数据驱动安全

2015 中国互联网安全大会
China Internet Security Conference

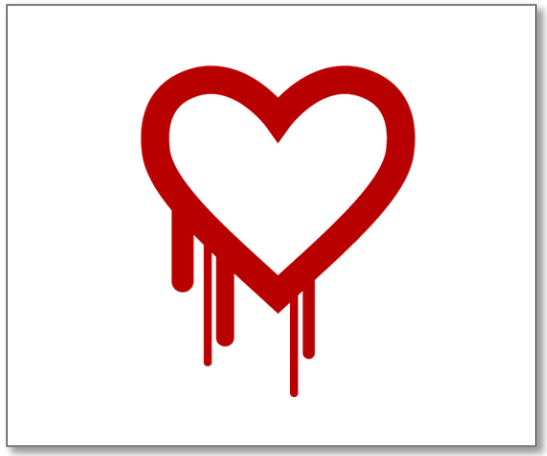
How to protect you and your company from the latest Internet security threats

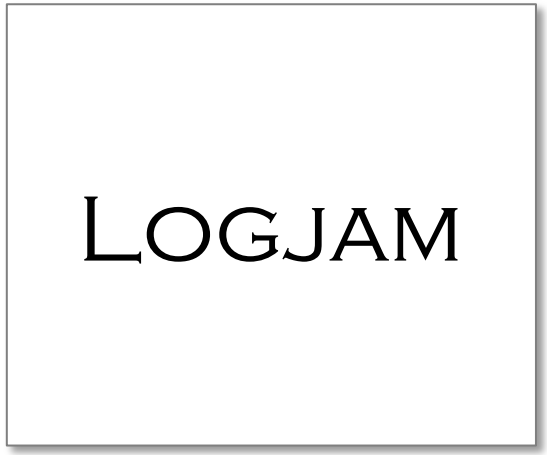
Hari Veladanda
Director, Engineer (Symantec Corporation)

Agenda

1	Major Internet security threats 主要网络安全威胁？
2	Why this many threats? 为什么有这么多威胁？
3	Is TLS Protocol safe? TLS Protocol安全吗？
4	Best Practices to protect you and your company 保护您和您公司的最佳措施
5	Future of Internet Web Security 互联网安全的未来展望

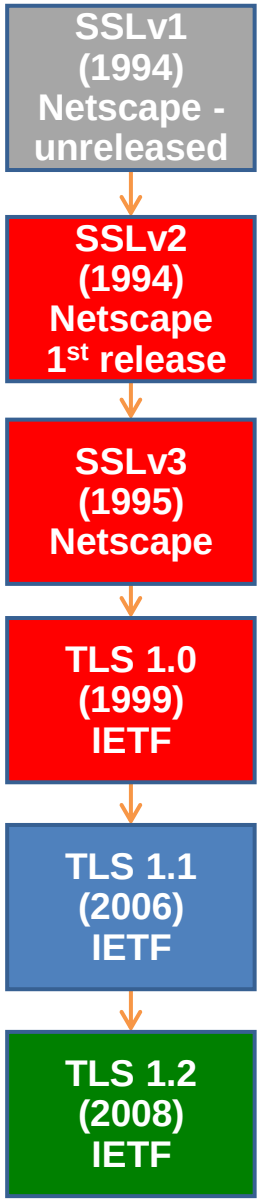
MAJOR INTERNET WEB SECURITY THREATS…





TLS HISTORY

- Multiple versions in use by both client and servers
  - Client start with strong and then fallback based on server support…
- Broad range of support



