Responsible Programming in Cloud Platforms

Joel Nider

Cloud System Technologies

Cloud platforms are driven by business needs

Customers demand fast & cheap

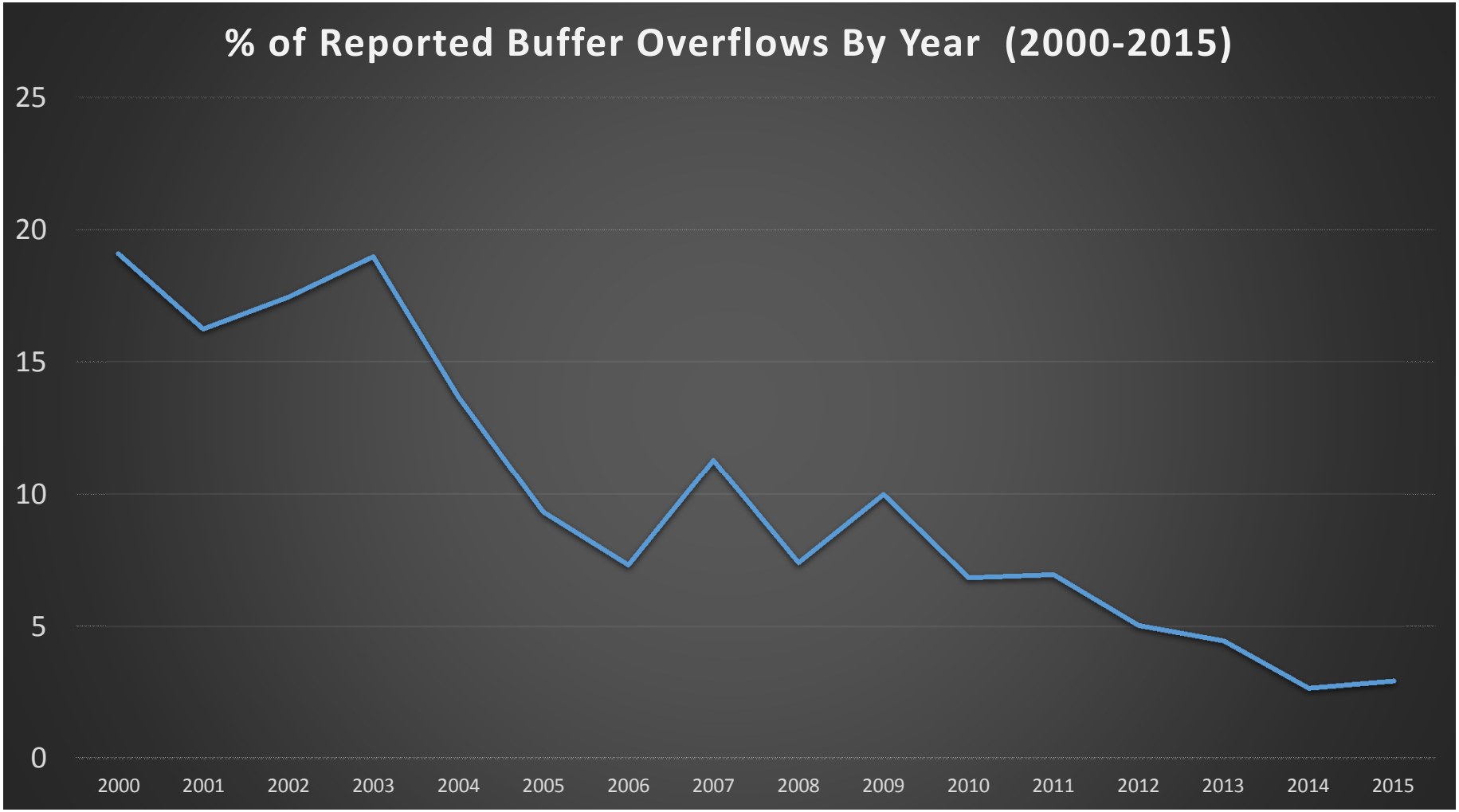
Security is a matter of effort

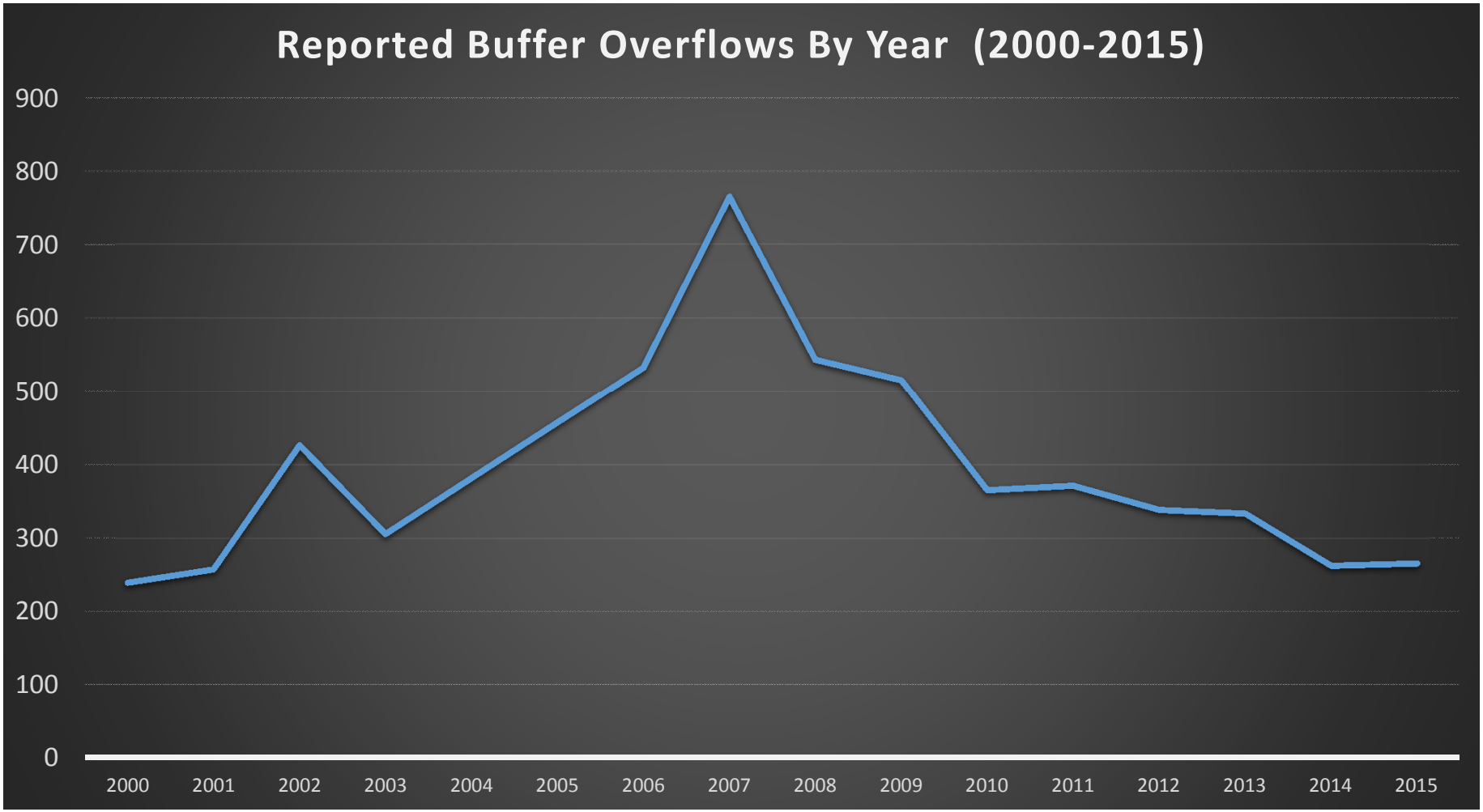
Serious Flaws Affect Everyone

- Heartbleed **(CVE-2014-0160)**
- Shellshock **(CVE-2014-6271)**

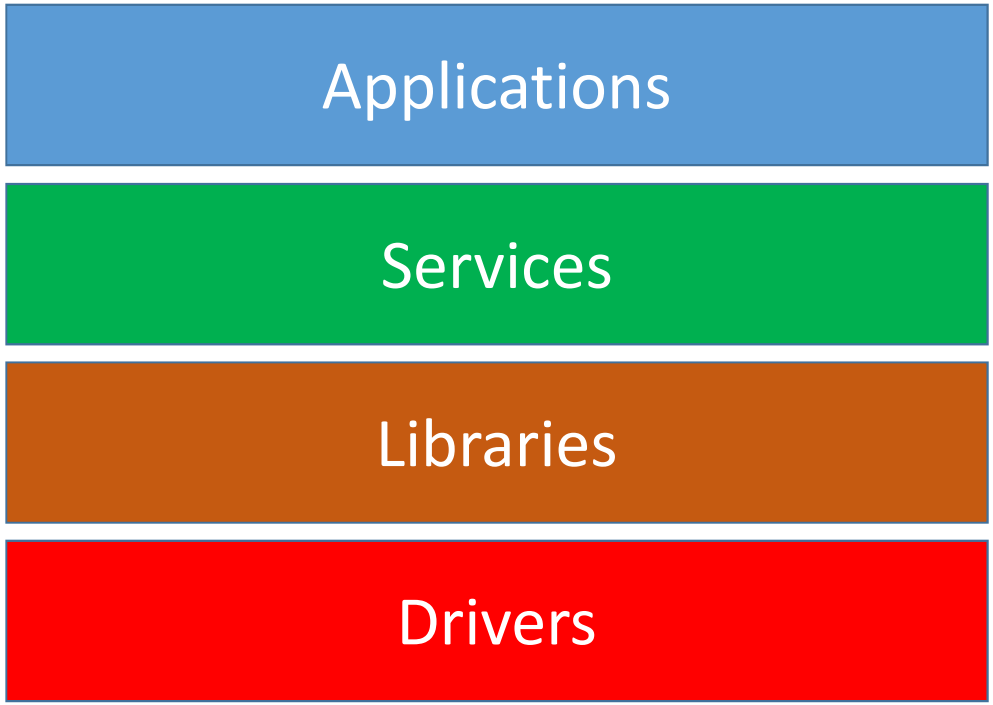
Vulnerabilities

- Approximately 9% of reported vulnerabilities are buffer overflows allowing arbitrary code execution


% of Reported Buffer Overflows By Year (2000-2015)
25
20
15
10
5
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015


Reported Buffer Overflows By Year (2000-2015)
900
800
700
600
500
400
300
200
100
0
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015

Buffer Overflows Affect Every Layer



Libraries: OpenJPEG (CVE-2016-8332)

- A buffer overflow in OpenJPEG 2.1.1 causes arbitrary code execution when parsing a crafted image

Drivers: Broadcom wifi (CVE-2016-8658)

- Discovered by Daxing Guo <freener> - Security Researcher from Tencent's Xuanwu Lab

```
--- a/drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c
+++ b/drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c
@@ -4527,7 +4527,7 @@ brcmf_cfg80211_start_ap(struct wiphy *wiphy, struct net_device *ndev,
                                                (u8 *)&settings->beacon.head[ie_offset],
