The HeartBleed Bug: What's Significant?

ICTA SLTy Report #3 rev 1.0

This paper is written by staff of the International Christian Technologists' Association (ICTA). They draw on decades of high tech experience, a network of world-class experts, and an unusual Spirit-Led perspective on modern technology. The term "SLTy" refers to Spirit-Led Technology.[50]

NOTE: This paper contains both Footnotes (Starting with #1) and Endnotes (Starting with #50). Footnotes are for immediately desirable links, while Endnotes contain additional explanations and reference sources.

Table of Contents

Introduction

This paper is a fresh take on an issue that many people have misconceived as yesterday's news: something minor that's of little consequence either personally or corporately.

Were you under the impression that the HeartBleed Bug is basically about *Web servers and passwords* to be changed?

It is far more than that. Yes, almost every popular website was affected. But the list also includes email services, telephone connections, secure video conferencing, Wifi hubs, encrypted office (VPN) links, database software, Instant Messaging, and even personal computers and smart phones. ALL of these can be affected. We have a simple demo showing that one click on a spam email link can cause a phone to be compromised if it has vulnerable browser software.[1]

Do you use any device that has online access? If so, HeartBleed can potentially affect you.

Have you been assured that your phone or tablet (whether Android, Windows, or Apple is immune… or has your service provider or financial institution been silent so you assumed all is well?

You have been lulled into complacency. Various vulnerable apps make *any* of the above devices vulnerable. Several organizations who initially thought they were immune have now come out saying they may have been compromised, while others are saying nothing, even though their products have proven vulnerable.

Put simply: do you use *any* device or software/ system that has online access? *If so, it needs to be checked. (See the Evaluation section on how to do this.)* In each case, a decision must be made:

- If *previous* vulnerability was *fixed*, what will you do about possible leaks of confidential information?
- If *currently* vulnerable and *not yet fixed*, what's the risk to you or those you serve of getting it fixed?
- If vulnerability is *unknown,* there's danger. What's the risk of continued use? (Sadly, many popular services, phones, tablets, etc are in this category.)
- If you use *web browsers*, does it matter if you are scammed by an identity thief?
- If you use a *single password* for many services, does it matter that an attack against any one service makes it that much easier to access your other accounts?

Again, for anyone responsible for protecting private or secure information, **the HeartBleed bug is so serious that the only safe assumption in the absence of clarity… is to assume the worst.** Even if your vendor/supplier/experts have made basic assurances that the problem was adequately investigated and

[1] This video shows how clicking a spam link in a phone results in the the user's phone being attacked. This same method can work in any vulnerable app, in any phone that's able to connect online. https://www.youtube.com/watch?v=bzKrtm7rFlc

resolved, it's likely that there are further issues, particularly if they did not provide detailed information[51]. Without good data, it's best to assume your provider is still vulnerable. In such a situation, **Ignorance is Dangerous.**

Our prayer is that this paper will help you learn enough to carry an important message to those around you:

- HeartBleed is a vital, risky issue;
- We all need to deal with it at the right time and right way;
- If we are vigilant and act with prudence and wisdom, we need not worry about the devastating consequences of complacency.

Following you will find answers, based on extensive verified sources in the end notes, to key HeartBleed Bug questions:

- **How serious** is the HeartBleed bug?
- **How do we fix** (remediate) HeartBleed?
- **What if we *can't* fix it?**

Throughout this report, we've tried to supply you with verifiable facts. Our HeartBleed message:

Humility **Yes**, Hysteria **No**

Only systems purchased and/or updated since January 2012 bear any direct risk, yet the risk extends indirectly to anything connected to vulnerable systems.
This last part makes the problem huge.

I. How Serious Is HeartBleed?

Most important, **HeartBleed is already here**; there's no time to prepare like there was for Y2k. That's why we're providing this quick-look report *before* all the facts are known.

Second, HeartBleed is huge yet limited. While only systems purchased and/or updated since January 2012 bear any *direct* risk, the risk extends *indirectly* to people and systems that connect to the vulnerable systems. **This last part makes the problem huge.**

As hinted above:

- Do *you use devices that have **online access?***
- *Do you **login online with id's or passwords?***
- *Do you use **money*** other than paper and coins?

Yes?

Then the HeartBleed bug can potentially affect you.

It *is* that serious.

*What about organizations you are a part of? Is your **business or ministry appropriately secure*** in this era of online financial, identity and privacy attacks?

- This report shows that *many initial HeartBleed reports were inaccurate. Plus, some product and service vendors large and small are not helping their customers discover* which of their products and systems are affected by HeartBleed.[52]
- *HeartBleed is a solvable challenge.* Individuals and organizations that ignore it could bear great loss, particularly now that the problem is widely known. It's possible your officers and directors could be held personally liable in a lawsuit.
- *HeartBleed is a business challenge*. Business decisions are required to allocate appropriate money, time, and human resources for mitigation. Decisions about legal and operational risks to your organization need to be made at the highest executive levels.
- *HeartBleed is a spiritual challenge*. Perhaps obvious for many who read this: those who follow Christ place trust in Him, not in technology. Today's events provide an opportunity to put that commitment to the test.

What Is HeartBleed?

In early 2012, an (accidental[53]) computer software bug was released in one of the core Internet security protocol libraries.

Imagine your office building…you have installed the best available security doors for the outside entrance. Inside, you also have all your internal office doors protected with locks. **But now because of this bug, it's as if all of the locks silently broke.**

Computer systems, products and equipment silently lost their "front door locks," and enabled attackers to randomly record many secrets that had been protected. Worse, it's often not possible to know if criminals peeked past the open doors.