MAJOR INTERNET SECURITY THREATS - 2014

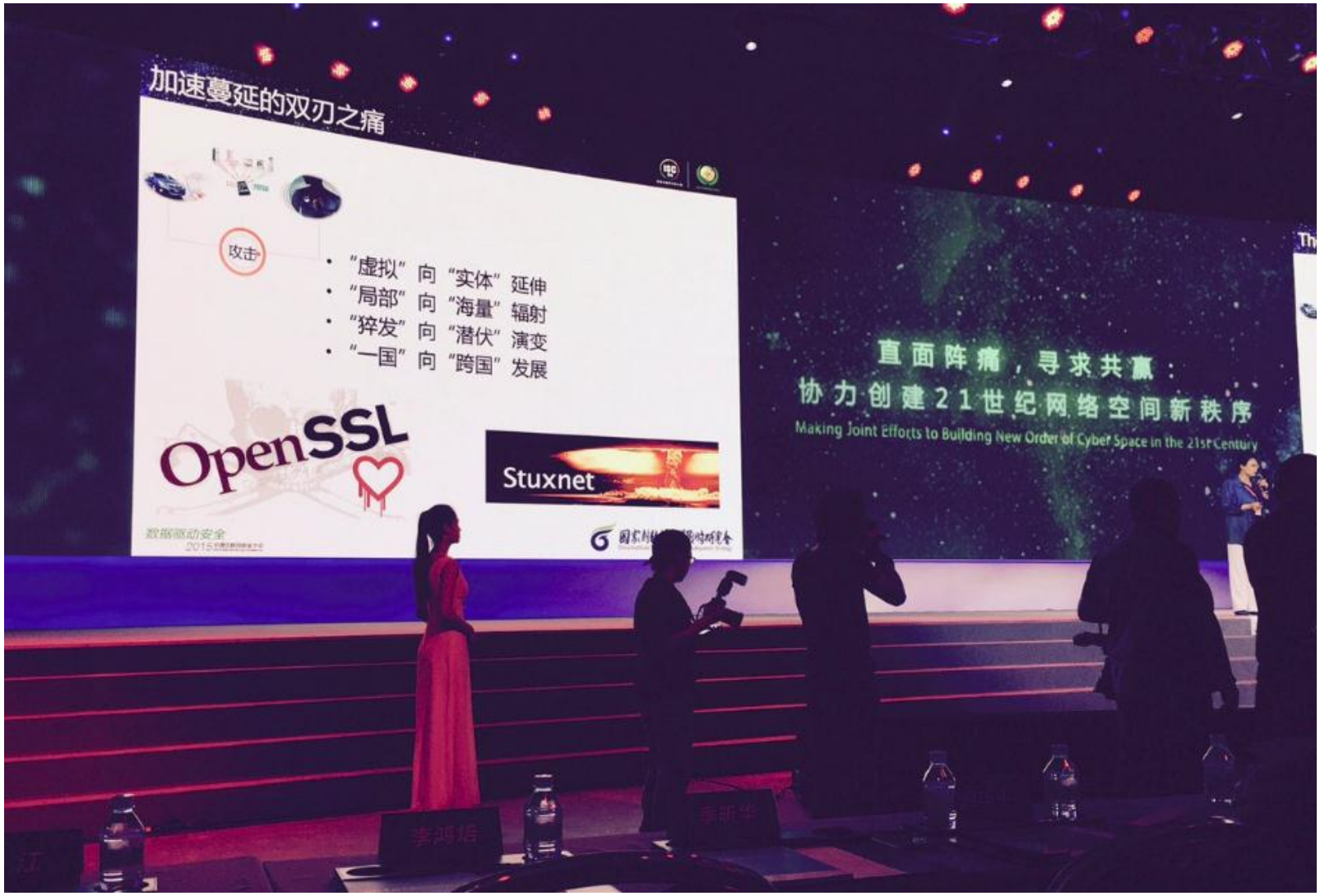
Heartbleed April 2014

- **Vulnerability description**: Allows attacker to retrieve private keys and decrypt encrypted traffic, steal user passwords, Personally identifiable information (PII) etc…
- **Impact**: Half a million widely trusted websites vulnerable**(as reported by Netcraft..)*
- **Root Cause**: Missing bounds check in the handling of the TLS heartbeat extension allowing attackers to read up to 64 kilobytes of the affected server's memory
- **Fix**: Upgrade OpenSSL library 1.0.1g

"Not a vulnerability with SSL/TLS Protocol but with implementation"

…programming mistake in popular OpenSSL library that provides cryptographic services such as SSL/TLS to the applications and services

