

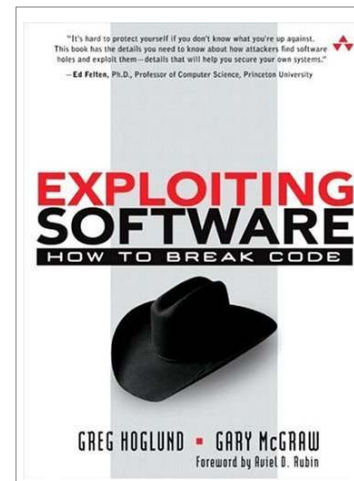
The State Of Incident Response”

Discussion Points

- Information Assurance (IA): Your Mission and Responsibilities
- The REAL Threat Landscape today: “It’s the Wild West!”
- Evolution of IA Tools; how did we get here?
- The State of Incident Response
- Defense-in-Depth: What’s Fundamentally Missing?
- Changing the Game: How Incidents are Handled Today, Why it’s broken, How it can be fixed?
- Opportunities for Improvement (next generation of IR tools)
- Questions & Answers
- References

HBGary Publications

- *Rootkits: Subverting the Windows Kernel*, Greg Hoggund and James Butler, Addison Wesley, 2005
- *Exploiting Software: How to Break Code*, Greg Hoggund and Gary McGraw, Addison Wesley, 2004



Who am I?

- Rich Cummings, Chief Technology Officer
 - 11 + Years Information Security Experience
 - Focused on Offensive & Defensive tools and techniques
 - 8 Years performing Incident Response Investigations
 - Department of Defense
 - Fortune 500 Companies
 - Guidance Software January 2002 – October 2007
 - 2000 - 2001 Independent Security Consultant
 - 1997-2000 Network Associates:
 - Principal Consultant; Attack & Penetration Testing & 911 Emergency Response Team
 - 1996 PricewaterhouseCoopers

Information Assurance Definition

- The DoD's Definition: Information Assurance is...
 - Information Operations that PROTECT and DEFEND information and information systems by ensuring their Availability, Integrity, Authentication, Confidentiality, and Non-Repudiation.
 - Information Assurance implies the ability to PROTECT, DETECT, and SUCCESSFULLY REACT to information attacks directed to your information infrastructure.

“Profound” Threat Landscape Assumptions

- There are *things we know* about the cyber threats
 - If I install this patch, I’m protected from these publicly available exploits...
- There are *things we know that we don’t know*
 - *How many rogue insider’s (with legitimate access) do I have?*
 - *How many 0-day attacks are out in the wild?*
- And then there are *things we don’t know that we don’t know...*
 - How many of my rogue insiders have multiple 0-day attacks?



Today's Threat Landscape

- To BEST defend our networks & information assets, we need to understand the Enemy and the REAL Threat landscape
- It's the wild west today on the Internet!
 - Cyber Crime is one of the *Fastest Growing Industries!*
 - 1997 – 2004 = 100,000 attacks on line
 - 2004 – 2006 = 200,000 attacks on line
- When will the Cyber War begin? - Is it going on Today?
 - Some predict a “Digital Pearl Harbor”
 - Why be “loud & proud” when you can be “silent & almost invisible”
 - I believe it's happening all day everyday...
 - “Death by a Thousand Cuts”

Threat Landscape Continued

- **Over the last 2 years there has been a Fundamental Shift in Internet Threat & Cyber Crime activity**
 - From Massive Attacks to Targeted Attacks
 - Fueled by Thriving Underground Vulnerability Market
 - 0-Day Vulnerabilities & Exploits sold for \$10,000 - \$100,000 each
 - Objectives of the Cyber Criminal:
 - \$\$\$ Financial Gain! \$\$\$
 - Theft of Information (national secrets, intellectual property, identity theft)
 - No longer do hackers seek reputation!
 - The Malicious code we are seeing in the wild today:
 - Unprecedented sophistication & covertness capabilities
 - The Malware today has excellent quality assurance (QA)
 - More stable than some commercial software
 - Professional Software Development Lifecycle Model
 - Significant financial backing by organized crime, rogue states and countries

