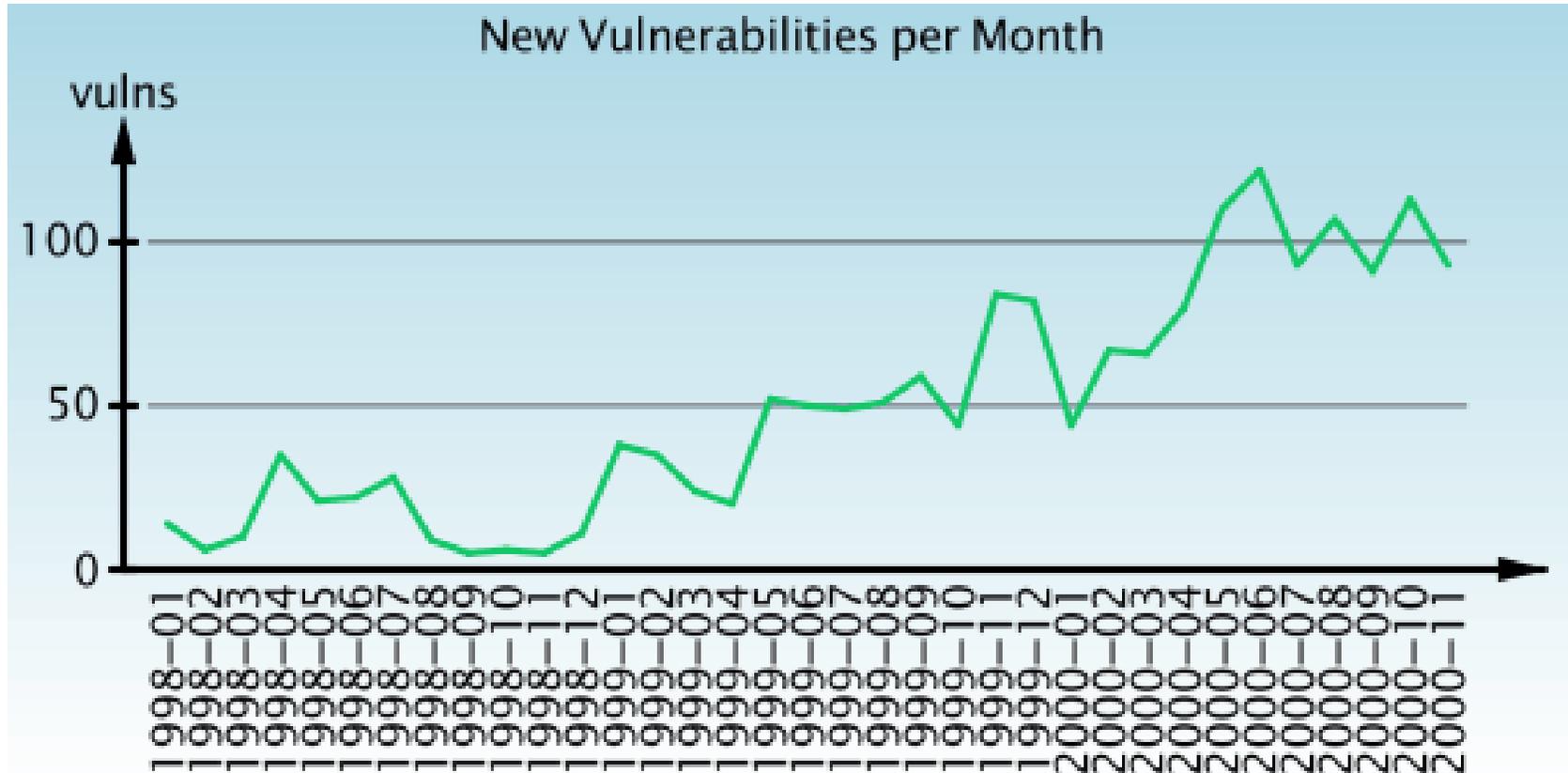


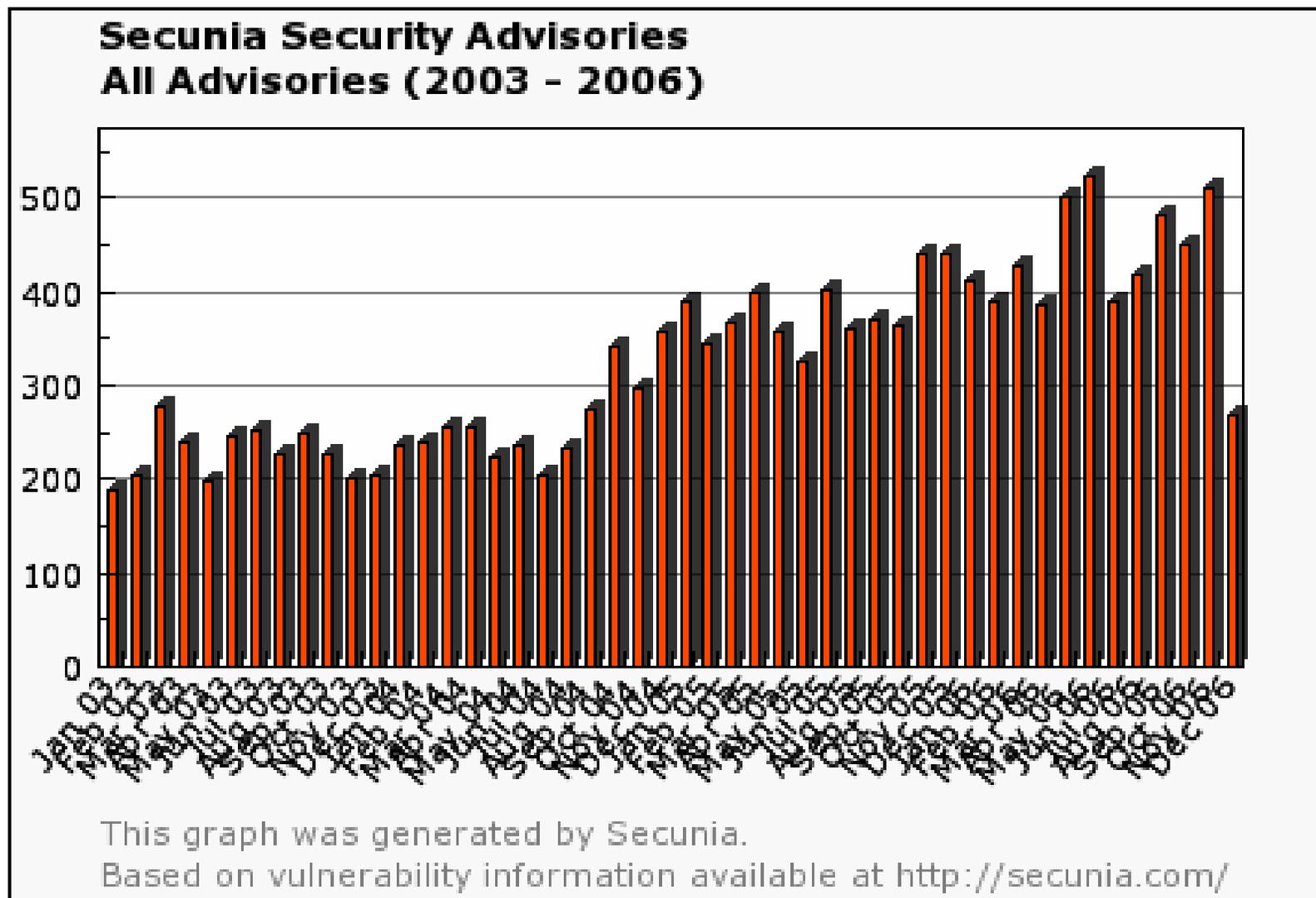
# Evolving Threat Landscape

**Paul A. Henry**

MCP+I, MCSE, CCSA, CCSE, CFSA, CFSO, CISSP, CISM, CISA, ISSAP, CIFI

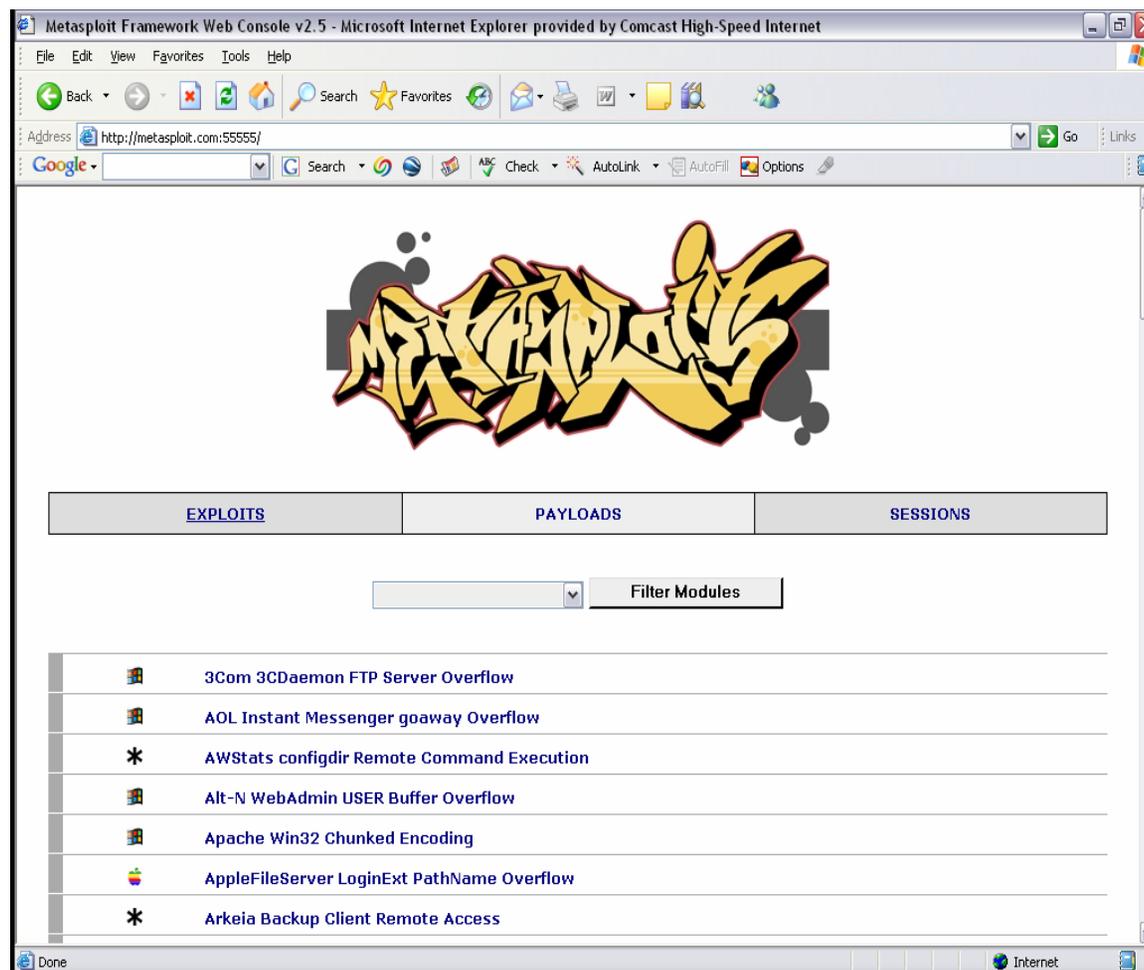
- Application Layer Threats
  - **Fuzzing still driving application layer vulnerabilities**
  - **Signature-based defenses have been rendered obsolete**
  - **Shift from Defending-Forward to Global Defense**
  - **Risk Mitigation Considerations**
- VOIP risk update
  - **New Trojan highlights Skype as a risk to the enterprise**
  - **Risk Mitigation Considerations**
- Spam – Hackers vehicle of choice
  - **Botnets drive spam to new heights**
  - **Risk Mitigation Considerations**
- Authentication
  - **Passwords are obsolete – get over it**
  - **Tools of the trade**
  - **Risk Mitigation Considerations**
- Digital Rights Management (DRM) fails to deliver on regulatory concerns
