# LogChaos: Challenges and Opportunities of Security Log Standardization

Dr. Anton Chuvakin

**Security Warrior Consulting**

Oct 2009

# Outline

You’ve heard about the solution …

… now comes the problem:

- World of logs today
  - Log chaos? Why? Why order is sorely needed!
- Past attempts to bring order chaos!
  - Why ALL failed?
- What does the future hold?

CAUTION
CHAOS FIELD
ESTIMATED STRENGTH: 47 KrZ
LIMIT EXPOSURE TO THIS AREA
AND REPORT ABNORMALITIES
IN YOUR LIFE AFTER EXPOSURE

# Log Data Overview

## What Logs?

- Audit logs
- Transaction logs
- Intrusion logs
- Connection logs
- System performance records
- User activity logs
- Various alerts and other messages

## From Where?

- Firewalls/intrusion prevention
- Routers/switches
- Intrusion detection
- Servers, desktops, mainframes
- Business applications
- Databases
- Anti-virus
- VPNs

# From Log Analysis to Log Management

- **Threat** protection and discovery
- **Incident** response
- **Forensics**, “e-discovery” and litigation support

- Regulatory **compliance** and **audit**
- Internal **policies** and procedure compliance

- IT system and network **troubleshooting**
- IT **performance** management

# Log Chaos I - Login?

```
<18> Dec 17 15:45:57 10.14.93.7 ns5xp: NetScreen
device_id=ns5xp system-warning-00515: Admin User netscreen
has logged on via Telnet from 10.14.98.55:39073 (2002-12-17
15:50:53)
```

```
<57> Dec 25 00:04:32:%SEC_LOGIN-5-
LOGIN_SUCCESS:Login Success [user:yellowdog]
[Source:10.4.2.11] [localport:23] at 20:55:40 UTC
Fri Feb 28 2006
```

```
<122> Mar  4 09:23:15 localhost sshd[27577]: Accepted password for
kyle from ::ffff:192.168.138.35 port 2895 ssh2
```

```
<13> Fri Mar 17 14:29:38 2006 680 Security SYSTEM User
Failure Audit ENTERPRISE Account Logon
Logon attempt by: MICROSOFT_AUTHENTICATION_PACKAGE_V
1_0    Logon account:  POWERUSER
```

# Log Chaos II - Accept?

Juniper

```
messages:Dec 16 17:28:49 10.14.93.7 ns5xp: NetScreen device_id=ns5xp  system-notification-00257(traffic): start_time="2002-12-16 17:33:36" duration=5 policy_id=0 service=telnet proto=6 src zone=Trust dst zone=Untrust action=Permit sent=1170 rcvd=1500 src=10.14.94.221 dst=10.14.98.107 src_port=1384 dst_port=23 translated ip=10.14.93.7 port=1206
```

Check Point
We Secure the Internet.

```
Apr  6 06:06:02 Checkpoint NGX SRC=Any,DEST=ANY,Accept=nosubstitute,Do Not Log,Installspyware,lieonyourtaxes,orbetteryet,dontpaythem
```

Cisco Systems

```
Mar  6 06:06:02 winonasu-pix %PIX-6-302013: Built outbound TCP connection 315210 596 for outside:172.196.9.206/1214 (172.196.9.206/1214) to inside:199.17.151.103/1438 (199.17.151.103/1438)
```

# Log Chaos Everywhere!

- No standard format
  - **No standard schema, no level of details**
- No standard meaning
  - **No taxonomy**
- No standard transport
- No shared knowledge on what to log and how
- No logging guidance for developers
- No standard API / libraries for log production

# Result?

```
%PIX|ASA-3-713185 Error: Username too long - connection aborted

%PIX|ASA-5-501101 User transitioning priv level

ERROR: transport error 202: send failed: Success

sles10sp1oes oesaudit: type=CWD msg=audit(09/27/07 22:09:45.683:318) :  cwd=/home/user1
```

# More results?

```
userenv[error] 1030 RCI-CORP\wsupx No description available
```

```
Aug 11 09:11:19 xx null pif ? exit! 0
```

```
Apr 23 23:03:08 support last message repeated 3 times
Apr 23 23:04:23 support last message repeated 5 times
Apr 23 23:05:38 support last message repeated 5 times
```

# But This … **This Here <u>Takes The Cake</u>…**

1. Logging usernames *AND passwords* to “debug” authentication (niiiice! ☺)
2. Logging *numeric error codes* – and not having documentation *ANYWHERE*
3. Logging *chunks of source code* to syslog (care to see a 67kB syslog message? ☺)

# Chaos2order: Why Logging Standards?

- **Common language**
- **Easier to report** on logs and explain the reports
- **Deeper insight** into future problems
- Easier system **interoperability**
- Common logging **practices**
- Easier to explain what is in the logs to **management and non-IT people**

# What Becomes Possible?

- All those super-smart people at SIEM vendors can **stop parsing** and **start analyzing**
  - What the events mean? Consequences? Actions? Maybe even prediction?
- Different systems can **mitigate consequences of each others' failures**
- We can finally tell **the developers "what to log?"** and have them "get it!"