If the problem is not solved ("locks" repaired) and secret keys[54] and ID's updated, confidential information will be compromised. For example, *login id's and passwords* become known, *identity theft and impersonation* becomes easy, and perhaps most important – data flowing across *normally-secure online networks can be transparently read or even transformed* by an attacker. Even past data can be easily decrypted in many cases. This exposure could include anything from email or social media messages to financial transactions.

Vulnerable: installed apps on smart phones & computers from every major vendor… telephone systems… video conferencing… home security…wifi hubs… backup systems…

What is Affected (and Not?)

First, here are some examples of devices and systems that *are* affected. Be prepared for surprises, given the lack of publicity for this issue. This is not at all a comprehensive list:

- A wide variety of installable **Smart Phone and computer apps, *including those from Apple (iPhone, iPad/iPod), Google and Microsoft***, have been found vulnerable[55]. One major example of corporate complacency (and certainly not unique): *Apple App stores contain vulnerable apps.* Unfortunately, there is not yet a significant public list of Apps and their HeartBleed status.
- Installed apps on smart phones and computers from every major vendor, from **databases** (FileMaker Pro) to **Office** software (Libre Office) to **computer games, instant messaging, video conferencing** and more have been found potentially or provably vulnerable. [56]
- Not only computers but also **devices are vulnerable,** including dozens of major products from vendors like Cisco (**IP phone** systems, video **conferencing**/ telepresence systems, and the popular **WebEx** "Web Cast" service.[57]), Apple (*AirPort Extreme* WiFi hub, *TimeCapsule* backup[58]), and many more.
- A number of **Smart Home security** services are vulnerable.[59]
- **Many online services were vulnerable, possibly including your bank.** Unfortunately the providers typically don't say much either from fear or ignorance.

Now, some examples of devices and systems that are *not* affected (again, this is not a comprehensive list):

- Any computer or service or device that was purchased and **last updated before 2012 is not directly vulnerable.** (However it may use logins, passwords or identity certificates that need changing due to exposure elsewhere.)
- **PayPal** is an example of a popular online financial service that was *not* affected. PayPal passwords do not need to be changed.[60] (If you've used the same password at other vulnerable sites, best to change it to reduce risk.)
- **No version of Microsoft Windows[61], Apple OSx or iOS operating systems, and only one version of Android** (Jelly Bean 4.1.* mostly found in Germany[62]) are vulnerable. However, **remember that software** available on every one of these platforms **is vulnerable.**

Why is this not in the news more?

Sadly, **too many are ignoring or minimizing the issue**, even though we know that the bug is more widespread than the popular media is communicating.

Due to blandly reassuring statements by some vendors, many organizations and individuals are assuming they are immune and are not even investigating. For example, here are reassuring *but incorrect* headlines from a popular daily Apple Mac media outlet:

Because of false headlines like these, too many are not even aware there's an issue….

> "Apple on 'Heartbleed' bug: *iPhone, iPad, Mac and iCloud unaffected*[63]"

> "*Apple's iOS, OS X don't have Heartbleed bug* but Android and BlackBerry's BBM do" … "*users can breathe a sigh of relief with the knowledge that their devices are not affected* by the catastrophic OpenSSL Heartbleed security flaw…*Apple products don't suffer from the bug*[64]"

Because of false headlines like these, too many are not even aware there's an issue.

Also, as of today there is very little geographic-based data available to indicate either the propagation of the HeartBleed bug, or its fixes, around the world. Users in the developing world are less-likely to have heard about HeartBleed. Fortunately, they also may be less-likely to be at risk because they often use older equipment. But even that assumption should be tested.

Real-World Risks

The honest answer today for this quick-look report: *nobody* fully knows how serious this bug is in practical terms. In fact, we may *never* know because of the nature of the bug. We've already discussed some of the actions already being taken to address HeartBleed. Now we'll look a bit deeper at what is at *risk*, and progress toward being able to *identify* products and services that are vulnerable.

What is at risk…

Can anyone accurately assess the risks due to the HeartBleed bug? We believe investigating the facts and applying some wisdom allows us to develop a reasonable understanding of the situation, even without comprehensive understanding.

First, here are some of the real-world risks due to this bug. Some of them are far more difficult to exploit than others. However, many of them are *proven* issues, not just theoretical problems:[65]

- Almost everyone eventually needs to change their passwords, just about everywhere, due to the risk of **login/password exposure**. The HeartBleed bug can directly expose login id's and passwords. It can also *indirectly* produce the same result, as it makes it much easier for an attacker to infiltrate a given computer system or network, and/or to decode messages traveling through an encrypted link. If you use the same password in multiple places, once it becomes known, criminals or opponents can easily attempt its use everywhere you have accounts. The result of such exposure can be anything from identity theft to impersonation to financial theft and more. Since **many people use the same password in multiple places**, an exposed password in one place can place other information and relationships at risk. (There's a section below on fixing passwords.)
- Attackers can more easily **impersonate online banking, email and other communication services or devices** if identity certificates are not replaced. A vulnerable service provider's identity certificates can be stolen (a bit like a driver's license – the certificate provides proof until expiration that the bank or service you're connecting to is actually who they say they are.) The result of such theft is that an attacker can get in the middle of your link[66] to that service, and perfectly emulate the service so that you are fooled thinking you are connected directly to your

intended institution—thus unintentionally sharing your private data.

When it comes to devices, consider an IP Phone system: an attacker can impersonate a phone, thus allowing them to send or receive calls "on behalf of" anyone in your organization. Unfortunately, even if the compromised certificate is replaced with a new one, *the now-invalid old certificate usually still appears valid* because very few systems check the global lists of revoked certificates[67].

