Vulnerability Disclosure

Penetration Testing and Vulnerability Analysis

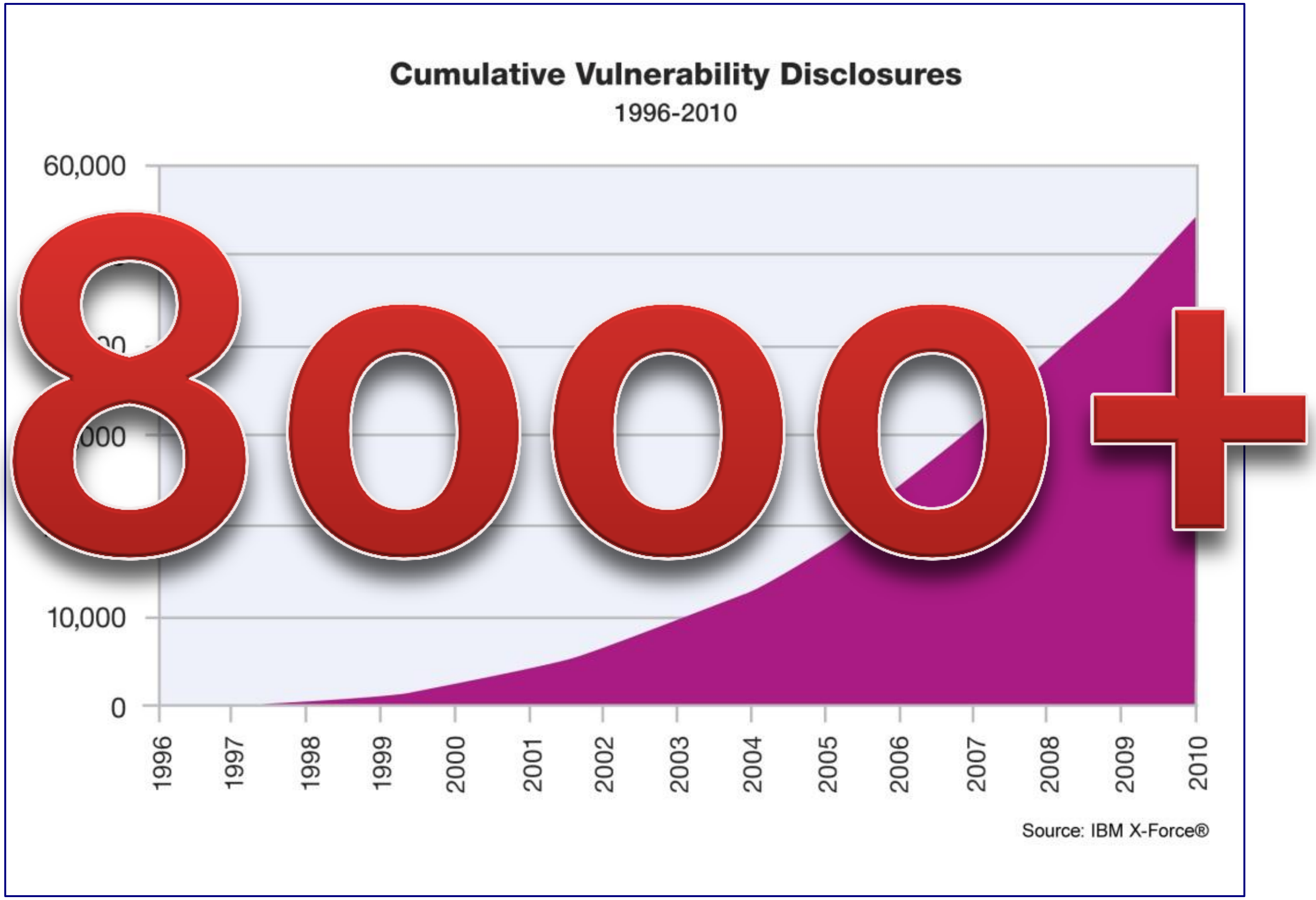
Dan Guido

Fall 2011

Background

Corbis/Alamy

Let’s Talk About Vulnerabilities



Source: IBM X-Force®

*IBM X-Force 2010 Trend and Risk Report

The Vulnerability Industry

- Companies pay to have them tracked
  - ZDI, iDefense, Secunia, Symantec

- Used as marketing tools by orgs and individuals
  - CORE, VUPEN, Tavis

- Purchased by vendors
  - Google, Mozilla, Barracuda, Facebook

- Consulting industry revolves around vuln mitigation
  - iSEC, Matasano, GDS, Intrepidus, etc etc

The Vulnerability Underground

- Rapidly consumed by mass malware
  - Crimepacks like Blackhole, Eleonore, and Mpack

- Used for fun by script kiddies everywhere!
  - Anyone see kernel.org get compromised last week?