# Various Logging Standards by Type

- **Log format**
  - Example: Syslog, *a non-standard standard*
  - Example: IDMEF, a failed standard
- **Log contents**
  - No standard to speak of: *logs = trash can* because application developers dump what they want there (and how they want!)
- **Log transport**
  - Example: Syslog (TCP/UDP port 514)
- **Logging practices / recommendations**
  - Example: NIST 800-92 (for security only)

# Old, Dead and Vendor Log Standards

*Old, mostly dead standards:*

- **CIDF** – DARPA (became IDMEF)
- **IDMEF** – IETF (never adopted by *anybody*)
- **CIEL** – MITRE (cancelled early)
- **XDAS** – Open Group

*Vendor “standard” efforts:*

- **CBE** - IBM
- **WELF** - Webtrends
- **CEF** - ArcSight
- **OLF** – eIQnetworks
- **SDEE** – Cisco+

# Example: IDMEF

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IDMEF-Message PUBLIC "-//IETF//DTD RFC XXXX IDMEF v1.0//EN“ "idmef-message.dtd">
<IDMEF-Message version="1.0">
<Alert ident="abc123456789">
<Analyzer analyzerid="hq-dmz-analyzer62">
<Node category="dns">
<location>Headquarters Web Server</location>
<name>analyzer62.example.com</name>
</Node>
</Analyzer>
….
```

# Outcome: Died of Old Age in Obscurity

Lessons learned:

- When building a standard, think about adoption
- Think about use cases, current and hopefully future
- Complexity =/= broad use (the opposite!)
- Limit academic input ☺

# Example: WELF