- Attackers can **decode encrypted data transfers**, including (in many cases) previously-recorded transfers. This includes everything from financial transactions to email, phone and other private communications. Without getting into the details, exposed identity certificates enable such decoding. In most cases it remains difficult for an attacker to gain *access* to the data stream. Anyone with physical access to either the equipment in your office, or with access to your online connections (eg local or national service provider) could accomplish this attack. This risk is probably of more serious concern to those working in limited-access nations, or who are responsible for protection of high-value data.
- Attackers can **modify financial transactions o**r other private data in the pipe. For example, it has been demonstrated how a "Man in the middle" attacker can modify the account and/or amount of a financial transaction.

Frustration When We Can't Fix It

We want to explicitly warn the reader: the HeartBleed Bug is unusual (but not unique) in the fact that *many v*endors and service providers are not paying attention, so even **a diligent person may not be able** to obtain the information needed to properly evaluate and fix the problem at this date[68].

That's quite frustrating, particularly for the experienced executive. When faced with a challenge, we prefer to identify the challenge, solve it, and move on. That's considere**d good management.**

The implication of this is manifold:

- From a management perspective, organizations (or individuals) budget for additional evaluation effort, ongoing monitoring of the situation, and sometimes costly temporary workarounds.
- From a spiritual perspective, we can learn to appreciate this as an opportunity to let go of our dependence on human control and focus more on our actual total dependence on the Lord.

II. Remediation Perspectives

Before we jump into the details of a remediation strategy, let's review some important elements of *perspective.*

First, please understand a few important details left out by almost everyone who talks about HeartBleed. Attention to these details will help gain a balanced view of the situation:

Fear of Lawsuits

We live in a selfish, greedy, lawsuit-happy society. As a result, many corporations are reluctant to say clearly what is or is not affected by HeartBleed—not because they don't know, but because their lawyers warn them to be careful. Thus, when asking your business partners about HeartBleed, use a *friendly, practical* approach that asks whether they have discovered any *past or present* HeartBleed vulnerabilities**,** and when they expect to have all of the critical issues resolved.

Once they speak out, learn how to interpret corporate statements:

- A company that produces a wide variety of online products and services will ideally provide a detailed list of which items were tested, which items were vulnerable. If they can't do that, it's safest to assume they have not done a sufficient job of evaluation.
- If they say everything is fine now, but suggest that passwords ought to be changed, it's best to view that as admission that there was a real vulnerability at some time.

Who is Affected vs. Response Needed

Many people focus on the fact that the HeartBleed bug itself may only need to be repaired in a relatively small number of devices and/or applications.

This ignores the connectedness of our world: keys, logins, and passwords used by every computer that *connected* to the vulnerable system may be compromised. (Consider a thief gaining access to a master key that works not only for your office but for many company buildings across the city.)

And now that we know just about all "client" devices (ie your phone) need to be checked**, it's not particularly helpful to ask "does this affect me?" Yes it does, if you have an online device or service.**

A more helpful question is this: **"If my device/system is vulnerable, do I actually care? Do I need to do anything about it?"**

At ICTA, we always try to keep in mind that we live by faith, not by computer password. Even if our data is vulnerable, the risk involved may be so small that it does not matter to us.

The reality, *only risks we are unwilling to bear need to be addressed.* (Of course, remembering to take into consideration others we are responsible for when evaluating risk.) For example, if I use a secure video link to protect identity of collaborators whose lives are at risk, or I securely share account numbers protecting large sums of money – I probably consider those to be well worth taking time to carefully protect against risk. On the other hand, I may not consider it high risk that HeartBleed has compromised the same link if it is only used for a weekly conversation with my children in the next town. Again, these are questions between you and the Lord… and your human stakeholders.

Front Doors, Back Doors

Almost all publicity to date about HeartBleed has focused on websites. We might **think of a website (server) as a "front door"** into a computer system or network. However, that's just the beginning of the challenge for most organizations. What other doors are there? **Most of us have no idea how many secure online "doors"** or gateways our phones, computers and organizations maintain. As hinted above, they include: email, Video and IP phone services[69], file sharing apps and services, VPN[70] links (to remote offices, home users,

executives with tablets/laptops/smart phones) and much more. In today's world, even a computer game can be a pathway for an attack on your network. (Did you know the famous "Target" credit card attack was initiated via their *Heating and Air Conditioning* supplier? Clearly, in the age of the Internet we need to be even *more* careful about "back doors.")

Why is this important? *Every broken security "lock" on a device must be fixed before that device is safe.* Fixing the website "front door" doesn't solve a thing if the email "back door" is still wide open. The same goes for your phone: if your news App is repaired but a database app is still broken, an attacker still has the potential to access secure info in memory, via the vulnerable database .

Because of the multitude of "doors", **multi-purpose devices such as phones and personal computers generally have more "doors" to be repaired.**

When it comes to computer servers, this principle generally impacts organizations differently depending on size. *Smaller organizations often use the same server* for multiple functions (e.g. websites, databases, email), which means there could be multiple "doors" that became vulnerable. *Larger enterprises generally have separate servers* for different enterprise functions, so a given HeartBleed vulnerability may have a smaller impact.

Executives, please note: unfortunately**, the media and our tech teams are often unaware that multiple vulnerabilities can exist,** and they convey a false sense of security after fixing the broken front door "lock." It will likely be some time before this reality is well understood and well communicated to the public.

As of this writing, we have not found *any* list that covers the multitude of potential vulnerabilities for any given product or service. Thus, caution is in order.

