Security Architecture

Layered Defenses for the Enterprise

St. Louis ISSA, January 17th, 2006

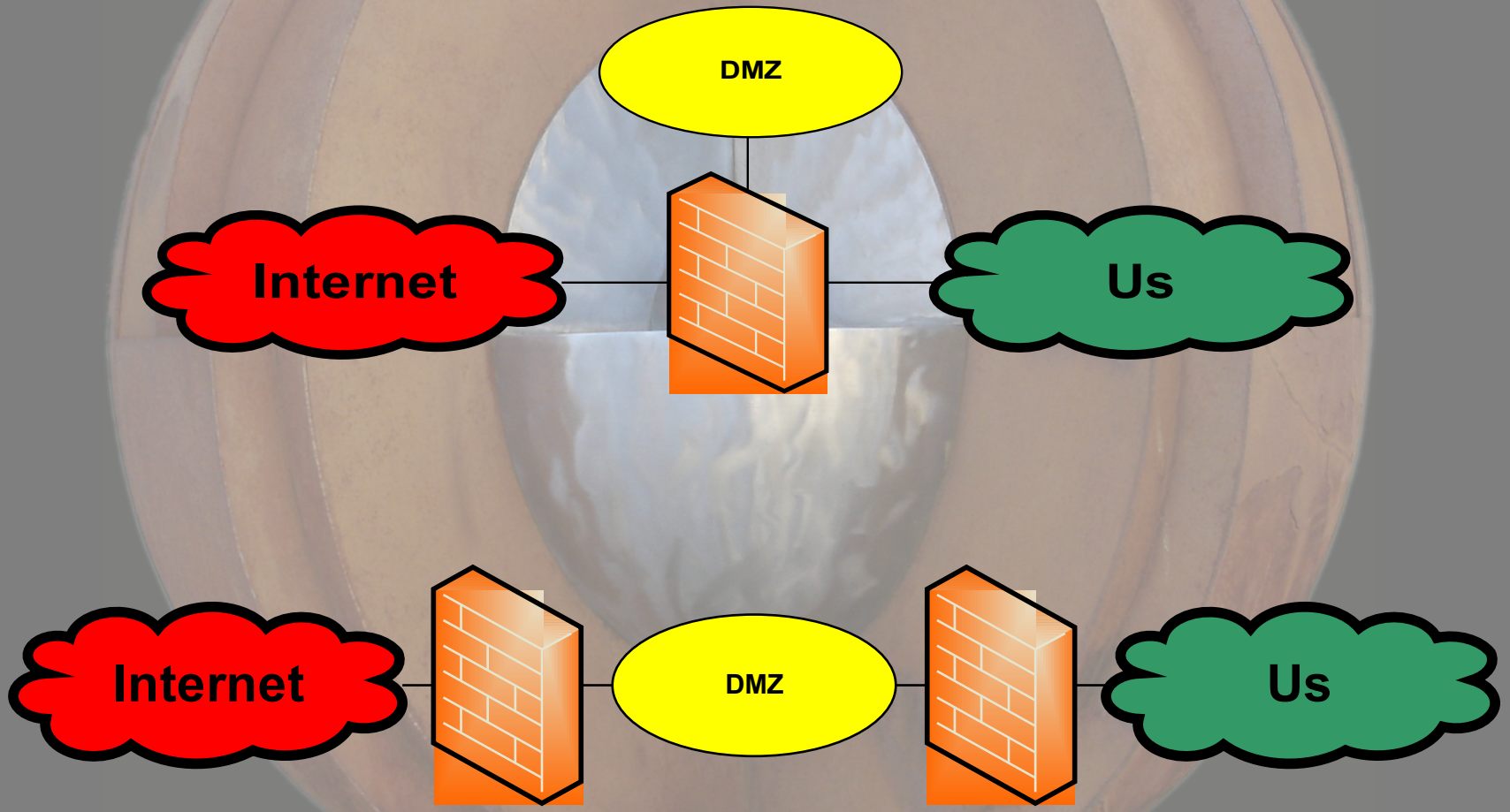
Agenda

- **Introduction**
- **Existing models**
- **Problems with existing models**
  - Case study: WMF vulnerability
- **Solutions**
  - Strategy
  - Tactics

About Me

- **Christopher (Chris) Byrd, CISSP**
  - Senior Security Administrator for Laclede Gas Company
  - Maintainer of the RioSec security weblog
  - cbyrd@lacledegas.com

Traditional Architecture



Firewall Sandwich

- Firewalls
- IPS
- Application Proxy and URL filter
- Load Balancers
- Switches
- A ton of Cat5 cable