- Discovered in the wild fairly regularly
  - Flash, Shockwave, IE, Windows kernel
  - APT groups, coordinated exfil of IP from US corps

How We Got Here

The Early Days

- Limited discussion of general security issues pre-89
  - Rutgers Security List
  - UNIX Security Mailing List

- Somewhat earlier, a wild Phrack appeared
  - First published in 1985
  - Original hacker e-zine, attacker-focused
  - Helped organize a community around offense

- Security is a problem, but nobody knows it yet

Private Communities Evolved

- Then the Morris Worm happened in 1988
  - Now it’s a problem and everyone knows it
  - Invite-only mailing lists set up in response
    - Zardoz, Phage, and Core

- MASSIVE target for hackers
  - http://www.underground-book.net/
    - Actually described zardoz as “The Holy Grail”
  - Archives widely circulated underground, parodied in Phrack

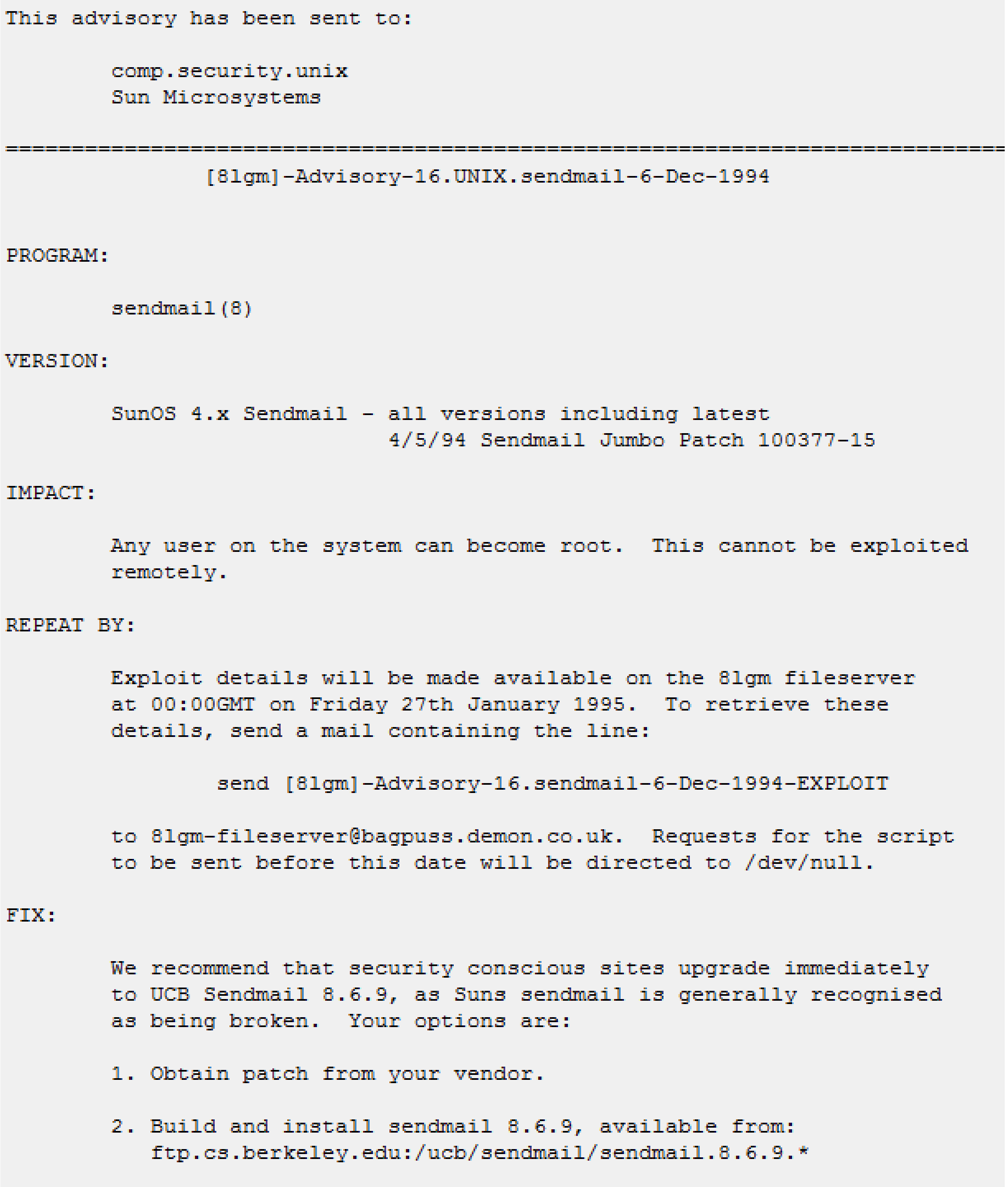
- Limited motivation to act if details are private
  - “Hey, this is interesting”
  - Brittle and ineffective at stated purpose