Contingency vs. Real-World planning

When faced with a difficult, complicated situation, many people panic about the complexity itself, believing Murphy's law: "If anything can go wrong, it will go wrong." Fortunately, Murphy's law is only valid as a *design* idea, not as something to apply in day to day living—especially if we have put our trust in the Lord! He does direct us and gives us strategy and plans we are to take.

- **Contingency planning** applies when *designing* systems. When designing a safe airplane, it is best to assume almost *any* part can fail. We then build the plane so it will continue to operate even if *many* parts are broken!
- **Real world planning** applies when preparing to actually *use* a product. When we prepare for our next trip, it would be foolish to assume every element of the airplane will fail.

So, it's important to remember that in the real world, complex systems, whether aircraft or security protocols, usually function correctly even when several of their parts are broken. That's how they are designed, and that's how they operate!

At the same time, remember that certain key elements of a system truly are crucial. Obviously, an airplane can't fly without wings. More subtly: is an open window an issue? It depends… An open window on the fifth floor of a building probably represents a much smaller security risk than if the open window is on an armored car with no one in sight.

III. Remediation Strategy

Whether you are a concerned individual or represent an organization, the primary steps in responsibly dealing with the HeartBleed problem are:

- **AWARENESS:** Acknowledge there's a problem.
- **SURVEY**: Check your organization *and outside connections* to identify critical systems, services, accounts and software. Strongly encourage your ministry partners to do the same.
- **EVALUATE:** Create and implement a plan to evaluate which systems, devices and connections *actually* have a problem (or had a problem in the past, potentially exposing your secrets.) While you're doing so, consider evaluating for other critical computer security problems. Other very critical issues are being found in more than ten percent of connected devices.[71]
- **FIX:** Develop and implement a plan to resolve critical issues (if you have responsibility), ensure outside responsible parties are addressing their issues, and that all appropriate secure certificates, keys and passwords have been changed.
- **TEST**: the results, to the extent possible, before assuming your confidential data and passwords are secure. This is important not only for your own confidence in moving forward, but also for ensuring that your workers and constituents can have confidence that your organization has addressed this important issue.
- **PLAN FOR CONTINGENCIES:** If you have budget responsibility for your organization, plan for unanticipated time and financial expenses over the next three to six months to address new surprises.

IV. Remediation Details

Awareness

You should now be aware and are interested in staying updated.

Survey

We recommend beginning your survey at a very high level. The survey's focus is on *online access* –the systems, devices, people, etc who connect online. In particular, our interest is *secure* online access, but it's often hard for non-tech people to know when secure protocols are used.

For an individual, the survey could be as simple as a brief mental list. For a large enterprise, the survey could become a significant spreadsheet or database requiring ongoing attention from full time staff.

Depending on the size of your organization (or personal family), you may want to begin by cataloging:

- Locations (offices, mobile users or teams)
- Networks and Systems (local and VPN networks, phone systems, collaborative teams)

- Device Types (phones, network cameras, backup boxes, and much more)
- Users (Individuals, corporate partners, etc)

(Large Enterprises must plan to survey a number of additional technology layers. See Appendix 3 for a brief overview.)

From that high level, you can then identify:

- Outside Services and Providers (websites, online shopping, banks, social media, file sharing, and so much more)
- Specific equipment (devices/products) with online access
- Major software packages with online access (browsers, databases, commerce servers, accounting, etc)
- App collections (do you or your team use apps from the Apple App store, Google Play, etc?)

At first the list will grow until it seems overwhelming. That big list may ultimately be important in two ways:

- Sorted and summarized in various ways to help understand *level of risk*, and *remediation effort*;
- As a detailed checklist for tracking *remediation progress*.

Network Survey Note:

A good high level strategy for prioritizing equipment and services in your organization (or home!) during the survey is to ask two key questions (if possible):

- Is it *visible* to the Internet? (If not, the only risk would be from anyone who has access to your internal network)
- Has it had any *traffic*? (You may not be able to answer this question. But if you can, and you know there has been little if any use of the device, then you may want to repair/update it but probably are not concerned about loss of secure information.)

Evaluation

Your survey results directly feed into the evaluation process. (Many people will do the Evaluation at the same time as the Survey. However, because so little is known right now, the evaluation may have to be repeated so we list it separately.)

It's easiest to group the Survey results into three sets of lists:

- Services/Providers (fixed by the Provider)
- Products/Vendors (you'll likely install Vendor fixes)
- Devices using multiple Apps (these need to be scanned for vulnerability and individual Apps addressed)

NOTE: If your organization is itself a product vendor or service provider, of course you should evaluate your own products and services as described below, and respond accordingly.

Overall Evaluation Notes:

Some aspects of HeartBleed are relatively easy to evaluate:

- It's quite **easy to check whether a website is vulnerable** to HeartBleed. In the end notes, we've listed several online resources that provide this service and/or keep reasonably current lists of still-vulnerable websites.
- There are good Scanner apps available for certain smart phones, such as Android.

That's the end of the "easy" list as of this writing. Current challenges include:

- **No scanner** is available for Windows or Apple phones.
- **Only very technical/custom scanners** are available for non-web services (such as email and VPN.)
- F**ew** companies keep track and/or admit **their own *past* vulnerability**. Remember, any online service (or device) that *was* vulnerable could have had its security compromised in an undetectable way. **If a company is vague about past vulnerability, it's best to assume they were vulnerable at some time.**

> *Any online service or device that was vulnerable could have had its security compromised in an undetectable way… given no response or a vague response, it's best to assume they were vulnerable at some time.*

- **Some companies are not (yet) saying anything, or are allowing the public to believe their products are immune**, without providing any evidence. This is especially troublesome when we can prove that there are real issues. As of this writing, the most significant vendor in this category is Apple computer.
- *Every* online device and/or service that uses secure data needs to be checked for vulnerability… As of today, **we've yet to see a multi-company "vulnerability list" that covers more than web vulnerabilities.**

Services/Providers

Services include everything from websites to banks to doctors offices – anything outside of your own environment that you connect to online..At this time, it is often difficult to get knowledgeable responses from banks and other service providers. It will be that much more difficult if you work in a developing nation. You may have to arrange for your own testing.