Hao Yeli – Deputy Director Innovation



MAJOR INTERNET SECURITY THREATS - 2014

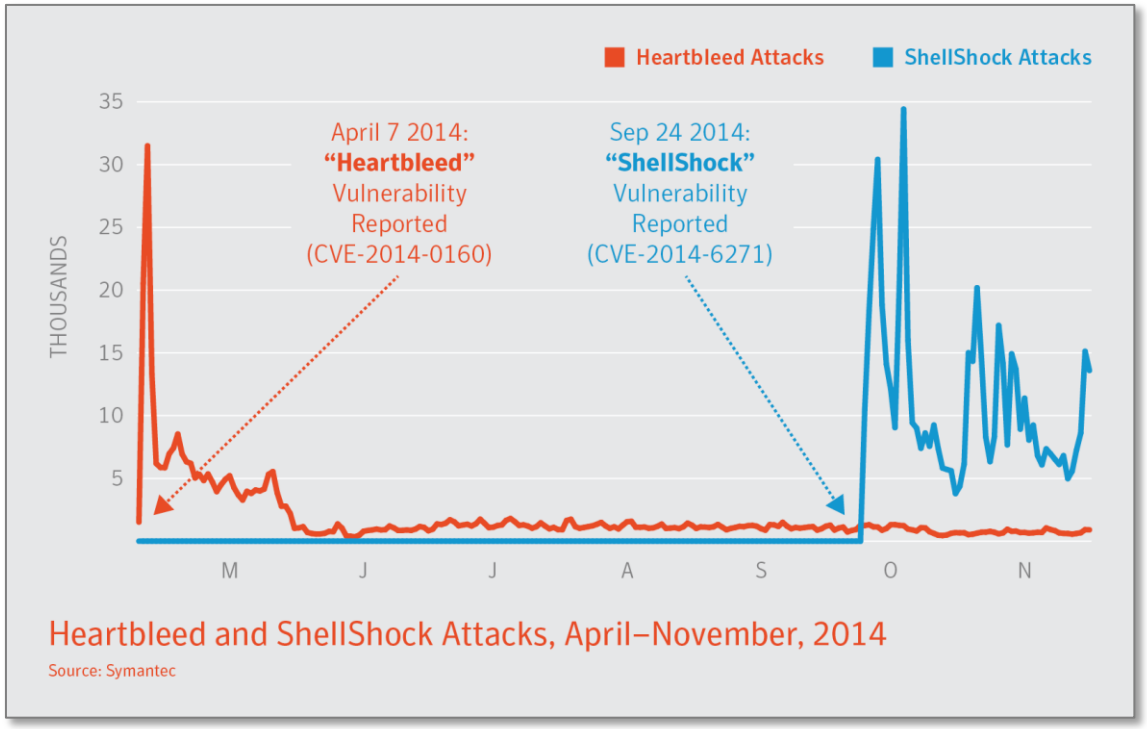
Shellshock September 2014

- **Vulnerability description**: An attacker can run critical shell commands…allowing the attacker to gain control over a targeted computer
- **Impact**: HIGH.. potentially affects most versions of the Linux and Unix operating systems. Has been in the wild for a long time. Allows control over the target machine and affects broader range of devices
- **Root Cause**: Shell was designed long before common use of internet…security was not the prime concern in its design
- **Fix**: Apply patch for specific distributions of Linux or Unix

"Unix Bash Shell vulnerability, Bug in the web server Operating System"

ShellShock
{bashbug}

HEARTBLEED AND SHELLSHOCK ATTACKS



Heartbleed and ShellShock Attacks, April–November, 2014

Source: Symantec

- Targeted attackers feast on zero days before they are discovered
- Heartbleed vulnerability exploited less than **4 hours** after becoming public
- Others jump in once they become public

MAJOR INTERNET SECURITY THREATS - 2014

POODLE October 2014

(Padding Oracle On Downgraded Legacy Encryption)

- **Vulnerability description**: an attacker can potentially interfere with the handshake process which verifies which protocol the server can use and force it to use SSL 3.0 even if a newer protocol version is supported
- **Impact**: Was supported by nearly every Web browser and a large number of Web servers. Because the attacker needs to have access to the network, this issue is not as severe as Heartbleed. Public Wi-Fi hotspots are potential avenues for this attack.
- **Root Cause**: faulty logic for negotiating SSL/TLS version
- **Fix**: Disable SSL 3.0 protocol in the client or in the server (or both)

"18 years old, insecure, obsolete protocol, still widely supported!"

