTP Auth Vulnerability
[4] - Cisco IOS HTTP Configuration Arbitrary Administrative Access Vulnerability
[5] - Cisco Catalyst SSH Protocol Mismatch Denial of Service Vulnerability
[6] - Cisco 675 Web Administration Denial of Service Vulnerability
[7] - Cisco Catalyst 3500 XL Remote Arbitrary Command Vulnerability
[8] - Cisco IOS Software HTTP Request Denial of Service Vulnerability
[9] - Cisco 514 UDP Flood Denial of Service Vulnerability
```

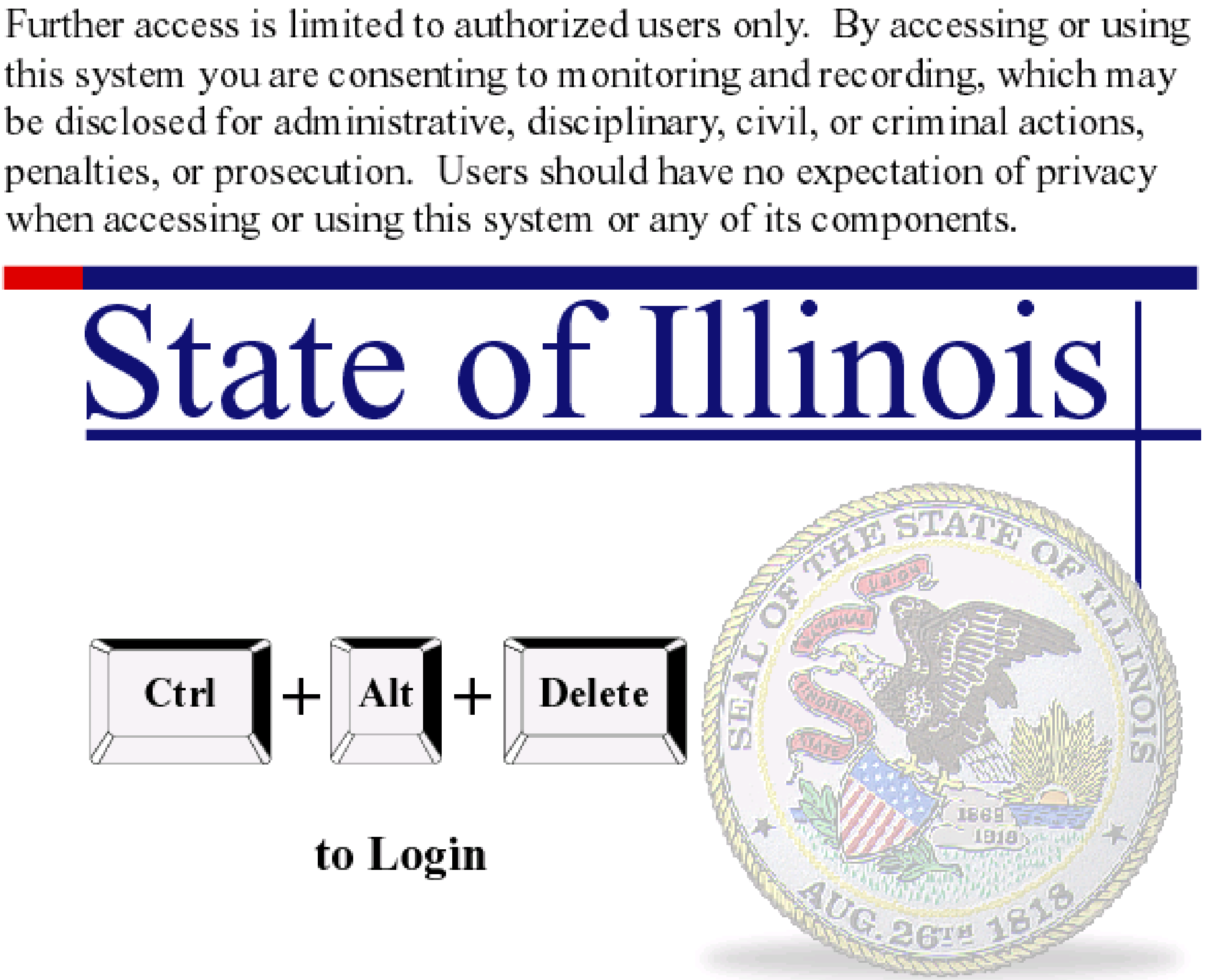
Demo (Sample audit report)

Post Testing Actions

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

BCCS
Keeping You Connected

Legal Notice



Further access is limited to authorized users only. By accessing or using this system you are consenting to monitoring and recording, which may be disclosed for administrative, disciplinary, civil, or criminal actions, penalties, or prosecution. Users should have no expectation of privacy when accessing or using this system or any of its components.