- **Website scanning:** SSL Labs has a free web-site scanner.[2] We recommend using this; it tests for many widespread vulnerabilities. (Unfortunately it does *not* test all HeartBleed issues, such as vulnerable email and other protocols.)
- **Banks: While many banks maynot have said anything at all, many other financial institutions are taking HeartBleed seriously,** at least to the extent of asking their tech teams and consultants to delve into the issue. Unfortunately, even the *best* public response we've seen[72] recommends users change their passwords, without explaining why. Remember that the nature of HeartBleed is that nobody can tell if secret data is compromised, so don't be reassured by statements that a provider has "no evidence" about compromised accounts..

[2] SSL Labs web (HTTP, HTTPS) scanner: https://www.ssllabs.com/ssltest/index.html

- **Online Shopping: Many online shopping systems, particularly the ones run by small to mid-size ministries and businesses,** have been found to be vulnerable. Some examples include *Magento* and *ZenCart.*[73] Providers of the software, and hosting providers as well, are actively patching their systems. (If you host such a system, you need to have it tested, and fixed if needed.)
- **Health Care and Government:** A variety of online healthcare and government websites and services, including HealthCare.gov, were vulnerable and are being fixed.[74]

Products/Vendors

Some detail hints for evaluating the equipment you use (*note that personal computers and phones are separately addressed below*):

- **Network scanning:** Tripwire offers a free comprehensive scan of up to 100 devices attached to your local network.[3] We highly recommend this; it found a number of other vulnerabilities on our own network.
- **Telecommunications**: Traditional phone systems and networks are not vulnerable. However, some of the new "IP Phone" systems *are* vulnerable (an attacker could listen in on calls and/or impersonate your phones.) Cisco is one example of a responsible vendor that is analyzing all of their products and providing patches.[75]
- **Corporate Data Links:** HeartBleed can affect secure connections between company offices, and between home/roving users and their corporate networks. In fact, one hacker has already been caught taking advantage of HeartBleed to completely bypass VPN "multi factor" security to gain employee-level access to a corporate network.[76] VPN products are being tested and fixes made available.[77]

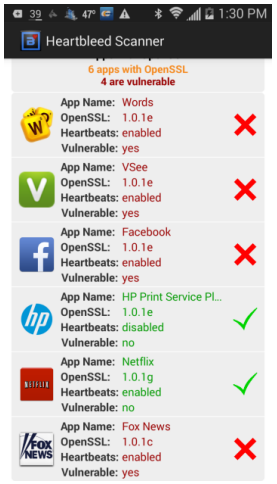
There's a *lot* of other online-connected equipment in our lives… and very little public awareness that HeartBleed affects more than just websites and passwords.

Even though this is true, it is possible that you don't need to be concerned about other devices. If you have no data or passwords that need to be kept confidential, then perhaps HeartBleed doesn't impact you as much as others.

If you do have such equipment--perhaps a WiFi router or backup system? A security system with web cams? A family photo sharing app on your smart phone (such as Facebook or Pinterest), where you also have a password-security app?, you need to test those devices and/or apps and decide what to do if they are not HeartBleed compliant.

(Example: All of the equipment on ICTA's network happened to be far behind on updates and was not vulnerable to HeartBleed. However, while surveying we discovered other serious security issues that are being addressed.)

Multi-App Devices



- **Android Phones:** we recommend using "HeartBleed Scanner" from Bluebox, in the Google Play store (free)[4].
- **Apple devices (iPhone, iPad, Mac, etc) and Windows phones:** as of this writing there are unfortunately no scanners available. This is a serious matter: we know some apps are vulnerable, yet there's no way for users to check their apps. ICTA is working to remedy this.[78]

(Example: we had a vulnerable news app on one smart phone and deleted it. We discovered through deep technical analysis that a video conferencing app was theoretically vulnerable on all devices. We've contacted the vendor, who is updating the app. Other apps in the screen grab on the right are still vulnerable.)

PC/Mac Hardware & Software Survey

If you need to deal with HeartBleed on one or more personal computers, see Appendix 1 below for help on the basic technical issues. If you need to deal with large computers or software systems, or if you run a large organization, *you need to get some technical help!*[79]

What If There's No Answer?

As of this writing, *it is very difficult or impossible to evaluate all systems and devices.* Most commonly this will be because you can't get a sufficient answer—or any response at all—from a service provider or vendor. In rarer situations, they can't create a fix (at least in a reasonable amount of time.) What then? Here are some suggestions:

- **Finish your survey** to at least recognize which devices and systems likely are *important* from a security perspective, the current *status* of understanding, and (for the important items) who is most likely to eventually provide useful information.

> *If there's no answer available, consider a more cautious approach. Ignorance is Danger.*

- Rapidly **consider a more cautious approach** for anything that's both important and has unknown status. Remember, ignorance is dangerous in such a case.
- If it is an important phone/tablet device, consider disabling as much software as possible (to minimize the risk of having one of the vulnerable apps active.)

