Information Leakage
or
Call a Plumber --- your Info is Leaking

Joe Klein, CISSP

Sr. Security Engineer, AVAYA

kleinj@avaya.com

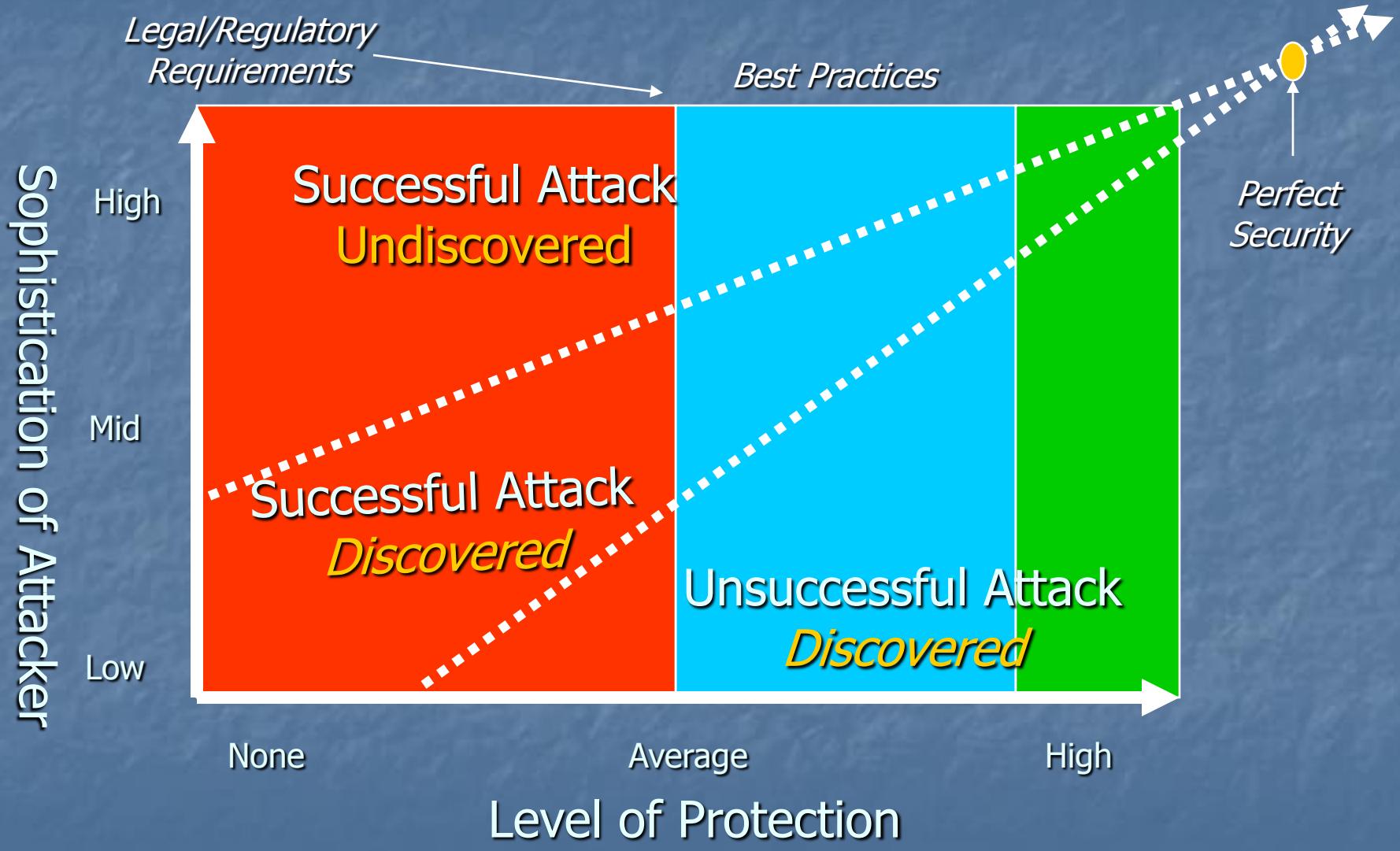
Overview

- Background for this Speech
- What is Information Leakage?
- What is the Risk?
- Types of Information Leakage?
  - Technical
  - People
  - Process
- How to Protect?

Background of the speech

- Art of War –
  - Not know yourself nor the enemy, you are lost
  - Knows yourself, but not the enemy and you are not likely to win
  - One who knows themselves and the enemy is certain to win

Sophistication of Attacker vs Level or Protection



What is Information Leakage(IL)?

Information which is released
purposefully or accidentally,
placing your staff, intellectual property, systems and networks
at risk.

What is the Risk of IL?

- Greatly improves the success of an attacker
- Places the organization at a competitive disadvantage
- Places organization at legal risk
- Can lead to physical harm of staff and facilities

Types of Information Leakage?