                                                settings->beacon.head_len - ie_offset,
                                                WLAN_EID_SSID);
-       if (!ssid_ie)
+       if (!ssid_ie || ssid_ie->len > IEEE80211_MAX_SSID_LEN)
                return -EINVAL;

memcpy(ssid_le.SSID, ssid_ie->data, ssid_ie->len);
```

Services: Redis (CVE-2016-8339)

- Discovered by Cory Duplantis of Cisco Talos
- A buffer overflow in Redis 3.2.x causes arbitrary code execution when a crafted command is sent

```
#define CLIENT_TYPE_NORMAL 0 /* Normal req-reply clients + MONITORs */
#define CLIENT_TYPE_SLAVE 1  /* Slaves. */
#define CLIENT_TYPE_PUBSUB 2 /* Clients subscribed to PubSub channels. */
#define CLIENT_TYPE_MASTER 3 /* Master. */
#define CLIENT_TYPE_OBUF_COUNT 3 /* Number of clients to expose to output
                                    buffer configuration. Just the first
                                    three: normal, slave, pubsub. */
struct redisServer {
…
clientBufferLimitsConfig client_obuf_limits[CLIENT_TYPE_OBUF_COUNT];
…
}

server.client_obuf_limits[class].hard_limit_bytes = hard;
```

What happens when **`class = CLIENT_TYPE_MASTER`** ?

PHP Applications: Moodle (CVE-2016-9186)

- Online learning used by HUJI, Tel Aviv University, Technion, BGU, Bar Ilan, etc

Impact

- CSA (Cloud Security Alliance) **Treacherous 12**
- Stealing from end-users
  - Identity theft/fraud
- Loss of service to end-users
  - DoS attacks
  - Hijacked resources
- Loss of business