Define the Problem

- **Security attacks are getting more creative**
  - Web app, client side, indirect (AWStats) attacks
- **0-day attacks are becoming more prevalent**
- **Despite security awareness training, spyware and phishing attacks still common**
- **Deperimeterization is common**
  - Jericho foundation group of CIOs and CISOs in Europe that encourages deperimeterisation

WMF Vulnerability

- 0-day (actually, at least -30day) exploit
- First known exploit ~Dec1, patch Jan 5
- Used the Escape/SetAbortProc sequence in an Windows Metafile record to execute shellcode
- Cause apparently due to legacy code
  - SetAbortProc is a GDI call that isn't used in WMF files
  - SetAbortProc originally designed for printing

WMF exploit demo

- **SpearPhishing attack**
- **Using Metasploit (www.metasploit.com) Framework v2.5**
- **Target is Windows XP Service Pack 2**
  - fully patched (as of 12/31/05)
  - [details of target AntiVirus]
- **DEP turned off (avoid VMWare virtual DEP)**
- **Variety of encoders and payloads possible**
  - Can “pivot” attacks, take full control of remote system
  - Can attack multiple systems using socketNinja or MSF3

What Didn't Work

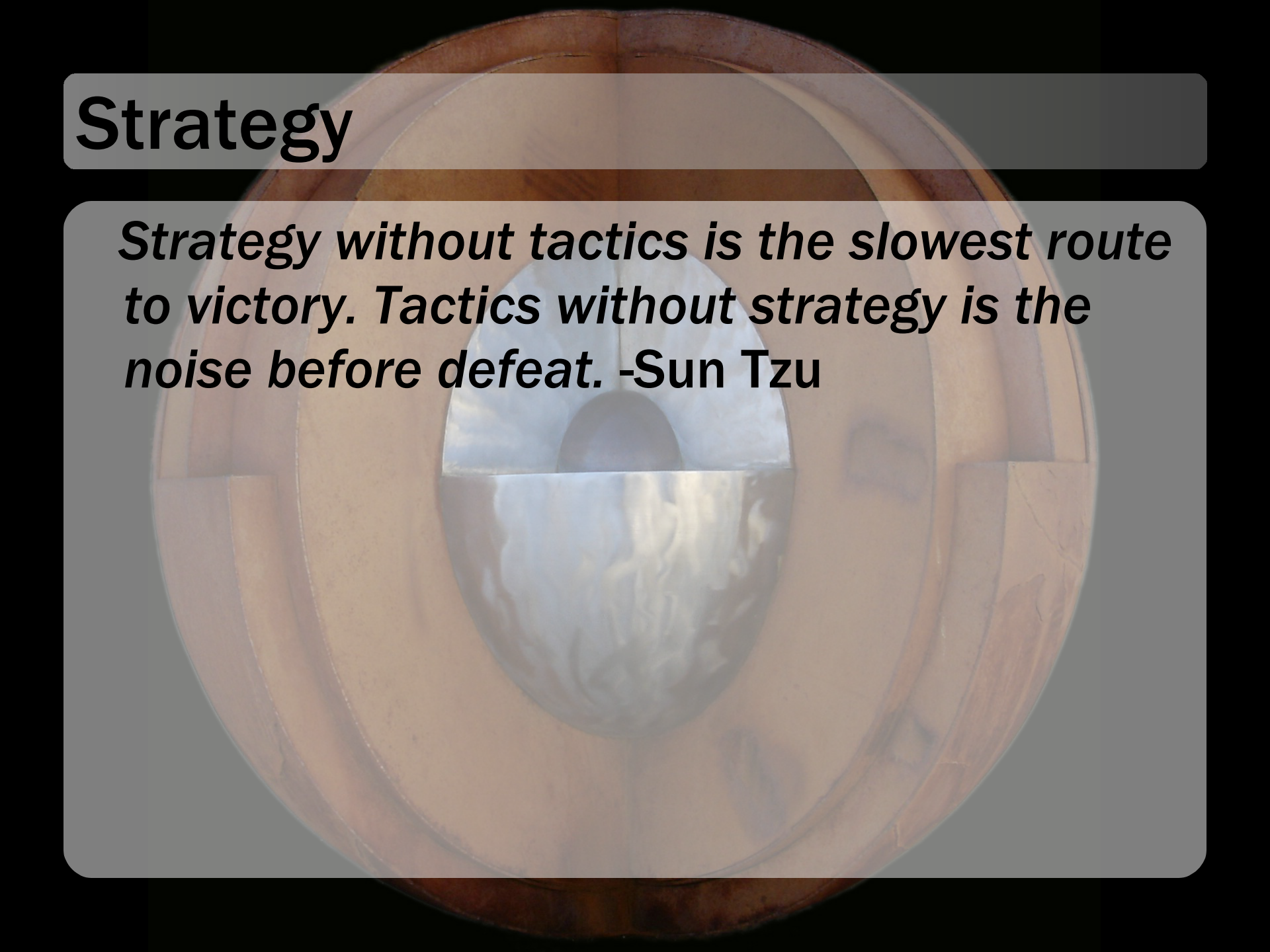
- **Firewalls**
  - Even to proxy firewalls this was normal behavior
- **Network Intrusion Prevention / Detection**
  - No signature for exploit
  - Encoders, changes to the WMF file, bypassed signatures when they were available
- **AntiVirus**
  - Once again, no signature
- **Email Gateways**
  - Exploit contained in graphic file, not executable