Today's Threat Landscape Continued

- Symantec documented 2500 new vulnerabilities in the last 6 months of 2006
 - 66% of these vulnerabilities affected Web Applications & Instant messengers
 - 7% affected Operating Systems
 - 94% of these vulnerabilities were REMOTELY exploitable
 - SPAM and Phishing attacks now contain embedded malicious code
- Zero Day activity is continually increasing:
 - 0-Day attacks increased by over 100% from 2005 - 2006
 - 12 New 0-Day in the last 6 months of 2006*
 - in 2007: On track to do over well over 100% growth

Today's Threat Landscape continued

- **Dramatic Increase in 0-Day Attacks in 2006**
 - 12 new 0-days from July 06 - Jan 07
 - Microsoft Office, IE, and active X controls
 - Email (spear fishing)
- **Why more 0-day Attacks then ever before?**
 - Tools to detect and exploit vulnerabilities readily available on the internet, easy to use!
 - Fuzzers, Debuggers, Decompilers, etc
 - Metasploit
 - “How to Guides” to identify and exploit vulnerabilities online
 - Professional Courses now teach you to identify and write exploits
 - www.immunitysec.com/education-overview.shtml
 - See graphic next slide

“Professional Unethical Hacker Training”



COMPANY	NEWS	PRODUCTS	SERVICES	RESOURCES	DOWNLOADS	EDUCATION	PARTNERS	RESELLERS	CLIENT LOGIN
---------	------	----------	----------	-----------	-----------	-----------	----------	-----------	--------------

EDUCATION

- ▶ Overview
- ▶ Current Schedule
- ▶ Windows Overflows
- ▶ Accelerated Windows Overflows
- ▶ Unethical Hacking
- ▶ Using Spike & Ollydbg to find new Vulnerabilities
- ▶ Auditing MSRPC
- ▶ Understanding and Exploiting Windows Heap Overflows
- ▶ CANVAS Training

Overview

Immunity's courses are not the standard "Ethical Hacking" "Penetration Testing" or "Vulnerability Assessment" courses. We do not teach you how to run Nessus, Nmap, or that you should have a policy against SNMP on your network. We do teach you how to write exploits, capitalizing on Immunity CANVAS to provide training that even someone with only a little programming expertise can succeed at. Once you leave our class, you leave as a changed person, able to take advisories and turn them into working exploits, or take a network protocol and find a vulnerability in a target program, or covertly penetrate a network successfully.

All Immunity classes are \$1000 per student per day (see descriptions for actual class durations). We have a minimum of 4 students per class, and a maximum of 12 students per instructor. Students in the Windows Overflows, Unethical Hacking, Heap Overflows and CANVAS training classes receive a single user CANVAS license included in the cost of the training.

Classes in France

In conjunction with our partner, Sysdream, Immunity is pleased to now offer classes in Paris, France.