- Many effects we are unaware of!

Athem Medical Data

Lior Arbel, CTO at Performanta:

"Another day and another huge data breach hits the headlines. We have unmistakably now entered a phase in cyber-aggression where hackers have realised that information is power and have begun to up their attacks on corporate targets to steal vital intellectual property or consumer data."

What can we do?

- Alex Holden: “Eventually, almost everyone gets breached.”
- Don’t be the easiest target
- Train programmers to be “security aware”
- Don’t enable features unless you have to (TLS heartbeat)
- Perform code reviews – even if its not your code!

Conclusions

- Security threats are real
- Security issues affect everyone in the cloud
- Security issues have a large impact (cost)
- Security can be improved by more careful programming

- http://www.reuters.com/article/us-cyber-passwords-idUSKCN0XV1I6
- http://www.zdnet.com/article/health-insurer-anthem-hit-by-hackers-up-to-80-million-records-exposed/
- http://krebsonsecurity.com/2015/02/data-breach-at-health-insurer-anthem-could-impact-millions/
- https://en.wikipedia.org/wiki/Shellshock_(software_bug)
- http://www.openjpeg.org/
- http://www.datacenterknowledge.com/archives/2015/03/16/security-breaches-data-loss-outages-the-bad-side-of-cloud/
- http://www.talosintelligence.com/reports/TALOS-2016-0193/
- http://www.talosintelligence.com/reports/TALOS-2016-0190/
- http://heartbleed.com/