  - **To much reliance on trusted users plagues DRM**
  - **Risk Mitigation Considerations**

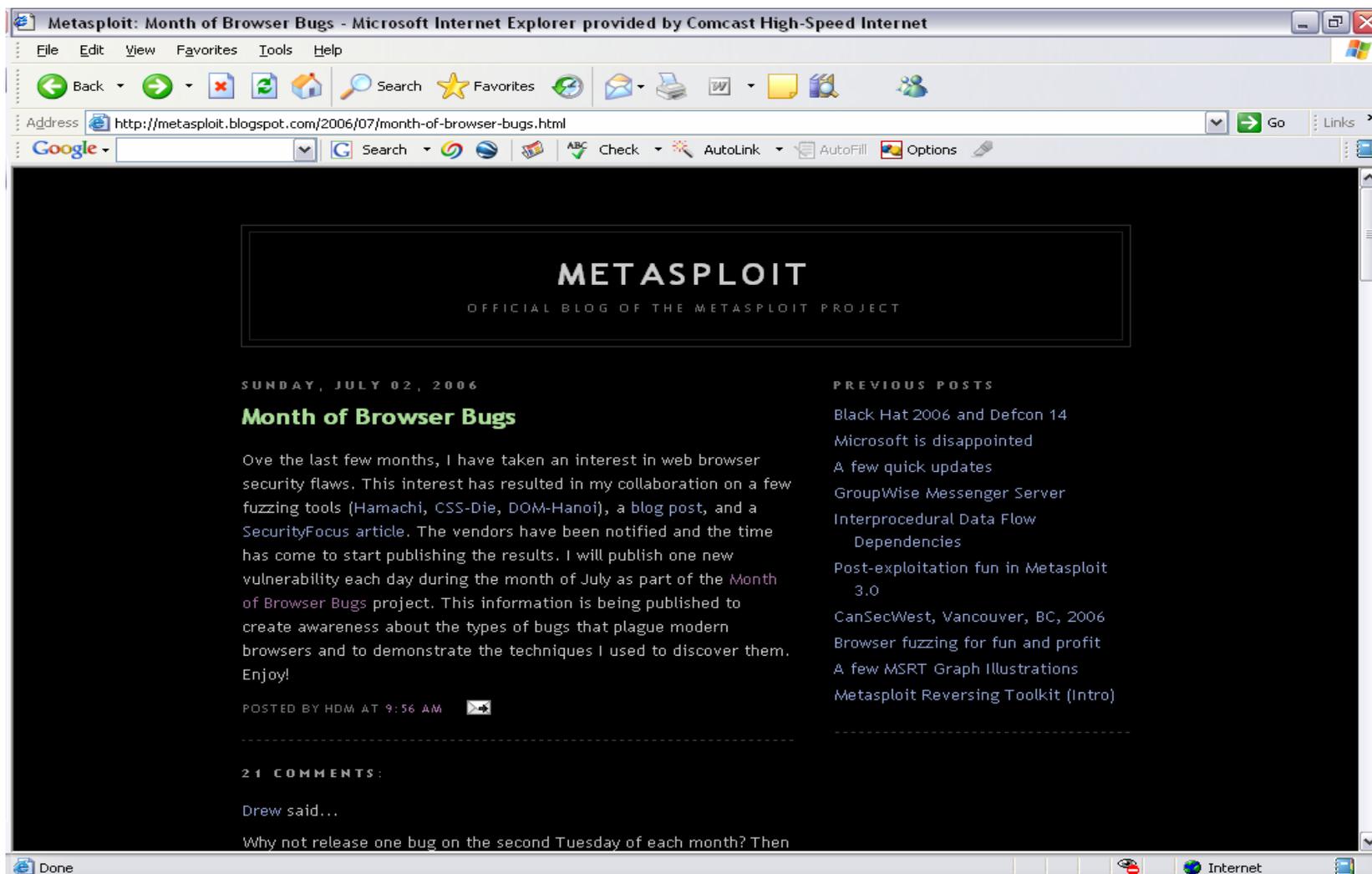




- **FUZZING**

- In the simplest of terms Fuzzing programs provide for an automated replacement for normal input and interfaces for a given protocol or application. This automated “replacement” input is computer generated, ambiguous and random in nature. By design Fuzzer’s seek to cause abnormal behavior in the protocol or application. The abnormal behavior is indicative of a software bug and can be further tested to determine if the abnormal behavior (bug) is exploitable.





## the Month of Kernel Bugs (MoKB) archive

### FAQ

#### What's the purpose of the "MoKB" ?

Publish one bug on daily basis for the month of November, 2006. Show tools and procedures useful for testing the strength and quality of kernel code (ex. networking, filesystem handling) in existing operating systems (Mac OS X, FreeBSD, Solaris, GNU/Linux, etc).