[3] Tripwire's free network scan: http://www.tripwire.com/state-of-security/vulnerability-management/how-to-detect-the-heartbleed-openssl-vulnerability-in-your-environment-2/

[4] *Bluebox HeartBleed Scanner* is a new product. We are not yet certain it checks all possibilities, but it is the best we have seen so far. https://bluebox.com/technical/heartbleed-bug-impacts-mobile-devices/

- Stay in touch with your list of sources so you will be aware when more information is made available. (ICTA is also planning ways to publish occasional updates of general interest on this topic. Please contact us if you would like to be on the list.)

Fix It

Browsers

Most people will want to make a change in their web browser settings. HeartBleed is forcing millions of secure identity certificates to be replaced; browser settings need updating to ensure you won't be scammed by an attacker using one of the now-invalid certificates.

However, we caution that these settings, while taking care of a real (yet hopefully low-probability) security risk, will most assuredly cause frustration for many users. This is because there are situations (such as using airport/hotel/medical wifi that force you to log in but use an invalid identity certificate) where these new and "better" settings produce a warning or block of an invalid certificate.[80]

To obtain the desired security improvement, follow the instructions below, and be prepared for occasional warnings under non-attack "reasonable" circumstances:

- In Google *Chrome*, click on *Settings > Advanced Settings* and scroll down to the HTTPS/SSL header. Tick the box next to *Check for server certificate revocation*.
- In Windows PC's, ensure Internet Options are correctly set (this affects *Internet Explorer, Safari for Windows* and other software that uses IE in the background.) Go to Internet Options, the Advanced tab, then scroll to the Security section and verify that *Check for server certificate revocation* is checked. It should be by default. If it's not, check it and restart the computer. (Instructions may be slightly different for different Windows versions.)
- In (Mac) OSx (affects Safari browser), go to *Keychain Access->Preferences->Certificates*. Hold down the Option key and change *OCSP* and *CRL* to "*require for all certificates"* and Priority to *"require both*."
- In FireFox, go to *Options -> Advanced -> Certificates-> Validation*. Check the box for *"When an OCSP server connection fails, treat the certificate as invalid"*

What to expect now that you've fixed the browser's settings?

- As before, most of the time you will notice no difference.
- **Better Detection:** If a web link (URL) takes you to an invalid/scam site, you will be warned, instead of being given no notice that this site is actually a fake.
- **False Positives:** As noted above, unfortunately there may be situations (e.g free wifi "host" at a local retailer) where you will see a popup warning about an invalid website, even when nothing is wrong. In the worst case you may have to turn off your browser's protection if it is crucial that you use the resource that produces the warning.

Passwords

Changing passwords… what a thankless job and yet crucial when security breaches take place. Here's ICTA's best advice for this important task:

Good passwords are:

- Hard to guess but easy to remember;
- Reasonably long (eight or more characters if possible);
- Different for every service that's important to you;
- Changed infrequently, except when necessary;
- *Not* written down.

How to accomplish all of that? Here's our strategy:

- Choose one good "baseline" or "core" password every year or two (see below)
- Append a variation that depends on the resource being accessed. ("bk" for bank, "cc" for credit card, "e" for email, etc)
- If someone requires frequent changes, add one or two digits (e.g. XYZZYcc15 for the March variation at the credit card site, using month +12)
- When you discover an old password still in use, update it to the current one.
- Never ever *ever* use a good password on a website until you are confident they have good security. (See below)
- If security warrants, create one Super Secret password that's only used to protect your most confidential information. *Very* few people should know this password. It should never be used online.
- If you must write something down, it's better to record hints about password content than the actual password. It's also better to record such information in a secure way, such as a "password database." We plan to evaluate these products soon.

One strategy for choosing a good core password:

- Pick a phrase you want to memorize (perhaps from scripture… we'll use John 3:16 for our example, but note, we do not recommend this very common quote.)
- Take the first letters from each word; use Upper case at least once, use at least one punctuation and at least one digit to result in 7-12 characters. (4Gsltw3.16)
- That's not easy for others to guess; it is quite simple for you to remember (do NOT use our example!!)
- Sometimes you will find services that can't handle punctuation, initial digits or upper case. Just change your core password to fit (fgsltw316)

How to know that a service protects password privacy:

- As soon as you've set up an account, try the "forgot password" system and/or use customer service to recover your password. Also examine any "new account" email or paper mail sent to you.
- What you should see: a method to reset your password and generate a new one. That's fine.
- What you should *not see:* If *any* communication from the provider is able to print, tell, show or otherwise communicate your password, then you know this provider is not using the best security practices. *Never trust them with a good password.*

VI. Conclusion

HeartBleed is a serious problem.

- Both computer software and devices can be affected. *Usually, software is the bigger issue.*
- *You need to seriously deal with it* both personally and in your organization.
- *However, there's no reason to panic*.
- Older non-online computer systems and devices are not affected.
- Yes, almost everyone will have to *change their passwords.* Many newer devices, phone apps and servers *need upgrades.*

The most serious HeartBleed risk is not technical, but spiritual and societal. If we cannot recognize the need to lean on God rather than on technology, the doomsayers will have won. And just as with fears of a run on the banks, if society panics about HeartBleed, it really *could* become a disaster.

As Christians we are called to be prepared in season and out of season. HeartBleed *is* having an effect on people around the world. More and more breakdowns and high tech thievery are being blamed on HeartBleed and other publicized security threats, right or wrong. As Christians, we are called to be a light to the world. Are you prepared, spiritually, emotionally, and physically, to help others who may be among those who are harmed by HeartBleed?

Sir, my concern is not whether God is on our side;
my greatest concern is to be on God's side,
for God is always right.

—Abraham Lincoln

"For God has not given us a spirit of fear, but of power and of love and of a sound mind.."