MAJOR INTERNET SECURITY THREATS - 2014

FREAK March 2015

- **Vulnerability description**: Force clients and servers to use weak encryption
- **Impact**: 26% https servers, 9.6% Alexa Top 1 million web sites* *(as reported by freakattack.com..)*
- **Root Cause**: Implementation defect; clients and servers neglected to remove support for obsolete cipher suites
- **Fix**: web server: disable support for TLS export cipher suites, upgrade to latest versions for browsers

"Not a vulnerability with SSL/TLS Protocol but with implementation"

MAJOR INTERNET SECURITY THREATS - 2014

Logjam June 2015

- **Vulnerability description**: allows a man-in-the-middle attacker to downgrade vulnerable TLS connections to 512-bit export-grade cryptography
- **Impact**: 8.4% of the Top 1 Million domains were vulnerable* (as reported by https://weakdh.org)
- **Root Cause**: Implementation defect; clients and servers neglected to remove support for obsolete cipher suites
- **Fix**: disable support for the export-grade (DHE_EXPORT) cipher suites

"insecure, obsolete cipher suites, still widely supported!"

LOGJAM

MITM

What is MITM.. “attack vector involves the attacker placing himself–or his malicious tools–between the victim and a valuable resource, such as a banking Website or email account. These attacks can be highly effective and quite difficult to detect, especially for users who aren’t aware of the dangers the attacks present.”

SSL/TLS Protocol is strong and people are trying to get around it by trying to insert between client and server.

GoGo flight

- Trying to limit/block video streaming from certain sites ex:youtube.com
- Browsers provided a warning…but high click through rate

SuperFish

- Customize Advertisements
- No warning as the hardware vendor added his own Root certificate to the Trust Store

HACKINGTEAM

- Code signing certificates are digital certificates that help protect users from downloading compromised files or applications. When a file or application signed by a developer is modified or compromised after publication, a popup browser warning will appear to let users know that the origin of the file or application cannot be verified or has been tampered with.
- CA's verify that Code Signing certificates are issued to legitimate Organizations and Individuals.
- CA's Revoke if its deemed to be used to sign Malware.

WHY THIS MANY THREATS & VULNERABILITIES?

- Implementation bugs
- Open Source : Used by many but reviewed by very few!
- Outdated software versions continue to be used
- Backward compatibility leads to unacceptable security risks
- Vulnerability discoveries are ultimately a good thing for the security Industry…highly skilled professionals around the world are looking at what we rely on to secure our connections and fix its flaws!

IS TLS SAFE ?

- YES, YES & YES !!!
- No better alternative …TLS remains the best
- TLS is extendable
- Protocol provides the ability to deprecate older algorithms like MD2, MD5, RC4, SHA1…
- Not only continue to use it but need to expand to ALL internet communications (Always On SSL)
- TLS has no performance impacts on modern hardware
- Pay attention to certificate being used and web server configurations…
- IETF is continuing efforts on TLS 1.3 to make it even further secure...

BEST PRACTICES TO PROTECT YOU AND YOUR COMPANY

- Obtain certificates from a Reliable CA
  - Security posture, Substantial market share, Certificate lifecycle management, support
- Right certificate for the right job
  - DV, OV, EV
- Key size: RSA 2048, ECC P256 – protect keys!
- Digest Algorithm: SHA256
- TLS 1.2 or 1.1
  - Disable SSLv3, TLS 1.0
- Cipher Suite
  - Enable PFS, ECDHE
  - Disable RC4