#### What tools have been used to detect the bugs?

For filesystem related bugs, **fsfuzzer** (ported to \*BSD, Linux and partially for Microsoft Windows). For other bugs, the still effective **isic** (capable of taking network stacks and NIC drivers to their knees), **sysfuzz** (with updated syscall blacklist for each system) and **mangle** itself (wrapped with a bash script or similar approach).

#### White, Red, Grey or Black Hat?

Hats are too old fashion. And they look sinister, right? :-)

#### Why not selling the bugs? Or report them to the vendors?

The goal wasn't to make money. MoKB goal was (and currently is) checking how many **unreported and unknown** issues can be found in kernel code out there, using simple, yet effective tools deploying techniques such as fuzzing and 'stress testing'.

#### Can I help or contribute?

Yes, during the MoKB, feel free to send bugs and proof of concept code. Also, mirroring this site will be really welcome. Please send the URL to the mirror site and it will be included in the list. If you want to go a step further, consider a donation.

### Files

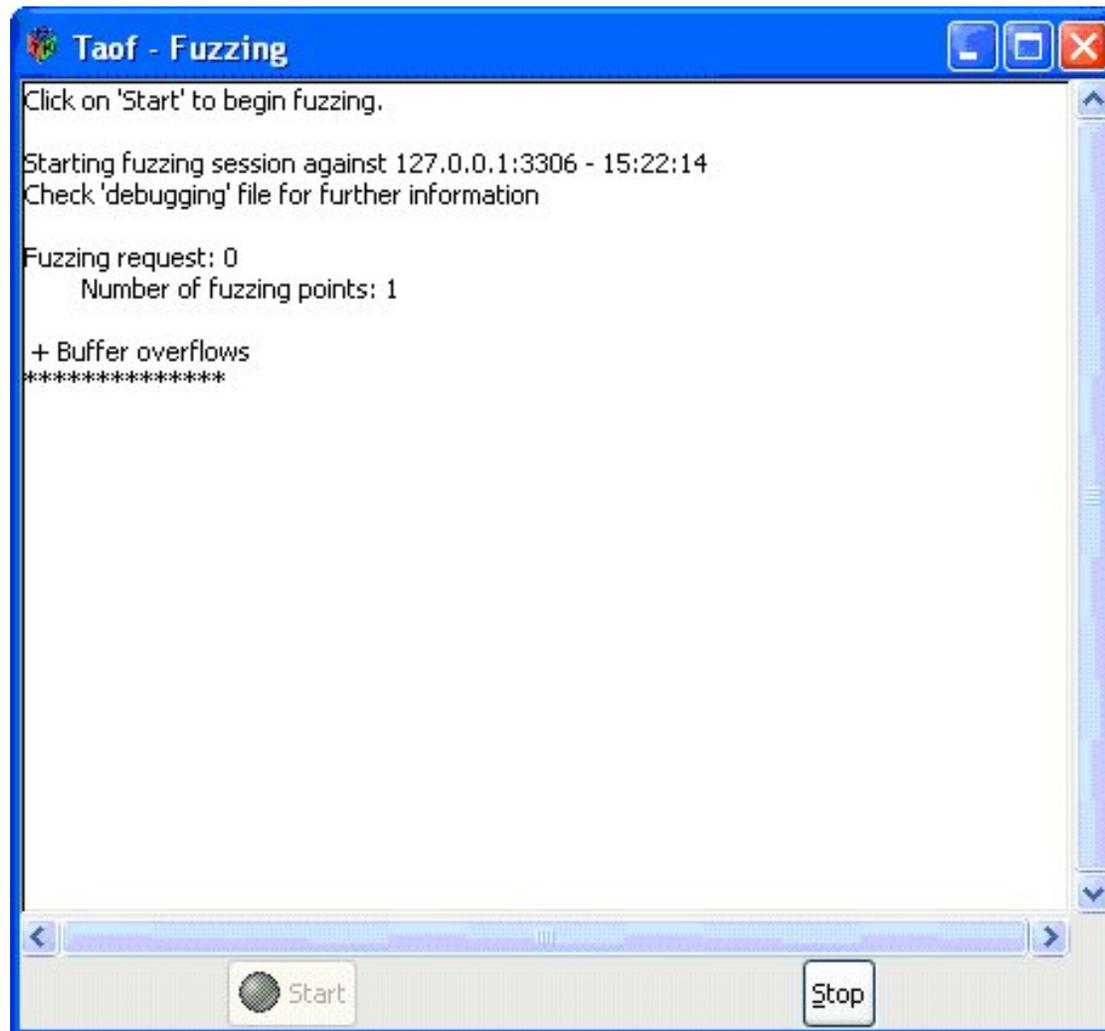
Available file list (tools, code, documents, etc).

Name/Filename	Description	SHA1/MD5
---------------	-------------	----------

Configure gadgets... X

 **Van Hollen To Run Democrats' Fundraising**  
Guardian Unlimited  
Download From AP By JIM ABRAMS/AP WRITER

- **Fuzzing APIs**
  - Scratch Antiparser PeachFuzzer SMUDGE SPIKE
- **TCP/IP Fuzzers**
  - fuzzball2 ISICip6sic Fuzzer CIRT Efuzz
- **Other Protocol Fuzzers**
  - BlueTooth Stack Smasher Radius Fuzzer Mistress Blackops SMTP Fuzzing Tool
- **Generic Fuzzers**
  - dfuz Appliedsec GPF
- **File Fuzzing**
  - File Fuzz
- **Other API Fuzzers**
  - COMRaider AxMan
- **Comercial Products**
  - BreakingPoint Systems beSTORM Codenomiconmu Security Hydra Spirent ThreatX



- **These are Day Zero Vulnerabilities**
  - THERE ARE NO SIGNATURES
- **Changing the code changes the signature – ARMS RACE**
  - Oh My - What if the bad guys automate it?

```
Nov 7 23:11:06 lisa snort[1260]: RPC Info Query:
216.216.74.2:963 -> 172.16.1.107:111
Nov 7 23:11:31 lisa snort[1260]: spp_portscan: portscan
status from 216.216.74.2: 2 connections across 1 hosts:
TCP(2), UDP(0)
Nov 7 23:11:31 lisa snort[1260]: IDS08 - TELNET - daemon-
active: 172.16.1.101:23 -> 216.216.74.2:1209
Nov 7 23:11:34 lisa snort[1260]: IDS08 - TELNET - daemon-
active: 172.16.1.101:23 -> 216.216.74.2:1210
Nov 7 23:11:47 lisa snort[1260]: spp_portscan: portscan
status from 216.216.74.2: 2 connections across 2 hosts:
TCP(2), UDP(0)
Nov 7 23:11:51 lisa snort[1260]: IDS15 - RPC - portmap-
request-status: 216.216.74.2:709 -> 172.16.1.107:111
Nov 7 23:11:51 lisa snort[1260]: IDS362 - MISC - Shellcode
X86 NOPS-UDP: 216.216.74.2:710 -> 172.16.1.107:871
```



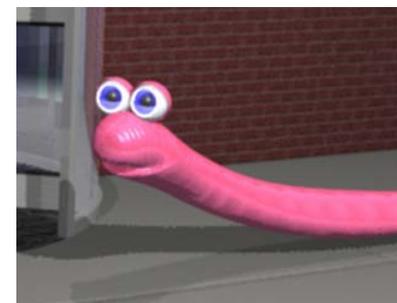
- I've used 5 simple methods, trying to evade being detected by the signature:
  - 1) I've replaced the location where EIP should jump when the exploit is activated, with a different valid address.
  - 2) I've replaced the VML element from "rect" with one of the other VML elements.
  - 3) I've replaced the payload with a different valid shell code.
  - 4) I've replaced the namespace key with a random key.
  - 5) A combination of all of the above.
- Please note that when I changed the code using any of the methods, the exploit still worked.
- The following is the results of each evasion method, when tested using Virus Total:
  - 1) Only 8 of the 10 Anti-Viruses detected the exploit.
  - 2) Only 6 of the 10 Anti Viruses detected the exploit.
  - 3) Only 5 of the 10 Anti-Viruses detected the exploit.
  - 4) Only 5 of the 10 Anti-Viruses detected the exploit.
  - 5) Only 1 (one!) of the 10 Anti-Viruses detected the exploit.
- As you can see, evading AV/IPS/IDS signatures of web page exploits is too easy.