Full Disclosure

- Eight Legged Groove Machine Security Advisory Service (8LGM) releases first modern advisories in '93
  - http://www.8lgm.org

- Basic format remains unchanged through today
  - Affected software and OS's
  - Description of impact
  - Fix and workaround information
  - Reported to vendor and to the public

- *Extremely* controversial at the time
  - Trend continued by lopht and eEye throughout the 90s



```
This advisory has been sent to:

        comp.security.unix
        Sun Microsystems

===========================================================================
              [8lgm]-Advisory-16.UNIX.sendmail-6-Dec-1994


PROGRAM:

        sendmail(8)

VERSION:

        SunOS 4.x Sendmail - all versions including latest
                             4/5/94 Sendmail Jumbo Patch 100377-15

IMPACT:

        Any user on the system can become root.  This cannot be exploited
        remotely.

REPEAT BY:

        Exploit details will be made available on the 8lgm fileserver
        at 00:00GMT on Friday 27th January 1995.  To retrieve these
        details, send a mail containing the line:

                send [8lgm]-Advisory-16.sendmail-6-Dec-1994-EXPLOIT

        to 8lgm-fileserver@bagpuss.demon.co.uk.  Requests for the script
        to be sent before this date will be directed to /dev/null.

FIX:

        We recommend that security conscious sites upgrade immediately
        to UCB Sendmail 8.6.9, as Suns sendmail is generally recognised
        as being broken.  Your options are:

        1. Obtain patch from your vendor.

        2. Build and install sendmail 8.6.9, available from:
           ftp.cs.berkeley.edu:/ucb/sendmail/sendmail.8.6.9.*
```

Full Disclosure Continues

- Issues with full disclosure
  - Creates a problem to force vendors to act
    - "If you don't react, I'm giving this to a bunch of 15 yr olds"
  - Lack of clarity around vuln research legal issues
    - Vendors first instinct is to get lawyers involved
  - Underground industry evolved around available info
    - Mass malware survives almost entirely on full disclosures
    - It's not 1995 anymore! Script kiddies grew up too!

- Full disclosure bottom line
  - "Researchers" keep at it b/c it makes them famous
  - Has FD resulted in a reduction of attacks? Hardly

Responsible Disclosure

- Worms in the early 2000s made some reconsider FD
  - ILOVEYOU, Code Red, Code Red II, Nimda, Sadmind, Slammer, Blaster, Sobig.F, Agobot, Bagle, Nachi…
  - Most worms reused code released by researchers

- "Responsible Vulnerability Disclosure Process"
  - Submitted to IETF by Christey and Wysopal in 2002*
  - Responsible – researcher withholds info until patch
  - Responsibilities targeted at researchers, not vendors