- Technology
- People
- Process

Technical

- Passive
  - Listening
    - Sniffers, scanning frequencies
- Active
  - Integration
    - War driving, war dialing, scanning networks

Technical

- Layer 2
  - Mac Address, SSID, Frequency Used
    - Identify Make of systems
- Layer 3
  - Active
    - nmap, qoso, xprobe, icmp, packeto
  - Passive
    - Sniffers, Kismet, radio scanner, etc

Technical

- Layer 4 and above
  - SNMP
    - System – processes, software, configurations
    - Network – internal networks, routes, protocols
  - Application Servers
    - Web sites: http://www.netcraft.com/
  - Chat, E-mail, Usenet, Mailing Lists
    - Look at header information of posting
  - Applications
    - See BH 2003 - - for details

Technical

- Special Cases
  - Firewalls
    - Firewalk
    - Firewall Fingerprint papers
  - Tempest – Emissions
    - Electro Magnetic
    - Other
  - Surveillance Devices

People

- Posting information on website
  - http://www.*target*.com
  - http://www.google.com/advanced_search?hl=en
    - Use domain option
  - http://webdev.archive.org/
  - http://www.google.com
- Technical Records
  - www.ARIN.net, www.whois.net
- Marketing Material, Advertisements, Press releases
  - http://www.cyberalert.com/
  - http://www.inboxrobot.com/
- Tradeshows
- The 'bar', smokers lounge, organizational parties

People

- Technical staff
  - Call to Vendor Technical Support
    - Gives full configurations, including passwords and network design to get help on problem
    - Outsourcing of Technical Support
      - Cisco, Microsoft, Oracle, Peoplesoft and others
      - Outsource Companies have a lower security requirements then original company
  - Posting questions on Internet (Usenet news, webpage's, etc)
    - http://tile.net/
    - http://www.google.com/advanced_group_search?hl=en
    - http://www.robofetch.com/

People

- Management
  - “Exception to Security Rules”
- Other
  - DR Drills

People

- Posting résumés, anonymous comments on "Financial Comment Board", Fu*kedcompany.com, etc
- Job Postings
  - http://hotjobs.yahoo.com/
  - http://www.brassring.com/
  - http://www.net-temps.com/
  - http://www.monster.com/
  - http://www.careerbuilder.com/
- Social engineering call's
- Mail/E-Mail deliveries
  - Trojans, backdoors

People

- News Searches
  - http://www.newsindex.com/
  - http://library.uncg.edu/news/
  - http://www.totalnews.com/
  - http://www.upi.com/
  - http://www.thepaperboy.com.au/welcome.html
  - http://www.onlinenewspapers.com/

People

- Address Phone Number
  - http://www.switchboard.com/
  - http://finder.geoportals.com/
  - http://www.infospace.com/
  - http://www.infobel.com/world/default.asp
- Other Personal Records
  - $ http://www.ussearch.com/wlcs/index.jsp
  - http://www.whowhere.lycos.com/
- Genealogy
  - http://ancestry.lycos.com/
- Phone Reverse Lookup
  - http://www.anywho.com/rl.html

People

- E-Mail Address
  - http://mesa.rrzn.uni-hannover.de/
- Class Mate.com
  - http://search.classmates.com/user/search/adv.tf
- ICQ
  - http://web.icq.com/whitepages/location/0,,,00.html
- Public Records
  - http://www.constructionweblinks.com/Industry_Topics/Public_Records/public_records.html
  - http://www.searchsystems.net/

People

- Hidden Gems
  - Intelliseek
    - http://www.invisibleweb.com
    - http://www.prefusion.com
  - Invisible-web.net
    - http://www.invisible-web.net/
  - Librarians' Index to the Internet
    - http://www.lii.org
  - Questia
    - http://www.questia.com/

Process

- Paper
  - Paper (Dumpster Diving)
- Backups
  - Tapes, CD's, DVD's and floppy's
- Technology
  - Hard Drives, PDA's, Cell Phones
- Cleaning Staff
  - Can they be trusted? Are you sure?

Process

- Posting by the Government
  - Financials & Personal Information
    - http://www.sec.gov/edgar.shtml
      http://www.hoovers.com/
    - http://www.searchsystems.net/
      http://www.infotoday.com/
    - http://www.dnb.com/us/
    - http://www.aicpa.org/yellow/ypgsec.htm
- Partners & Vendors Disclose Relationships
  - Google - link: target.com
  - http://amexb2b.disk11.com

How to Protect?

- People:
  - Limit what is posted publicly to the net
  - Education staff about danger
- Process
  - Perform/Have someone perform a Competitive Intelligence search on a regular bases
  - "extreme damage" items must be removed 'from view'
- Technology
  - Consider changing banners on systems
- General:
  - Create a classification system based on the risk
    - No damage to organization or people
    - Some damage to organization and/or people
    - Extreme damage to organization and/or people
  - Consider posting a few slivers of information – Misinformation
  - Perform all the other 'best practices' in security

Information Leakage
or
Call a Plumber --- your info is leaking

Joe Klein, CISSP

Sr. Security Engineer, AVAYA

kleinj@avaya.com