<http://blog.info-pull.com/2006/10/13/vml-exploit-and-idsantivirus-engines-evasion-doom-or-vomm/>

- **A new worm called Warezov aka Stration, Stratio is providing signature evasion by creating a new version every 30 minutes and updating already infected machines with the new code**
- **Over 300 variations have already been seen in the wild**
- **According to at least one AV company this worm was the most common malware found in spam messages for the month of October and a few hundred thousand computers are already infected**
- **One can safely assume that this worm is but a preview of things to come**

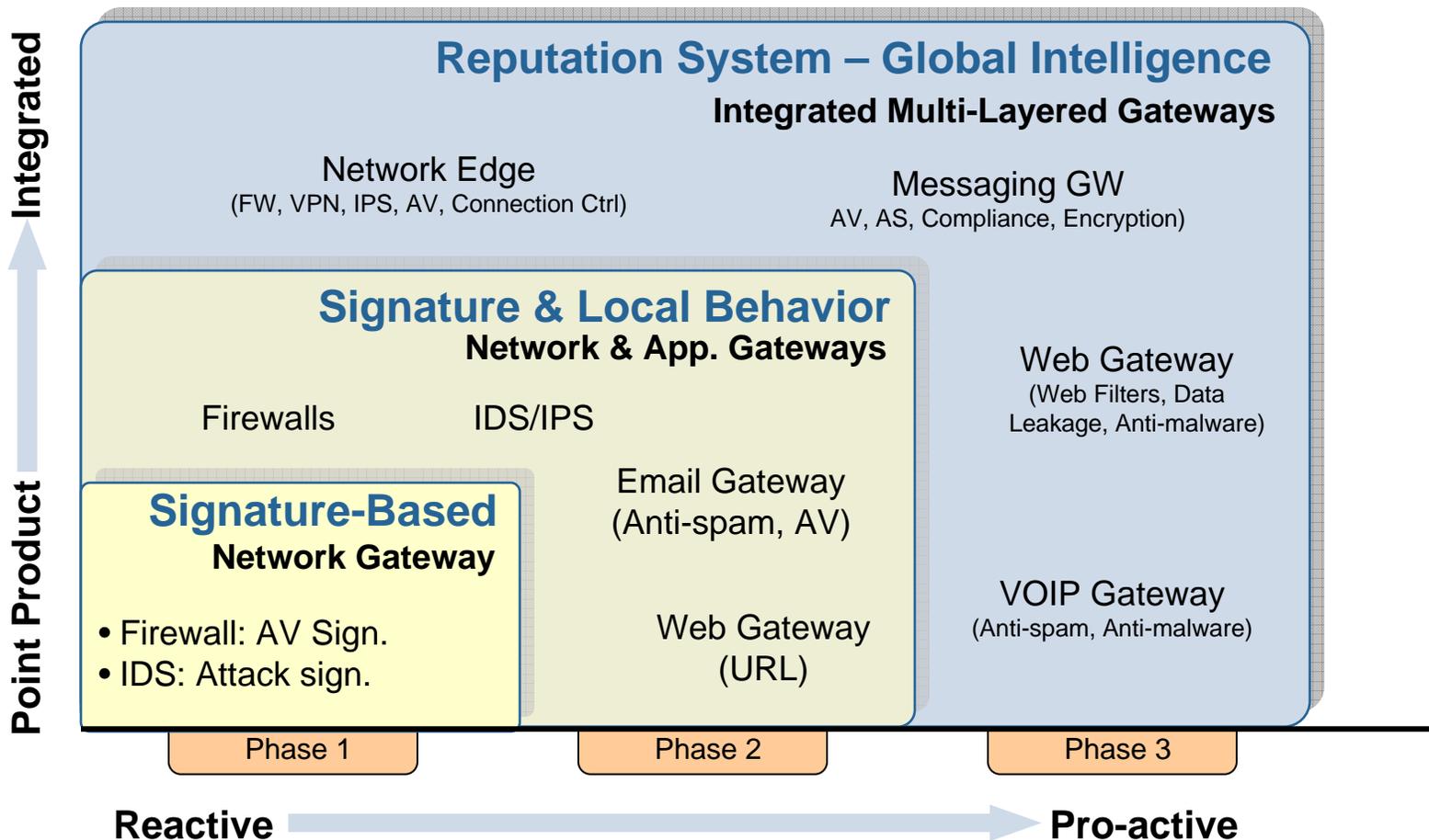
Known "Bad"	
Year	CVE Entries
1999	1,589.00
2000	1,241.00
2001	1,580.00
2002	2,218.00
2003	1,565.00
2004	2,665.00
2005	4,813.00
2006	5,381.00
<b>Total</b>	<b>21,052.00</b>

500 new  
+ vulnerabilities +  
each month

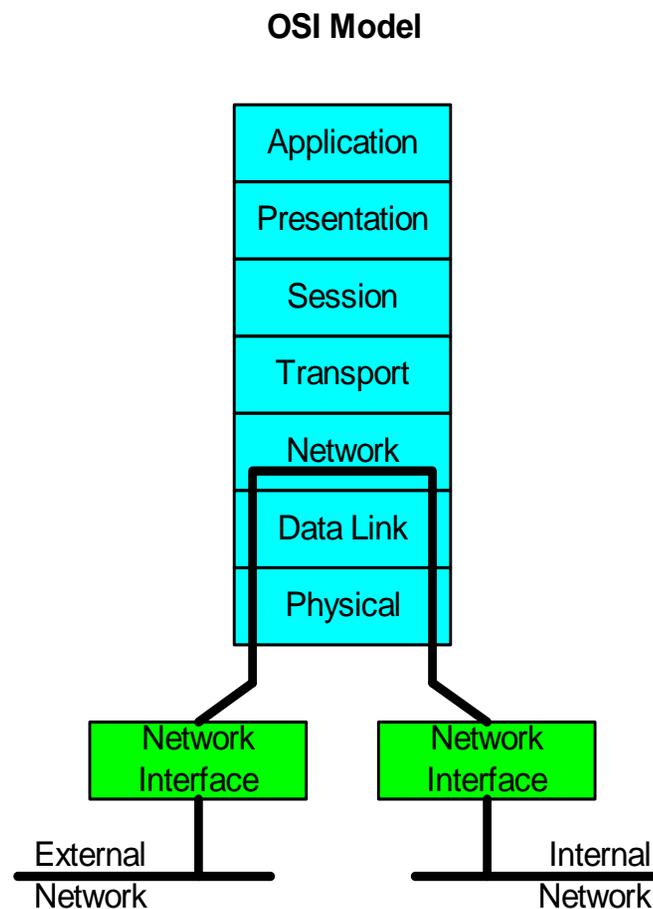


***Signature-based defenses  
are obsolete!***

- Shift from Defending-Forward to Global Defense



- **Application layer “Filtering” Band Aid is now simply obsolete**
- **Your left with nothing but a Stateful packet filter**
  - Offers no protection
    - Never sees the exploit



- **Negative Security Model**
  - ***Allow all traffic*** to freely stream through the security device
  - Then...***identify the bad***
    - The bits of traffic which are ***known to be threatening***
    - Typically depend on checking against ***attack signatures***
  - ***Anti-virus and IPS systems*** are classic examples
  - These countermeasures have ***less and less time to react*** to new attacks
  - New hacking tools like VoMM eliminate any chance of detection with a signature

- **Positive Security Model**
  - *Only allow legitimate traffic!...*
  - ...and then...*deny everything else!*
  - Positive security countermeasures are extremely effective at *preventing unknown attacks*
  - Simply configure the countermeasure to *understand all legitimate, acceptable traffic requirements*
  - *Known behavior is the key baseline* used to check all traffic against
- **An easy way to remember the difference between the two methodologies is:**
  - *Negative security model based products attempt to enumerate all of the bad while positive security model based products only allow that which has been defined by the administrator as good.*

## Physical World



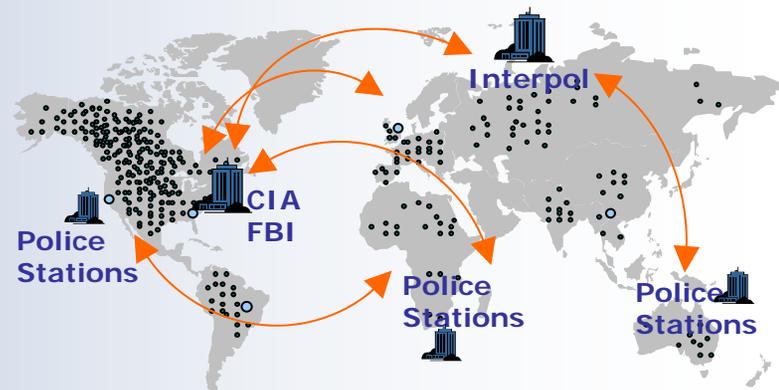
Intelligence Agents

**Deploy agents**  
officers around the globe  
(Police, FBI, CIA, Interpol.)

**Global intelligence system**  
Share intelligence information  
Example: criminal history, global fingerprinting system