State of Illinois

Ctrl + Alt + Delete

to Login

BCCS
Keeping You Connected

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

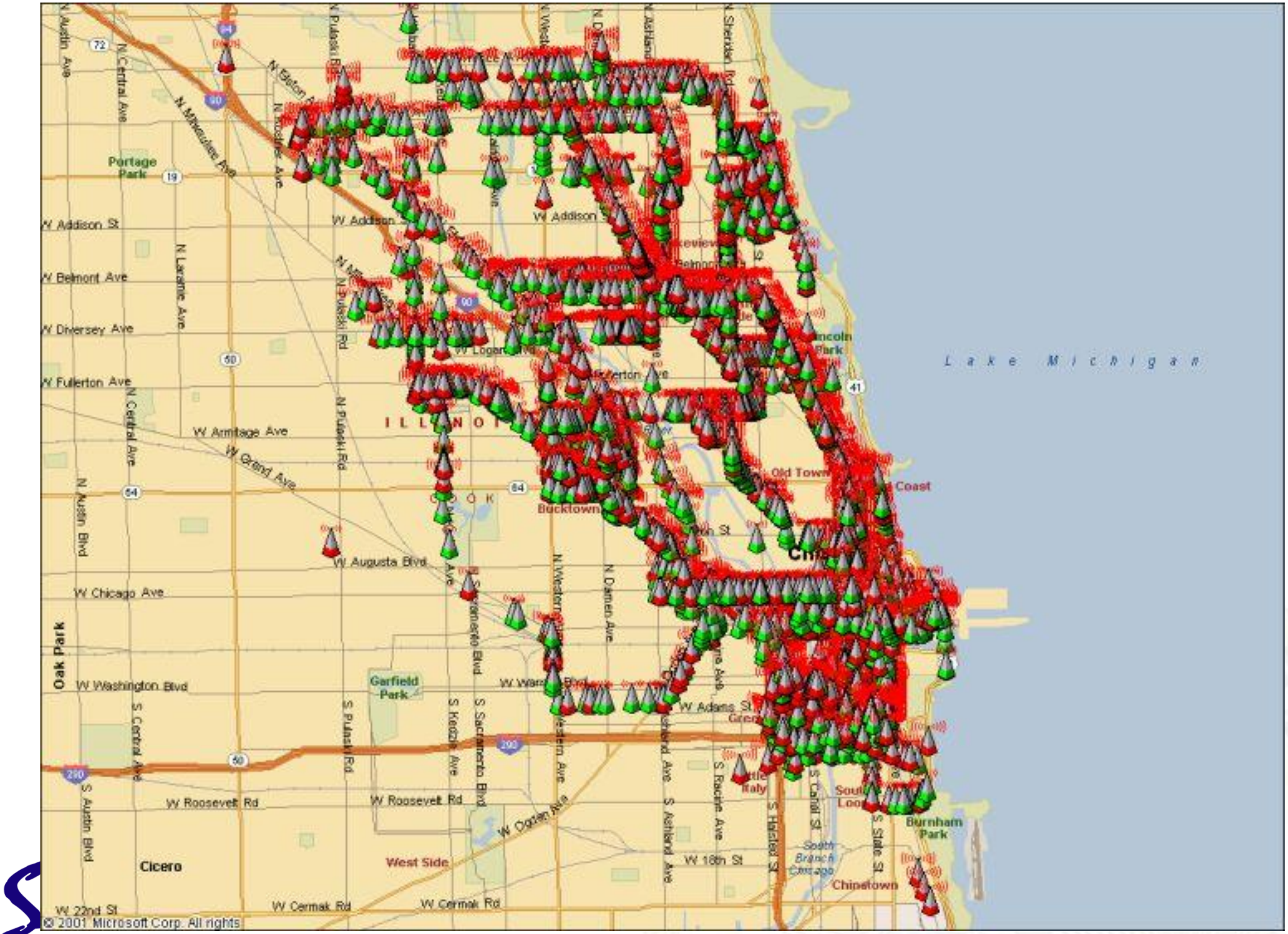
BCCS
Keeping You Connected

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


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

Resources

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

Security Awareness Material

- www.illinois.gov/bccs/services/catalog/security/assessments/Pages/awareness.aspx