—II Tim. 1:7

Do not let your hearts be troubled.
Believe in God, believe and trust also in Me.

—John 14:1

Appendix 1: Technical Notes

Hardware/Device Issues

Although testing is still underway by many vendors, preliminary results show that few of the most popular *hardware* products are vulnerable to HeartBleed.

- Windows computers (workstations, laptops, servers, etc) are not vulnerable at the hardware level.
- The same is true for Apple computers, although as noted above, an Apple Wifi device and backup system are *vulnerable*.[81]
- Smart Phone hardware is resistant to HeartBleed.
- Many IP Phone systems are *vulnerable.*[82]

That said, for other devices it is important to check with your vendors to learn if you have any risks. We urge you to check with the vendor of any device that connects to the online world in some way. If they can't answer the question, the safest assumption is that the device might be vulnerable.

Software Issues

Software is generally a bigger issue than hardware when it comes to HeartBleed. Why? Because most software today is regularly updated online… so if there was ever a possibility your software was vulnerable… then most likely it actually did expose confidential data at least for a while.

Software is generally a bigger issue than hardware when it comes to HeartBleed

In addition, unlike bugs found in common operating systems such as Windows or Apple iOS/OS X… the core software library that contains the HeartBleed bug is often embedded separately into individual software packages. This means that **each and every software package must be checked.**

You'll need to verify whether there is or was a vulnerability, and then decide what to do about it.

Unfortunately, while there are many lists of safe/vulnerable websites, we've yet to find any similar lists of software. We'll add more to this section as more information becomes available.

Appendix 2: HeartBleed Websites

We find very little published information that is factual and transparent (i.e. most avoid admitting the truth, in order to protect the "brand.") ICTA is collecting a list of sites that we will eventually be able to recommend. For now, we can only recommend certain kinds of sites that list HeartBleed vulnerabilities.

We recommend evaluating a "list" site based on several factors:

- If a particular vendor's site, are they transparent about the existence of the bug in their own products and services?
- If appropriate, does the list cover more than just web services? (I.e. email, VPN's and more)
- Is there evidence from other sources that the list may be less than forthcoming about the reality of the issue in the products listed?
- Does the list reveal not only the current status, but also whether there ever was a problem?

As an example, we take note of weaknesses in some of the most popular online lists:

- The Mashable List: says Microsoft and Apple have no problem. This ignores that software running on those platforms (including phones etc) *is* vulnerable.
- The "Alexa One Million" list: only shows websites, and only shows current issues, not whether a website had a problem in the past.

Appendix 3: Enterprise Big Picture

Below is a list of typical three-tier enterprise data center/web infrastructure elements, showing some of the possible devices where OpenSSL could be in place.

1. Edge routers
2. DMZ firewall
3. Load balancer
4. Web servers (Apache, IIS)
5. Tier 2 firewall
6. Application servers (WebSphere, JBoss, Weblogic, IIS,etc)
7. Database servers
8. Other backend systems - Mainframe, MQ, Authentication devices (HSM, etc), LDAP servers

In addition, many enterprises also implement a variety of other significant appliances or applications, such as intrusion detection systems, network sniffers (span ports, etc), monitoring systems (HP Openview, Nagios, etc.) Larger environments will also incorporate a variety of Application Performance Management (APM) tools.

Normally, much of this infrastructure is only accessed by System Administrators over secure in-house connections. But because those inside connections are typically assumed to be secure, the enterprise infrastructure is far more vulnerable to an attacker who can impersonate an insider.[83]

End Notes

[50] Complex technology insight requires an understanding of the areas being examined. Pete Holzmann and Cecilia Mikolajczak combine many decades of computer system and network design and development experience, ranging from mainframes to "embedded systems" inside consumer electronics, from desktops to mobile systems, from Silicon Valley to remote parts of the developing world. In 1993, Pete (and his wife Leslie and children) moved to Colorado Springs after many years as a technical and management consultant in Silicon Valley contributing to a wide variety of groundbreaking products. Cecilia joined them in 2000 following her own journey as a high tech professional.
We are grateful to ICTA's community of technology professionals who contributed to this research paper in so many ways.

[51] What information is important? First, have they checked and fixed *all* potentially vulnerable ports/protocols/software (Web – HTTP, Email – SMTP/POP3/IMAP, VPN and possibly others)? Next, once they've fixed the software, have they replaced *all* potentially compromised security certificates? Many protocols use a "self signed" certificate that requires extra effort to update.

[52] In some ways, HeartBleed is worse than having non-encrypted systems, because it silently reveals confidential data that normally would never be exposed.
Two examples of vendor response for now: Cisco provides much of the infrastructure of the Internet. As of 5/5/2014 they have evaluated all but a dozen products; 270 are ok while 72 are vulnerable.
http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed Meanwhile, Apple has not yet made any official statement; of particular concern: users do not know that a number of downloadable products on the Apple Stores are vulnerable. (Our own research plus see here: https://discussions.apple.com/message/25441381

[53] How did this happen? All computer programs of any significant size contain mistakes simply because of the complexity involved. An experienced programmer made the mistake; his work was reviewed and approved by an even more experienced person.
http://www.dailynewsen.com/breaking/page/technology/german-engineer-who-created-heartbleed-bug-says-it-was-an-accident-h2470359.html

[54] A complete explanation of the terminology and multiple levels of security is more than a little complicated. Here's a brief summary:

- Computer and device identities are often protected by secret keys, called Certificates (or "certs"). These form proof of identity in various protocols, such as the HTTPS "lock" that shows up in web browsers. They also function as the secret key that locks most encrypted communications.
- Certs can be externally purchased along with some level of background checking and authentication that you (the owner of the Cert) really are who you claim. Often, less-visible encryption certs are "self-signed." Self-signed certs don't prove identity but unless compromised they are a valuable encryption lock.
- Encrypted links between devices are protected by the above "certs" and also by per-session keys.
- Finally, specific users can authenticate themselves via a standard login id and password.