**Results**

**Effective:** Accurate detection of offenders  
**Pro-active:** Stop them from coming in the country



## Cyber World



Intelligent probes

**Deploy security probes**  
around the globe (firewall, email gateways, web gateways)

**Global intelligence system**  
Share cyber communication info, Example: spammers, phishers, hackers

**Results**

**Effective:** Accurate detection of bad IPs, domains  
**Pro-active:** Deny connection to intruders to your enterprise



SANS SANS Homepage SANS Bookstore SANS Reading Room SANS Portal

**GREEN** **IT Security**  
Where IT Security professionals start their day.  
[www.itsecurity.com](http://www.itsecurity.com)  
Ads by Google - Advertise on this site

**SC AWARDS 2006**

**Handler on Duty: Tom Liston** 19:29:15 UTC Dec 19 2006, 15:29:15 Dec 19 2006

Trends Top 10 Reports Contact About INFOCon Presentations Links XML print

Handler's Diary: Soap Boxing;Skype 'worm' whinnies...

## Handler's Diary December 18th 2006

[previous](#) - [next](#)

### Skype worm

**Changes between the current version and version 1 are highlighted.**

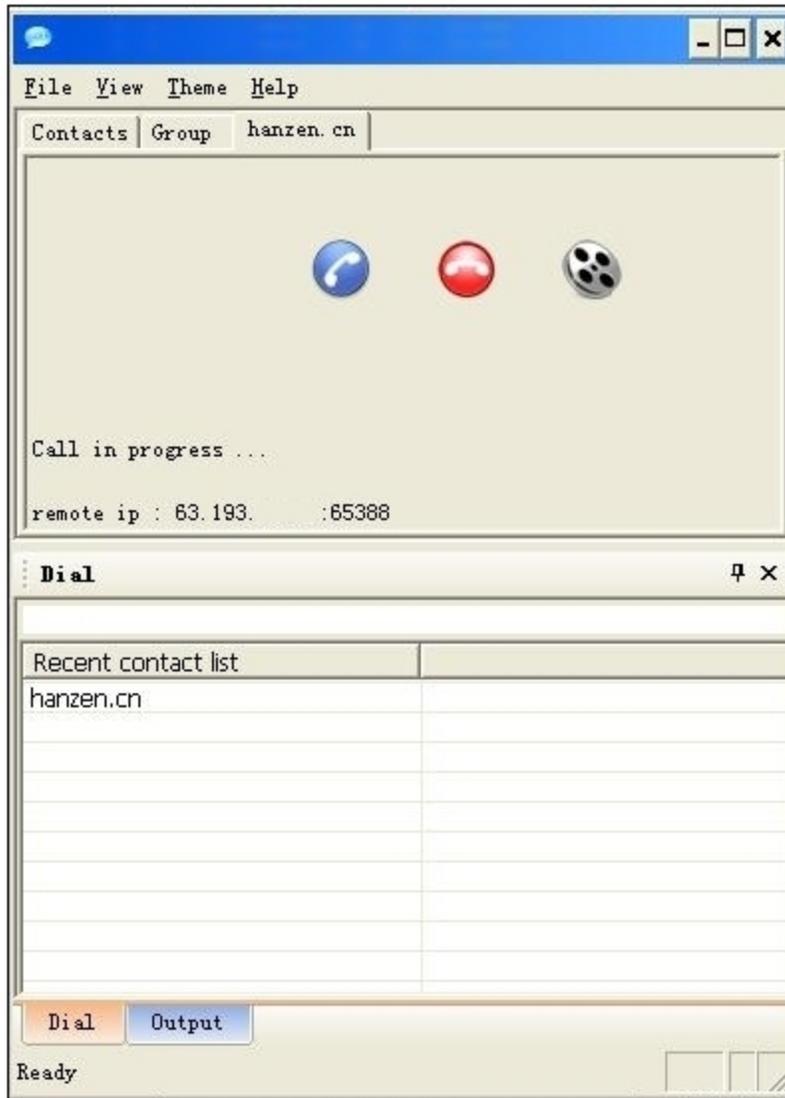
Published: 2006-12-18,  
Last Updated: 2006-12-18 23:54:28 UTC by Toby Kohlenberg (Version: 2)

We are hearing some details of a new worm spreading via Skype IM, it appears to be using a custom (or at least unusual) packer and the network traffic appears encrypted as well. Please send us any info you might have on it.

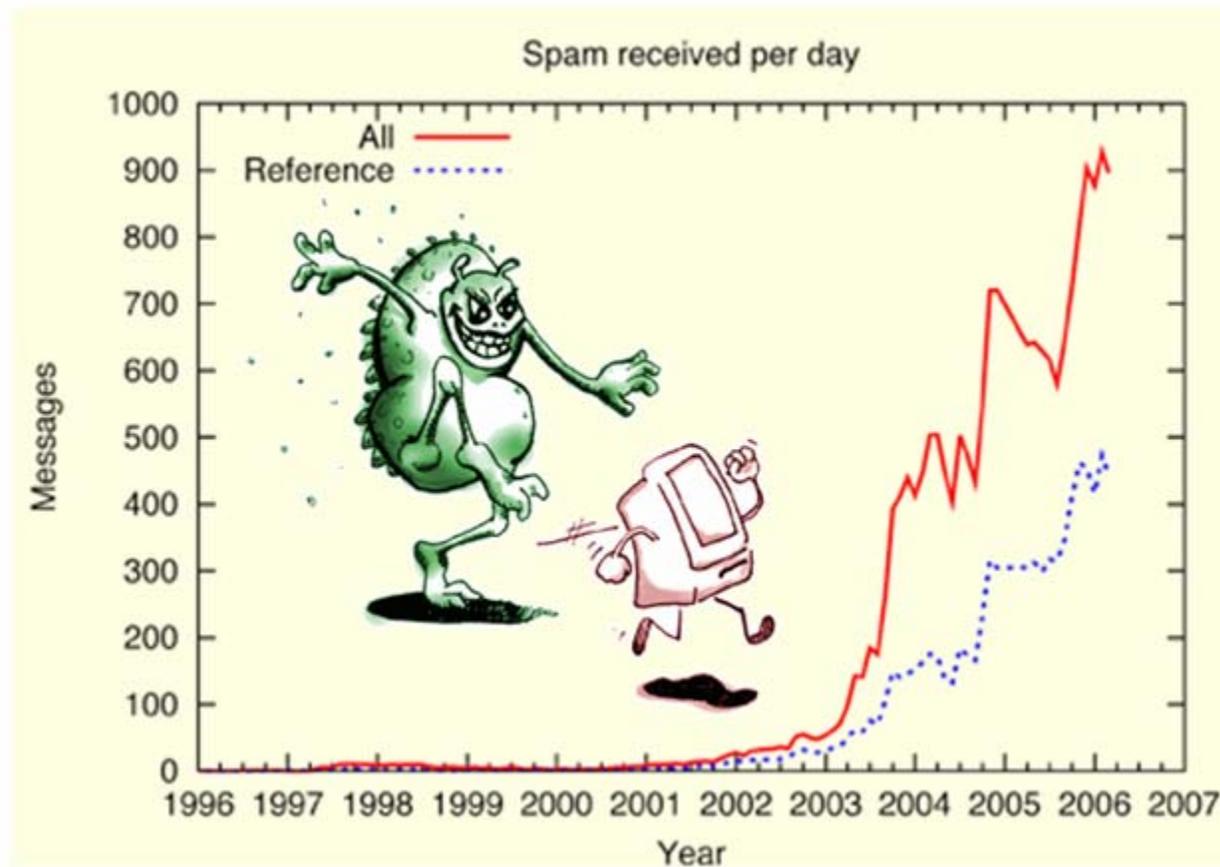
Thanks for the responses, we do know about the Websense blog post.