BEST PRACTICES TO PROTECT YOU AND YOUR COMPANY

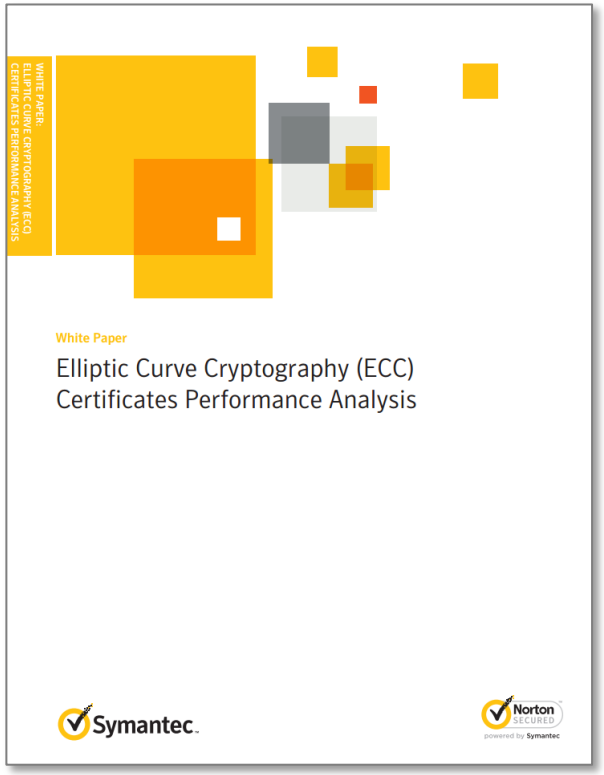
- Regular updates of Open Source and operating system software
- Always On SSL
- HTTP Strict Transport Security (HSTS)
  - Will not allow any insecure
- Encrypt your web site 100%
  - Encryption being optional is probably one of the biggest security problems today
- Complete Website Security Tools : you can check for the latest vulnerabilities…
  - https://cryptoreport.websecurity.symantec.com

Future of Internet Web Security (World of TLS is changing…)

- Mandate for https by end of 2016 for all US Government websites
- Apple: Mandatory https for mobile apps in IOS 9 & OS X 10.11
- Non https sites will be marked as “insecure” by certain browsers
- Chrome, Firefox – certain features only w/https (i.e. geolocation)
- http2 requires https (IE, Firefox, Chrome, Safari)
- Microsoft requirement to add OIDs for DV/OV/EV
- Microsoft proposed name constraints for Government owned CAs worldwide
- HSTS: IE11 on Win 8.1 and Win 7
- IPv6 support for certificate revocation (2016)
- Reddit: Default https July 2015
- All Wikimedia projects are now https only
- Certificate Transparency rollout

FUTURE OF INTERNET WEB SECURITY

- ECC certificates
  - Better Security
  - Better Scalability, Performance
- Quantum Resistant
  - RSA 3072
  - ECC P384
- Internet of Things (IoT)
  - While we look at IoT as being part of the future, attackers are there today
  - IoT devices like routers, baby monitors, security cameras and home automation systems under attack



FREE Download

HOW TO CONTACT SYMANTEC?

Symantec. | 企业

中国 简体中文 | 购物 | 搜索赛门铁克

产品与解决方案 | 支持与社区 | 安全响应中心 | 试用与购买

赛门铁克网站安全全球合作伙伴网络

赛门铁克网站安全全球合作伙伴网络

为客户提供极具吸引力的高增值服务和支持

赛门铁克网站安全解决方案 (WSS) 拥有强大的全球合作伙伴网络。赛门铁克 WSS 合作伙伴都拥有本地支持和销售团队，在您需要网络安全防护时，他们将为您提供可信赖的咨询服务。此外，这些授权合作伙伴将以本地货币结算的形式提供增值销售、服务和支持。立即联系赛门铁克下列任一WSS 合作伙伴，即可通过我们的合作伙伴网络进行购买：

iTrusChina Co., Ltd.
北京天威诚信电子商务服务有限公司
中国北京
北京市海淀区上地八街7号院4号楼401室（南门）
100085
+86 4006-365-010
SymantecSSL@itrus.com.cn
https://www.itrus.cn/

TrustAsia Technologies, Inc.
亚数信息科技（上海）有限公司
中国上海
上海市徐汇区桂平路 391 号新漕河泾国际商务中心A座22层 2201 室
200233
+86 400-880-8600
symantecssl@trustasia.com
https://www.trustasia.com

感谢您选择在线信任领域的领导者——赛门铁克。十分感谢您的惠顾！

与销售人员联系

+86 10 6195 0164 or
提交问题
Trust Center 登录

Thank you

Thank you

Thank you