```
WTsyslog[1998-08-01 00:04:11 ip=10.0.0.1
  pri=6] id=firewall time="1998-08-01
  00:08:52" fw=WebTrendsSample pri=6
  proto=http  src=10.0.0.2 dst=10.0.0.3
  dstname=1.example.com
  arg=/selfupd/x86/en/WULPROTO.CAB
  op=GET result=304 sent=898
```

# Outcome: Lives Happily in Oblivion ☺

Lessons learned:

- If you use something and like it, it does not make it a standard
- If you go outside of intended use cases, FAIL happens.

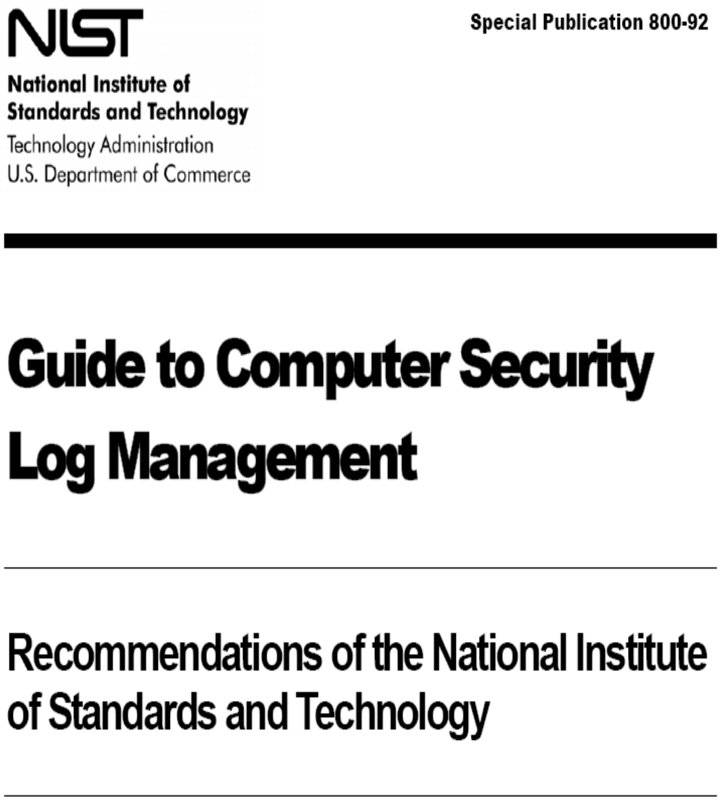
# What Killed’em ALL?

**Lack of adoption – BIG one!**

- “Solution in search of a problem”
- “Overthinking” designers
- Standard complexity
- Emphasis on XML
- Vendors and their tactical focus (or “marketing standards”)
- Narrow approach (e.g. just security)

# What Worked? **NIST 800-92 Guide to Log Management**

"This publication seeks to assist organizations in understanding the need for sound computer security log management. It provides practical, real-world guidance on developing, implementing, and maintaining effective log management practices throughout an enterprise. "



NIST

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-92

Guide to Computer Security Log Management

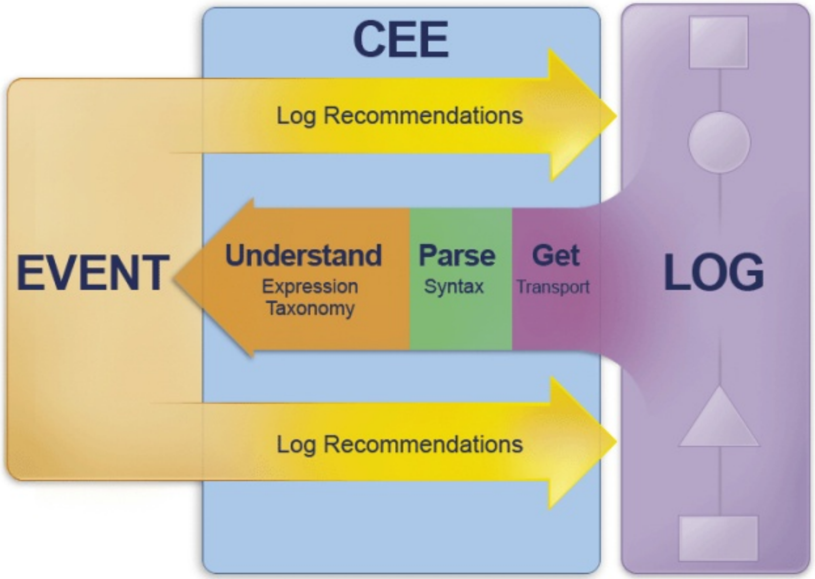
Recommendations of the National Institute of Standards and Technology

# Pause …

How we want the world of logging to look like?

# Common Event Expression (CEE)

*CEE = Syntax + Vocabulary + Transport + Log Recommendations*



- *Common Event Expression Taxonomy*
  - To specify the event in a common representation
- *Common Log Syntax*
  - For parsing out relevant data from received log messages
- *Common Log Transport*
  - For exchanging log messages
- *Log Recommendations*
  - For guiding events and details needed to be logged by devices (OS, IDS, FWs, etc)

Common Event Expression Impacts

- Log management capabilities
- Log correlation (SIEM) capabilities
- Device intercommunication enabling autonomic computing
- Enterprise-level situational awareness
- Infosec attacker modeling and other security analysis capability

# Conclusions: Future of Log Standards

- Log standard is sorely needed
  - About 30 years of IT has passed by without it
- CEE standard **will be created**; CEE team has learned the lessons of others
- CEE standard has a higher chance than any standard to be adopted
  - OK fine: “CEE standard **will be adopted**!” ☺

**Let’s get to work!**

**LogChaos must die! ☺**

# Questions?

**Dr. Anton Chuvakin**

**Principal @ Security Warrior Consulting**

**Email:** anton@chuvakin.org

**Google Voice:** 510-771-7106

**Site:** http://www.chuvakin.org

**Blog:** http://www.securitywarrior.org

**LinkedIn:** http://www.linkedin.com/in/chuvakin

**Twitter:** *@anton_chuvakin*

# More on Anton

- **Book author:** “Security Warrior”, “PCI Compliance”, “Information Security Management Handbook”, “Know Your Enemy II”, “Hacker’s Challenge 3”, etc
- **Conference speaker:** SANS, FIRST, GFIRST, ISSA, CSI, Interop*, many, many others worldwide*
- **Standard developer:** CEE, CVSS, OVAL, etc
- **Community role:** SANS, Honeynet Project, WASC, CSI, ISSA, OSSTMM, InfraGard, ISSA, others
- **Past roles:** Researcher, Security Analyst, Strategist, Evangelist, Product Manager, Consultant