[previous](#) - [next](#)

SANS 2007



- **Only permit outbound connections that meet the business needs of the organization**
- **For permitted connections use a proxy that supports:**
  - Generic Body Filter to provide the ability to identify Skype connections
  - SSL scanner to identify “proper” SSL usage
    - Skype SSL is not protocol compliant hence can be easily blocked
- **Use desktop antivirus that provides real-time scanning to provide scanning of attachments in Chat conversations as they are decrypted by Skype**



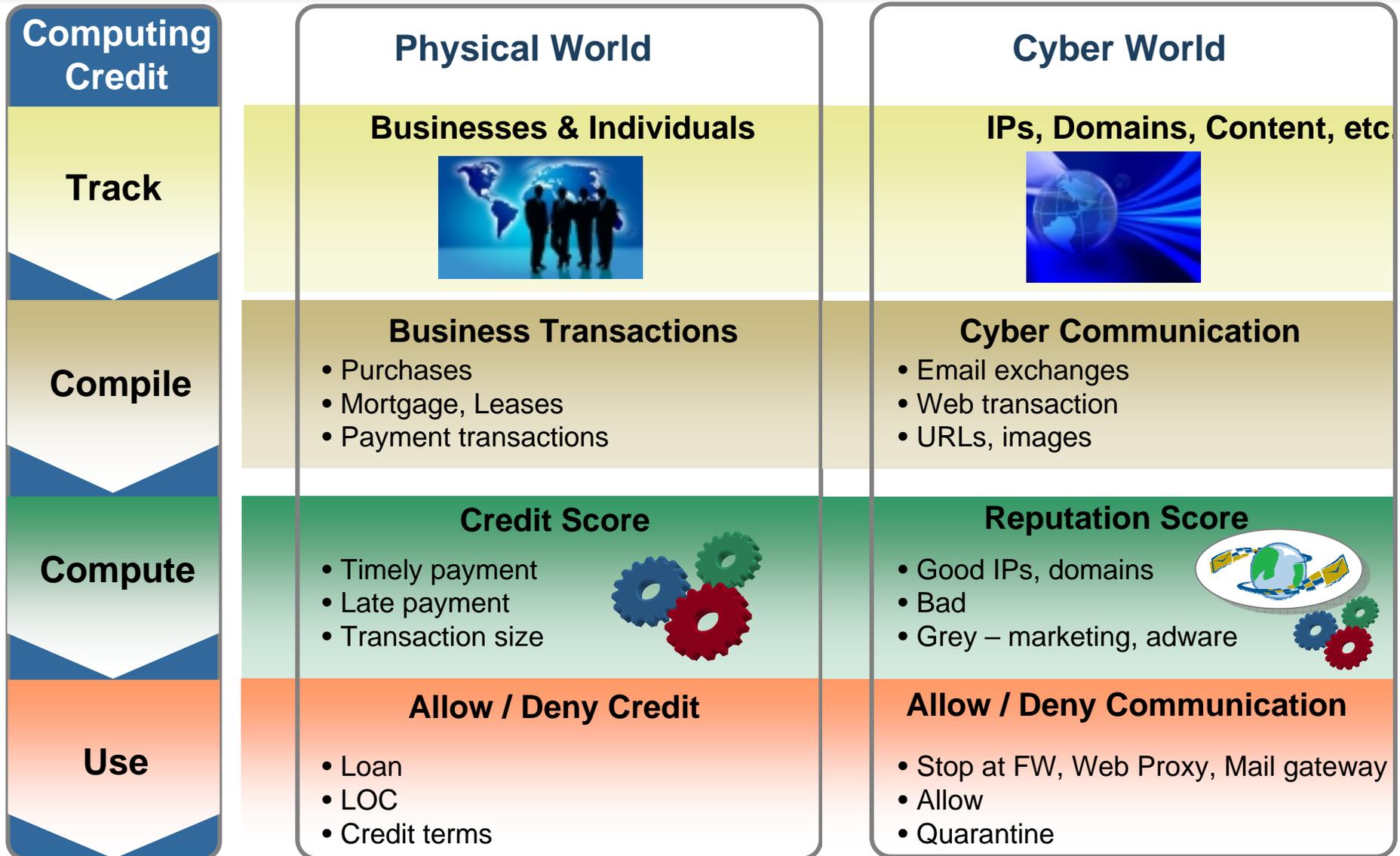
- **Remain Anonymous**
- **Fast – blanket the world in seconds**
- **Click Here – still effective**
  - Patch for Human 1.0 still not yet released
- **Preview pane eliminates the need for “Click here”**
- **Vehicle of choice for malware**

**Survey: More phishing suckers out there than we thought**

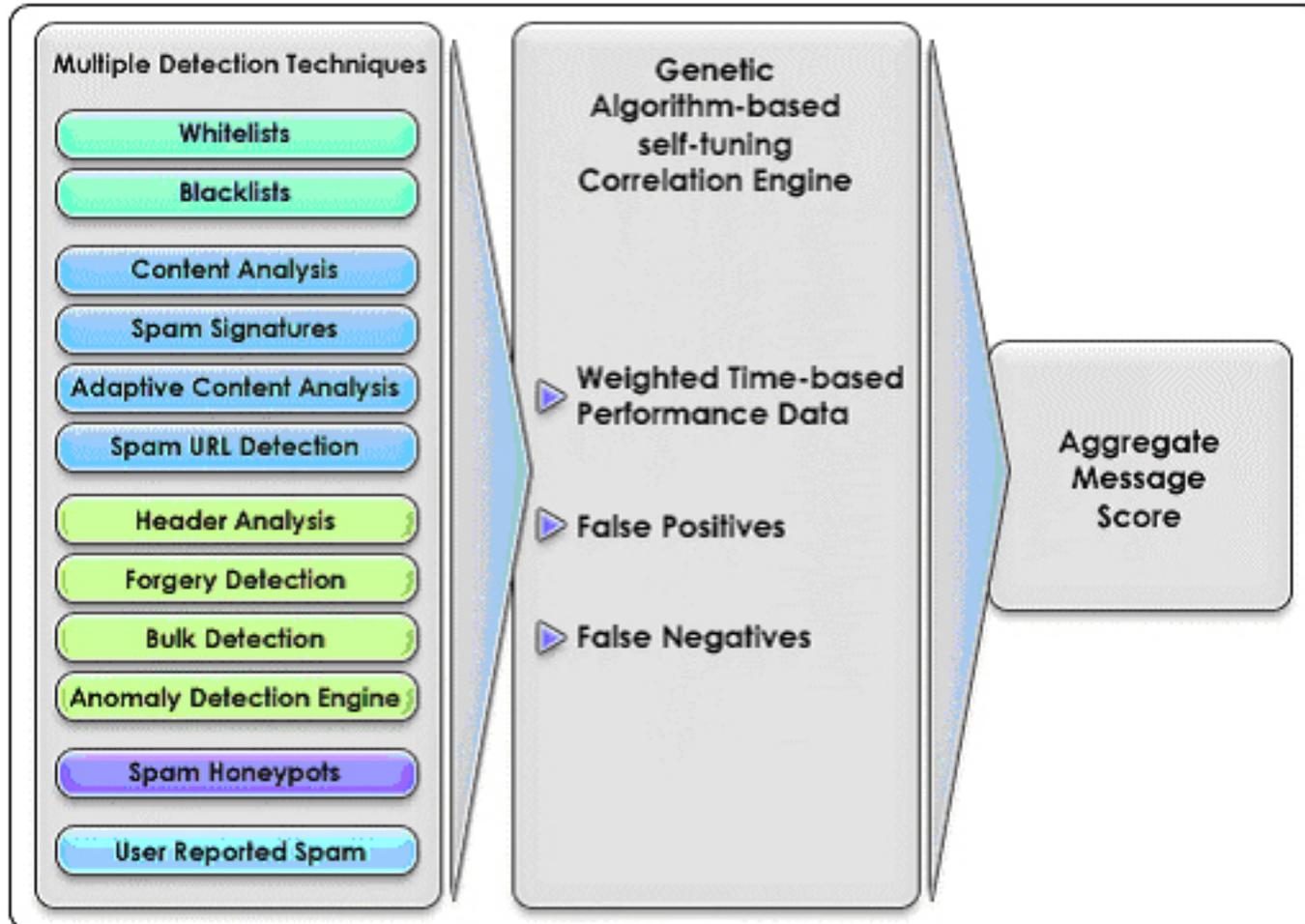
**Indiana University simulates e-mail scams used to swipe data from eBay customers.**

*By Network World staff, Network World, 10/18/06*

Phishers might be getting takers on as much as 14% of their trick messages, much higher than previous estimates by network security watchers, according to a University of Indiana study.