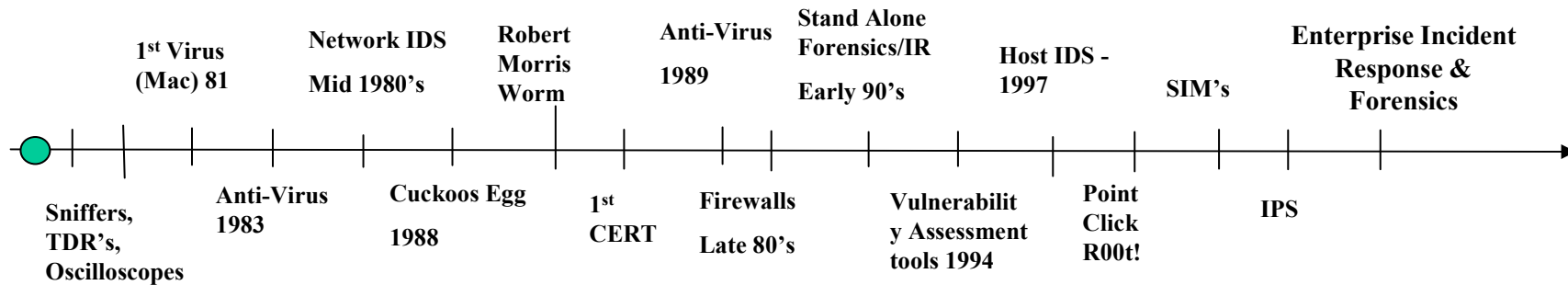
The State of Incident Response

- **CERT Policies have NOT kept up with IR Technology!**
- **Current tools DO NOT provide the end-point VISIBILITY required for optimal decision making**
- **Rootkit Technology is everywhere!**
 - **2003 – 2006: 700% increase in rootkit technology seen in malware & PUPS (potentially unwanted programs)**
- **IDS & Sensor data alone is no longer good enough**
 - **it's only 33% of the picture**
- **Classified Message Incidents/Data spillage**
- **Insider Threat is very difficult to detect:**
 - **Load Knoppix, spoof the MAC address and wreak havoc.. How do you detect that?**

The State of Incident Response

- **Current processes rely heavily on known bad signatures**
- **Current manual or broken processes extend the "time of exposure"**
- **Current Incident Response processes rely too heavily on Sensor Data alone**
- **Current Antivirus technology is ineffective against these non-signature-based threats**
 - **AusCERT Oct 2006 "most popular AV software today misses 80% of latest malware: trojans, rootkits, and viruses"**
- **COTS tools do not facilitate rapid assessment & triage capabilities**
 - **Diagnose, Identify, Contain, Preserve, Report & Share findings...**
- **Currently capabilities make it impossible to perform Enterprise Collateral Damage Assessment for known intrusion "footprints"**
 - **in a forensically sound fashion below the OS)**

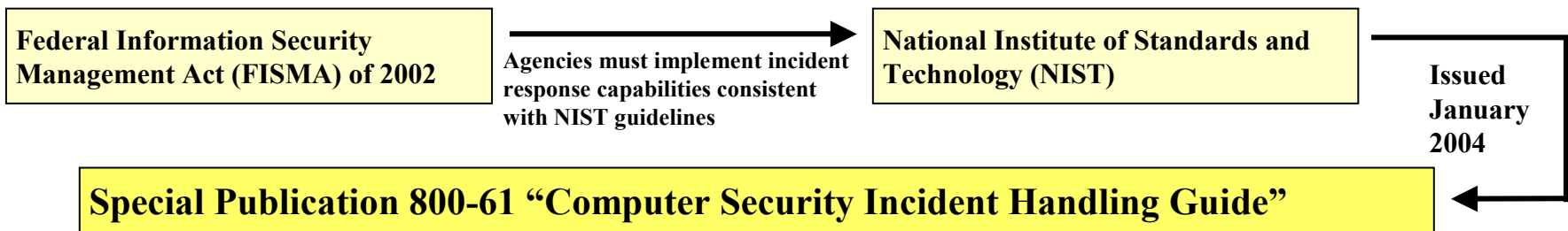
• Generic Timeline/Evolution of Information Security tools & networks



- **Points to consider:**
- Tools were/are created to solve specific problems of the time period, often 2 years later...
- Tools start out as stand-alone and then evolve into Enterprise class solutions
- Tools & techniques often start out as open source and then evolve into commercial applications that are supported & certified
- Even with all these security measures in place, incidents are rapidly growing in frequency, sophistication, scope and with a whole new level of covertness...