What Did Work

- **Behavior based HIPS**
  - Blocked the execution of code in data space
  - [Specifics of HIPS systems that worked]
- **Data Execution Protection (DEP)**
  - Included in Windows 2003 SP1 and XP SP2
  - Worked on 64-bit Athalon systems and VMWare because of hardware support
- **Human intervention**
  - Manual signature updates
  - Blocking WMF by signature (partial countermeasure)

Strategy

Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat. -Sun Tzu



Strategy

- Least Privilege
- Control Change
- Examine Trust
- Weakest Link
- Separation
- Three-Fold Process
- Preventative Action
- Proper Response

More information on these in “Inside the Security Mind: Making the Tough Decisions” by Kevin Day

Positive Security Review

- Enumerating Good instead of Bad
- Enumerating Bad is the same idea as “default permit”
- Understanding your business and technology environment

Improve the Architecture

- Assume that compromises will happen
- Limit company exposure from untrusted systems
- Limit damage from compromised trusted systems
- Monitor, contain, repair
- Understand your environment

Risks to the Perimeter

- Decentralization
- External partners
- Mobile systems
- Client Wireless and Rogue AP
- Remote access and modems

Wireless Risks

- **Rogue Access Points**
- **Wireless clients**
  - "Evil Twin" attacks
  - Automatic ad-hoc sharing in default config
- **Bluetooth**
  - Vulnerability in bluetooth drivers can be remotely exploited

Establish the Perimeter

- **Opposite of deperimeterization**
- **Think about walled city analogy**
- **Control Wireless**
  - No rogue AP
  - Client wireless settings
- **Control wired port access**
  - 802.1x instead of MAC address filter
- **Investigate NAC (Network Access Control)**
- **Firewall, encrypt, control mobile systems**

Application proxies

- **Enforces RFC compliance**
- **Has much deeper understanding of traffic**
- **Some can block traffic based on “magic” filetype**
  - Signature of binary file [first x bytes – research]
  - For example, block WMF files no matter what the extension is
- **Can limit traffic based upon methods and size**

Zone Systems

- **Create Zones based on:**
  - Value
  - Trust level
- **Zone systems using:**
  - Physical separation
  - Firewall
  - PVLANs
  - IPSec logical isolation

Separate the Networks

- For high security environment
- Provide physically separate networks and systems
- Thin clients can help reduce the cost
- E-mail, Internet not available on “securenet”
- A formal method to transfer data between nets may be required

Logical isolation with IPSec

- **IPSec can authenticate port access**
- **Encryption is not required (use ESP-Null)**
  - Encryption can be disabled for performance
- **Gateway systems**
  - Some services will need to be available for systems to join and authenticate
    - **DHCP, LDAP, Kerberos, DNS, IKE**
- **Access can be further restricted by AD groups**
- **Issues to address:**
  - Non-Microsoft systems must be handled by gateway
  - Non-Domain systems require certificates to auth
  - Performance (according to MS, ~1-3% CPU increase)

Layer 2 Isolation Using PVLANs

- **Private VLANs can separate systems on the same VLAN**
- **Ports configured one of three modes**
  - Promiscuous
  - Community
  - Isolated
- **Commonly used for hosts on DMZs**
- **Drawbacks:**
  - Doesn't work with VTP or dynamic VLAN membership
  - Careful consideration to preventing L2 isolated systems from communicating on L3

Host protection

- **HIPS**
  - Behavior based
  - Signature based
- **Host firewalls**
  - Can zone systems
  - Protect mobile systems
- **AV (of course)**
  - Some AV now includes buffer overflow protection

Monitoring

- **Where to monitor**
  - Perimeter
  - Between zones
- **Types of monitoring**
  - Behavior
  - Anomoly
  - Signature
- **Network Security Monitoring (NSM)**
  - Captures alert, flow, and packet data
- **Network Forensics**
- **Rogue detection**

References

- SANS Internet Storm Center
  - http://isc.sans.org
- RioSec Security Weblog
  - http://www.riosec.com
- Photo of EOSphere Sculpture on the UBC campus
  - Derivative work under Creative Commons Attribution 2.0
  - Original “The core” by Hendrik Kueck February 18th, 2005
  - http://flickr.com/photos/hendrik/510321/