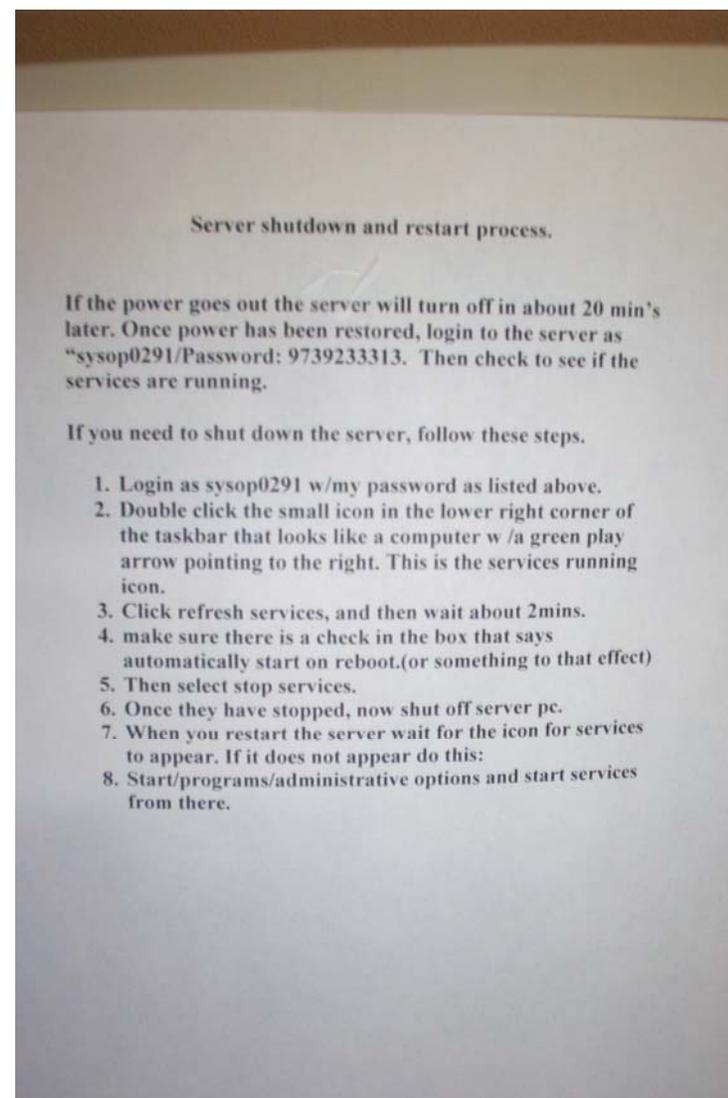


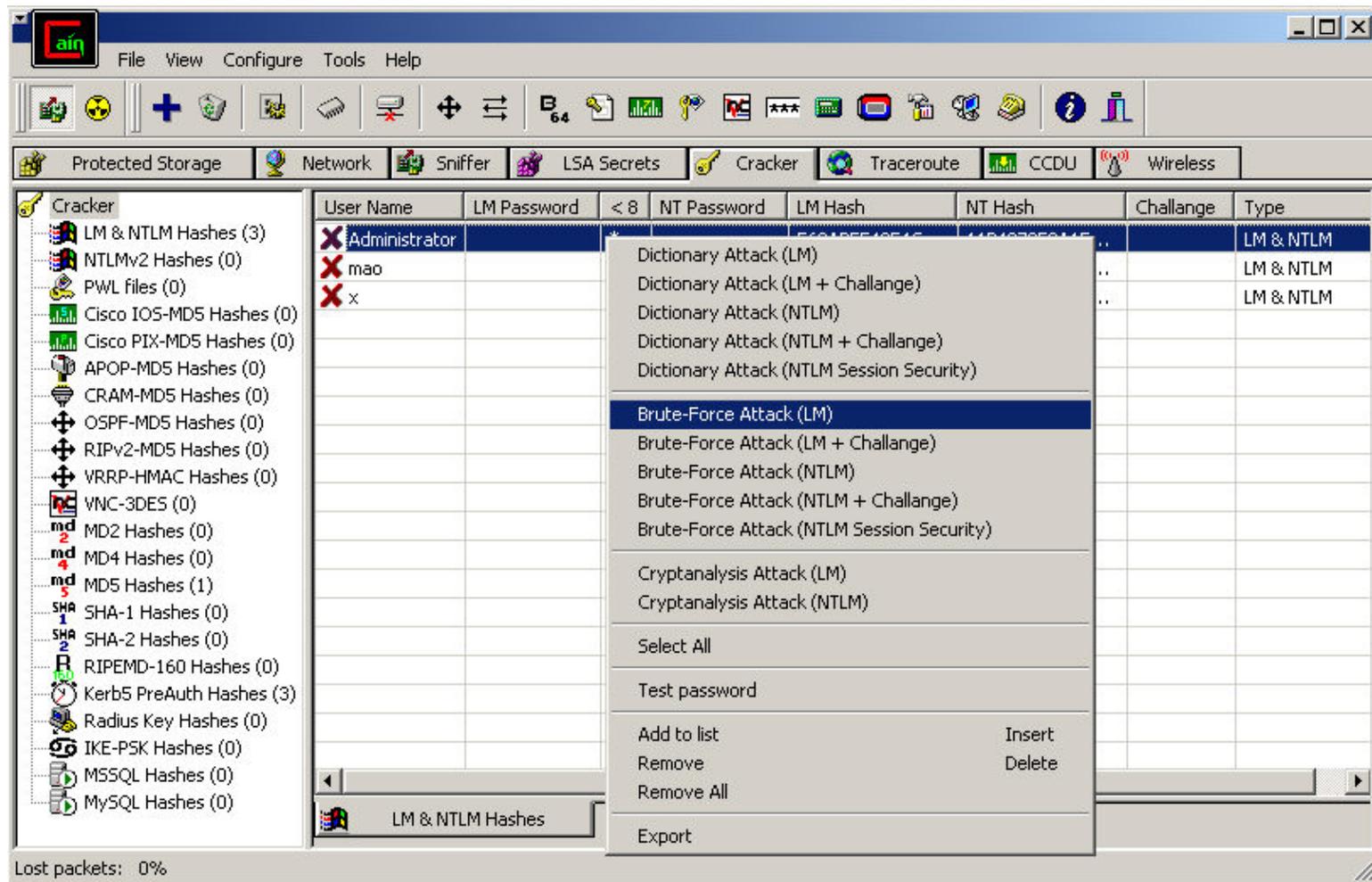
# Not your Grandfathers Blacklist...



- **Trying to filter email content puts you in an arms race with the spammers**
  - Reputation based defenses should be your first layer of defense
  - Filtering has it's place – but only as a second layer of defense
- **SPAM is part of an overall blended threat and can only be effectively mitigated with a multilayer approach:**
  - Multilayer security approach is the most effective solution
    - AntiSpam
    - AntiVirus
    - Application Layer Defenses – Positive Security Model
    - Global Intelligence – Reputation score
- **Anti-spam methodologies can benefit dramatically from the shift from Defending-Forward to Global Defense**
  - Dolt.... Don't accept email from known spammers and Botnets

*"There is no doubt that over time, people are going to rely less and less on passwords. People use the same password on different systems, they write them down and they just don't meet the challenge for anything you really want to secure." Bill Gates 2004*