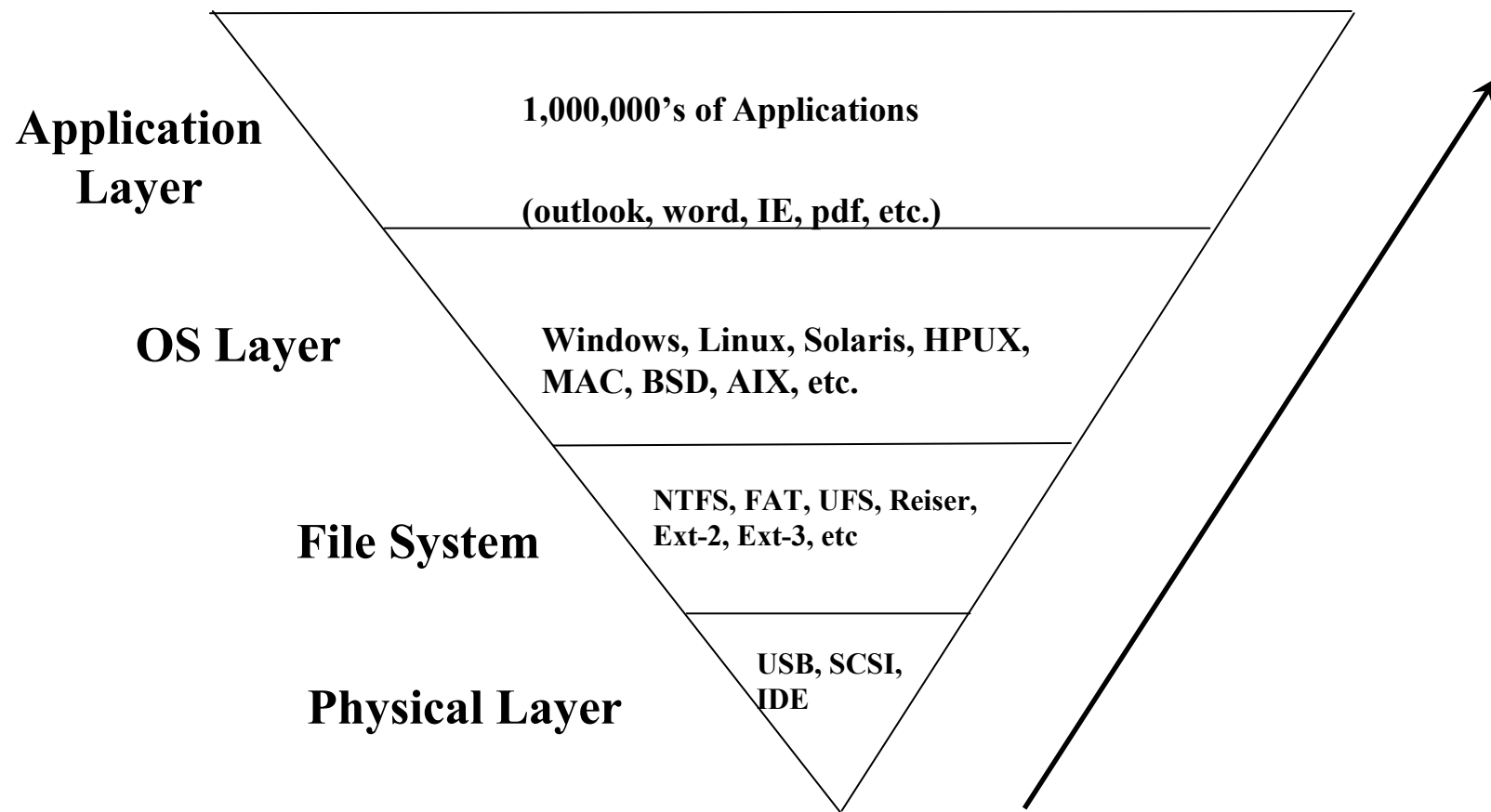
NIST Requirements for Incident Response

The NIST Requirements:



Technology Requirements of 800-61							
Immediate Response	Initial Snapshot	Minimally Invasive	Forensics hard drive acquisition	Forensics Analysis	Court validated technology	Chain of Custody	Volatile Data Acquisition and analysis
Allows immediate enterprise-wide response	Allows for immediate snapshot target machines	Affect nothing on the machine	Ability to preserve data	Forensic analysis capabilities	Must meet court evidentiary requirements	Maintains chain in a manner acceptable in court	Immediate capture and analysis of enterprise-wide volatile data

Computer Forensic OSI Model



IR Requires both Static and Volatile Data

Data At Rest



Direct Disk Access:

- See and search at the disk level
- Read only access – don't alter data on system under investigation
- Don't rely on the OS for file system interpretation.. Critically Important!
- Preserve findings in court approved fashion

Volatile Data



RAM Data:

- Must be able to search, analyze, and preserve all volatile data
- Injected dll's, memory resident exploits, backdoors
- Hidden Processes like rootkits
- Running processes, sys files, and dll's

How are incidents detected?

- **How are Incidents Detected & Diagnosed (Verified) Today?**
 - Network/Traffic Analysis & Monitoring (IDS & SIM tools)
 - Log Analysis (firewalls, routers, servers, etc)
 - Anti Virus
 - Deviations from System Baselines
 - Hash Analysis
 - Disjointed tools
 - Port Scans, log collectors, Isof, etc
 - Host-Base IDS
- **Counter Attacks to Defeat Incident Detection!**
 - Barrage Jam!
 - Encrypted Attacks!
 - Zero-Day!
 - Code Encrypters & Packers!
 - Memory Resident malware (never touches the disk)

How do you respond?

- **How do you Detect, Diagnose & Respond?**

- **Sensor Grids:**

- Only part of the equation
 - Must have host data to confirm hypotheses
 - Must be able to perform Rapid Root Cause Analysis for future Protections

- **Disjointed Tools: Batman tool belt?**

- Trusted CD's & Floppies
- Doesn't Scale, Prone to Analyst errors!

- **Traditional Forensic Response**

- 1 machine at a time, Doesn't Scale!

- **Do nothing!**

- Wipe, Rebuild, Patch & Proceed (NOT GOOD!)
- Learn Nothing... who did what, when, why & how????
- Cannot Prosecute
- Cannot Prevent or Detect similar attacks in the future!

The Future of Incident Response

- **Integrated & Scalable Approach:**
 - Host IR & Forensic system integrates with IDS/SIM/Content Filter tools to automate the collection/analysis of IR data
 - Uses Database on backend to track status, results, and generate reports
- **Automatic Reverse Engineering of Malware & Unknown files**
 - Active Forensics
 - Automated Program Analysis – To rapidly develop behavioral profile of applications
- **Physical Memory Clones:**
 - Commercial Tools to perform ultra deep diagnosis of live RAM
- **Immediate Creation of Malware Footprints:**
 - IR systems will provide a “GUI Wizard” to create immediate malware signatures on the fly
 - Today customers wait weeks for updates to Anti-Virus software for new malware
- **Integrates with Extremely Large Hash Database**
 - 1,000,000 Files on 5000 Machines, Which are Good, Bad, Ugly?
 - Remove the Noise & get to Signal Right Away!
- **Integrates with Hard Disk Encryption products**
 - Allows investigation of computers with Full Disk Encryption products
- **Hardware Level Debuggers to Identify Hardware Level Malware**

Conclusion

- Incident Response tools need to evolve with the bad guys...
- Every machine must be diagnosed at the lowest possible levels...
 - Forensics Understanding
- No amount of Protection can stop today's threats... they can get through all your defenses
 - the best defense to these Zero-Day attacks is a SCALEABLE IR & Forensic "Diagnosis" Capability
- The Cyber Criminals tools & techniques are years ahead of the Network Defenders
- Manual Efforts cost too much: Time, Money & Technical Resources

Thank you!

Rich Cummings

Email; rich@HBGARY.com

Mobile 703-999-5012