- Branded researchers as *irresponsible*, bred contempt

* http://tools.ietf.org/html/draft-christey-wysopal-vuln-disclosure-00

Current Status

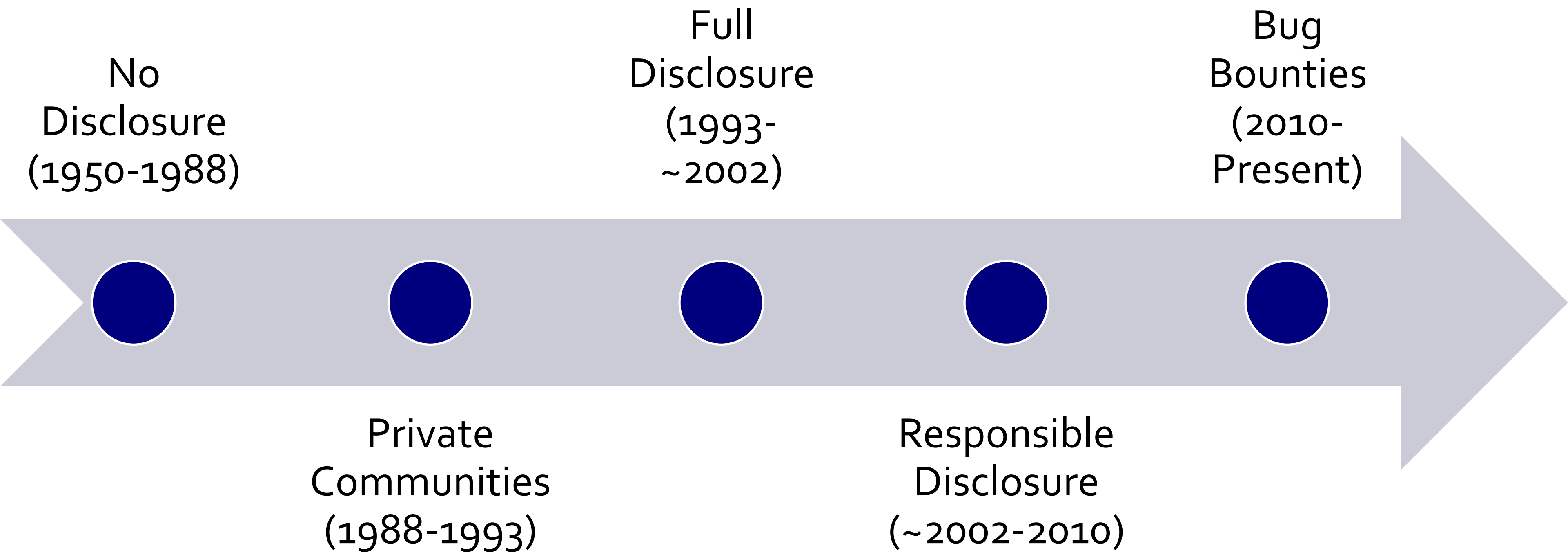
- Coordinated Vulnerability Disclosure
  - “We swear we won’t sue you”
  - Vendor acceptance of responsibility for security issues
- vendorsec Mailing List
  - Invite-only mailing list for sharing vulnerability details
  - Identified as compromised in March 2011
    - Remember kids, learning from your mistakes is evil
- Delayed Disclosure
  - Issue PR release and do newspaper interviews about vuln
    - Usually incites researchers to co-discover. Oops!
  - Disclose at an enormous conference 3 months later
    - Maximize marketing benefit, self-interested

The Rise of Bug Bounties

Company	Scope	Bounty	URL
Google	Web and Native	$500 - $3133.7	http://goo.gl/5LCJs
Facebook	Web	$500	http://goo.gl/w3Kuu
Mozilla	Web and Native	$500 - $3000	http://goo.gl/NRwpe
Barracuda	Appliances	$500 - $3133.7	http://goo.gl/1SKGU
ZDI	Popular Software	$500 - $5000	http://goo.gl/OEnc8

...plus a litany of smaller projects like:
tex, tarsnap, djbdns, qmail, hex rays, and ghostscript

Trends in Disclosure



No Disclosure (1950-1988)

Private Communities (1988-1993)

Full Disclosure (1993-~2002)

Responsible Disclosure (~2002-2010)

Bug Bounties (2010-Present)

My Thoughts

- FD was necessary due to lack of awareness of impact
  - Companies hacked in *August 2011* – United Nations, News Corp, RIM, HKEx, eBay, Nokia, DigiNotar…

- Focus on vulnerability mitigation assumes that attackers are constrained by access to them
  - Vulns abused by mass malware / year: *~15*
  - Vulns discovered in-the-wild by APT / year: *~15*

- “The Exploit Intelligence Project”
  - http://vimeo.com/24329182
  - http://goo.gl/o4XFp

Ethics

- The CS6573 Vulnerability Disclosure Policy
  - We follow Coordinated Vuln Disclosure (CVD)
    - Shared responsibility of researcher and vendor
  - Report through a 3rd party such as CERT or ZDI
    - Reduce exposure to legal issues
  - Make every effort to limit impact to users
    - No details until patches available, unless…
  - If the vendor isn't playing ball, disclose

- http://go.microsoft.com/?linkid=9770197

Resources

- Legal Issues
  - eff.org/issues/coders/grey--hat--guide
  - eff.org/issues/coders/vulnerability--reporting--faq

- Places that handle disclosure for you
  - CERT - https://forms.cert.org/VulReport/
  - oCERT - https://www.ocert.org/
  - ZDI - http://www.zerodayinitiative.com/

- History
  - http://securitydigest.org/
  - http://www.underground-book.net/