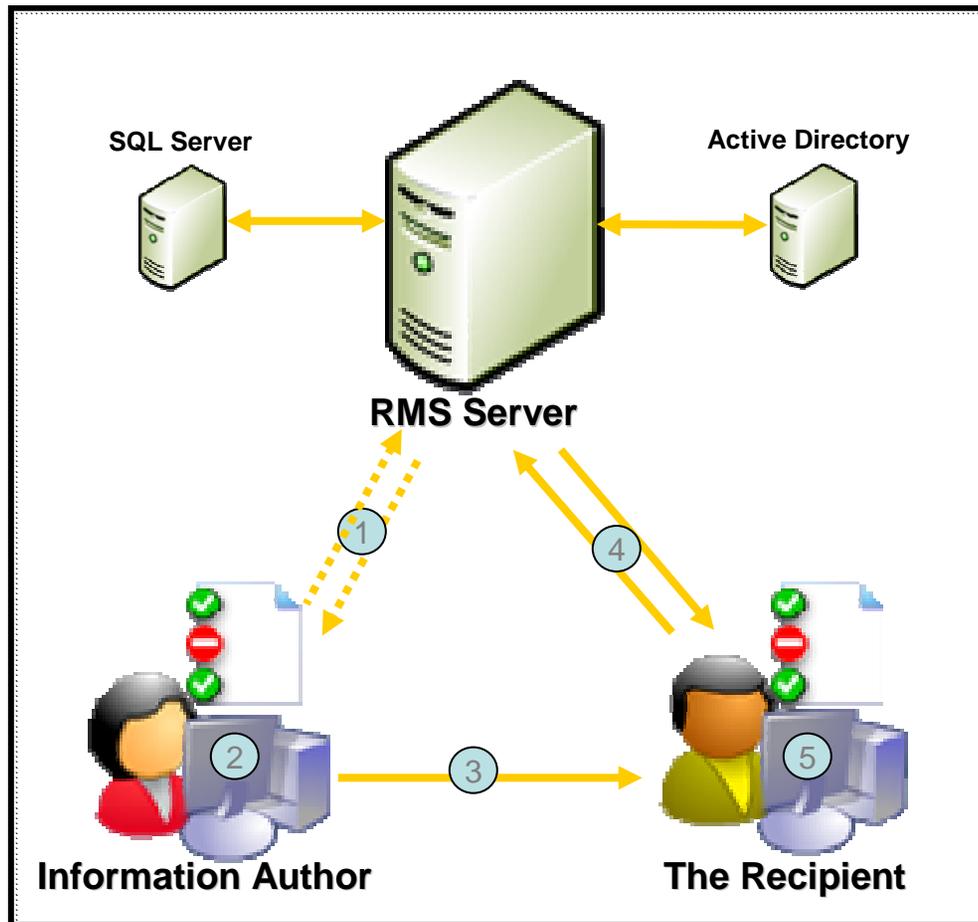


- **Rainbow Tables**

- Pre-computed hashes for every possible combination of letters, numbers and symbols
- Perfect in a Windows environment
- Has also been implemented for MD5 Hashes



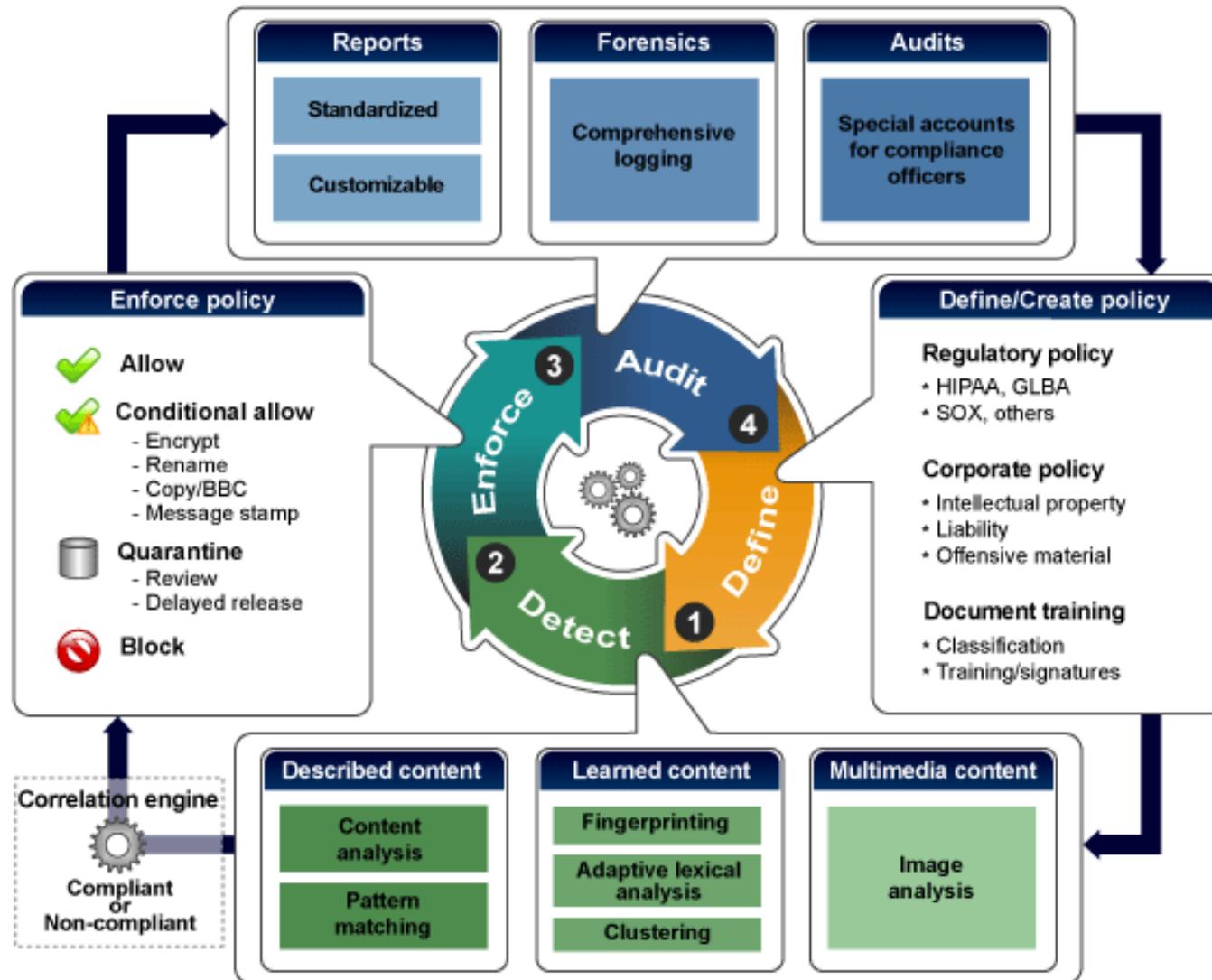
- **In-Band authentication will be hacked – it is simply a matter of time**
  - Remember “On Screen” Keyboards ;-)
- **Two Factor Authentication; Out-Of-Band in the form of SmartCards, Tokens or Biometrics are the only effective solutions**
  - If the hacker can't touch it he/she can't hack it
- **Authentication can also benefit in the shift from Defending-Forward to Global Defense**
  - Risk mitigation from Man-In-The-Middle attack
  - Risk mitigation from user mistakenly authenticating from compromised (Trojaned) PC - I.e. Kinko's or airport lounge



1. Author receives a client licensor certificate (CLC) the first time they rights-protect information.
2. Author defines a set of usage rights and rules for their file; Application creates a "publishing license" and encrypts the file.
3. Author distributes file.
4. Recipient clicks file to open, the application calls to the RMS server which validates the user and issues a "use license."
5. Application renders file and enforces rights.

- **According to Microsoft DRM is not:**
  - ...100% unbreakable, hacker-proof security
  - ...A complete security solution by itself
  - ...Protection against analog attacks
- **While eliminating the need to create a data dictionary it still requires that the user assign rights to each and every document**
  - Administrative workload is actually higher than alternate solutions
  - Secure Content Management (SCM) offers lower administrative overhead
- **Simply put DRM places too much control in the hands of the user**
  - There is no safety net for user error in rights assignment
  - What about the disgruntled user
  - SCM provides the safety net missing in DRM

# Learned Content is a better alternative



- **SCM is clearly a more secure alternative to DRM**
  - Eliminates user error in rights assignment
  - Provides a safety net for user error
  - Works across multiple protocols
  - Data dictionaries take the user out of the equation
- **Automatic Learned Content is the next generation**
  - Drop the file in a folder and it automatically learns the content

- **Application attacks are still seeing explosive growth**
  - Application defenses, Positive Security Model and Global Intelligence affords the most effective risk mitigation
- **VOIP risks are increasing**
  - Non standard protocols prevent policy enforcement
  - If it can not be secured it must be blocked
- **Email continues to grow as a threat vector**
  - Fueled by Botnets SPAM represents 95% of received email
  - Reputation based systems can reduce Spam by 80% without the overhead of filtering
- **Passwords are simply obsolete**
  - Out-Of-Band Two Factor Authentication is the only effective solution and when combined with Global Intelligence offers the highest risk mitigation
- **The Data leakage issue can not be solved by DRM**
  - SCM reduces the associated risks but carries administrative burden
  - Automatic – Learned Content eliminates the risk while at the same time minimizing administrative burden

# Questions?

# Thank You

## Paul A. Henry

*MCP+I, MCSE, CFSA, CFSO, CCSA, CCSE, CISM, CISA, CISSP, ISSAP, CIFI*

Vice President, Technology Evangelism

Secure Computing

Paul\_henry@securecomputing.com