[55] One good list that covers some of the most popular apps on all platforms is at: http://www.digitaltrends.com/mobile/heartbleed-bug-apps-affected-list/

(We're still looking for a vendor-specific list covering apps for Apple, Google/Android, and Microsoft)

[56] Some vulnerable Mac apps:
FileMaker Pro:
http://help.filemaker.com/app/answers/detail/a_id/13384/~/filemaker-products-and-the-heartbleed-bug
Libre Office:
http://www.libreoffice.org/about-us/security/advisories/cve-2014-0160/
Call Of Duty:
http://www.theregister.co.uk/2014/04/10/call_of_duty_heartbleed_fragging/

[57] A report on Apple devices is here:
http://recode.net/2014/04/22/apple-issues-security-fixes-for-ios-mac-and-airport-extreme/

Cisco's list is in the link provided above in Endnote #51.

[58] Airport Extreme and Time Capsule vulnerability and fixes are discussed here: http://recode.net/2014/04/22/apple-issues-security-fixes-for-ios-mac-and-airport-extreme/

[59] Several services were found vulnerable, so far including SmartThings, Revolv, and Zonoff (Staples Connect)
http://readwrite.com/2014/04/14/heartbleed-myths-debunked-fact-fiction

[60] https://www.paypal-community.com/t5/PayPal-Forward/OpenSSL-Heartbleed-Bug-PayPal-Account-Holders-are-Secure/ba-p/797568

[61] Microsoft's statement is found here:
http://blogs.technet.com/b/erezs_iis_blog/archive/2014/04/09/information-about-heartbleed-and-iis.aspx

[62] A free app in the Google Play store scans both the Android OS and all installed apps for HeartBleed vulnerability.
https://bluebox.com/technical/heartbleed-bug-impacts-mobile-devices/

[63]Denial headline #1 http://macdailynews.com/2014/04/10/apple-on-heartbleed-bug-iphone-ipad-mac-and-icloud-unaffected

[64]Denial headline #2 http://macdailynews.com/2014/04/11/apples-ios-os-x-dont-have-heartbleed-bug-but-android-and-blackberrys-bbm-do

[65] Most of these examples have been personally tested or verified by the authors. Additional references are provided in certain cases.

[66] This is known as a *Man In The Middle* attack, for obvious reasons. Governments have long been suspected of having the ability to successfully monitor encrypted communications in this way. The HeartBleed bug is certainly one way this could be accomplished.

[67] Just considering web browsers, by default *none* of the mainstream browsers check the revocation lists (Internet Explorer, Safari, Chrome, Firefox.) A newer standard called

OCSP can be easily bypassed. And in a coincidence of bad timing, the version of Firefox released in January 2014 removes the ability to enable such checking. One of the better technical discussions can be found at http://news.netcraft.com/archives/2014/04/24/certificate-revocation-why-browsers-remain-affected-by-heartbleed.html

[68] Yes, a technical expert can invest a lot of effort in evaluating any given product or service with no help from the vendor, but this is a costly, resource-intensive process.

[69] As an example, Cisco is one of the world's premier providers of networking equipment and services. Several dozen of their major products, including some versions of well-known services such as WebEx meetings, IP phones and cameras, have proven vulnerable. Cisco does not yet know the answer for dozens of products. http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed

[70] VPN or *Virtual Private Network* links are commonly used to connect multiple sites of an organization, or offsite users at home or on tablet/laptop, or to connect an organization with a major service provider. One of the most popular VPN tools is OpenVPN, which comes in both software form and embedded into various networking equipment (routers, modems, etc.)

[71] SSL2 has serious issues and has been deprecated for more than half a decade. Yet it still is accepted by many servers. http://contextis.com/research/blog/server-technologies-ssl2-should-it-keep-you-awake-/

[72] Bank public statement: http://www.aafcu.com/heartbleed_bug_information.html

[73] Online shopping carts vulnerable: http://www.ecommercebytes.com/cab/abn/y14/m04/i10/s01

[74] http://www.foxbusiness.com/personal-finance/2014/04/22/why-heartbleed-may-be-more-troubling-for-healthcaregov-in-long-run/

[75]Some IP Phone systems from Cisco are vulnerable: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140409-heartbleed#@ID

[76]Hacker breaches VPN multi-factor authentication: http://www.databreachtoday.com/mandiant-heartbleed-leads-to-attack-a-6766

[77] OpenVPN vulnerable, and fixed: http://www.reddit.com/r/VPN/comments/22jzse/openvpn_has_been_updated_to_close_the_heartbleed/

[78] ICTA is encouraging others (including contacts at Apple) to remedy the situation. In the meantime, we are experimenting with a phone app test method that requires significant technical expertise. We're glad to share it with readers who have interest.

[79] Many commercial providers provide HeartBleed technical help. We encourage asking how they test for email and VPN vulnerability (some don't even know that's a problem.) Ask if they test Apple equipment if you have Apple devices. ICTA would be pleased to hear from any organizations specializing in providing help to Christian ministries.

[80] A technical discussion of certificate revocation trouble can be found here: https://www.imperialviolet.org/2014/04/19/revchecking.html

[81] See endnote #58.

[82] See endnote #52.

[83] We are grateful to our friend who works as a Fortune 50 corporate System Administrator, who supplied this concise "Large Enterprise" overview.