Cybersecurity in Boise

Dr. Brent Kirkpatrick[*]

September 9, 2016

Intrepid Net Computing

www.intrepidnetcomputing.com

[*] bbkirk@intrepidnetcomputing.com

Abstract

Using the buttressIT$^{\mathrm{TM}}$ audit methodology, Intrepid Net Computing has evaluated the cybersecurity of Internet Service Providers in the city of Boise, Idaho. Our audit methodology is a statistical and experimental science method that allows examination of broad indicators of the health of computer networks.

This report outlines the cyberinfrastructure currently in use. We assess the cybersecurity vulnerabilities of the services offered by a number of Internet Service Providers. We reveal some activities of the most prominent hackers and give IP addresses for their rogue servers. We give a roadmap to improving cybersecurity in and around the city.

1 Introduction

Hacking harms our whole economy, from small business to big business and from the technology industry to the health care industry. On average, businesses loose millions of dollars in each cyberattack. The cost to our economy as a whole is on the order of billions of dollars.

The average cost of a single data breach is now \$4 million [1]. The average cost per stolen record is \$158. Compared with information from 2013, this is a 29% increase in the cost of data breaches. The cost of recovering from hacking is soaring.

Preventative computer security is the best way to reduce the soaring costs of recovering from hacking. Since the cost of recovering from data theft is outrageous, it is more affordable to prevent theft by constant innovation in security measures. The cost of innovating and implementing these security measures is minuscule when compared with the economic cost of recovering from theft. Preventative measures include: audits, upgrades, and proper network design.

Intrepid Net Computing addresses today's cybersecurity challenges with data science and artificial intelligence. In our world of ubiquitous computing, the number of computers in the average workplace out-numbers the number of people. Computers are everywhere: in cars, in cell phones, in watches, in toys, in calculators, as well as in the more traditional devices: laptops, tablets, and desktops. In this world, cybersecurity has become commensurately difficult. To address these challenges, Intrepid takes a system-level view to collect and analyze data that reveals the cybersecurity of a group of networked computers.

The remainder of this report will discuss several key components of the Internet infrastructure and its security. Each component will be graded on the subjective scale used by Intrepid Net Computing to compare the security of various locations. This is a shield rating where the number of shields awarded each section indicates preparedness to face computer security challenges. Five shields indicates optimal preparedness and zero shields indicates critical problems.

2 Physical Infrastructure

The physical infrastructure of the Internet is unknown. Dozens of organizations contribute to creating and maintaining the existing infrastructure which consists of fiber-optic cables, telephone cables, coax cables, dedicated high-speed cables, underwater cables, satellite connections, and cell towers. Since no single entity is responsible for the entire infrastructure, no single entity knows the network map. Since the Internet grows organically in a distributed fashion, entities trust each other to maintain their portions of the infrastructure and to communicate regionally about infrastructure planning.

Discovering the layout of the physical infrastructure in a city is a scientific problem. This problem is similar to the geographic information system problem of discovering and updating a good atlas of roadmaps. In data science, when we wish to discover the structure of an unknown network, we turn to statistical methods that infer the network from data. In computational biology, network discovery methods are used to study the network of life [2] and chemical interaction networks [3]. Similar methods can be used to discover the layout of the Internet.

Intrepid Net Computing has collected data and used a network-discovery method to estimate the layout of the Internet. Figure 1 shows our rudimentary estimate of the layout of the Internet infrastructure. With more care, a much more detailed network diagram could be inferred using our audit method. The accuracy of this estimation can be assessed by comparing this estimate to the knowledge resources that city-planners access when planning Internet infrastructure upgrades.

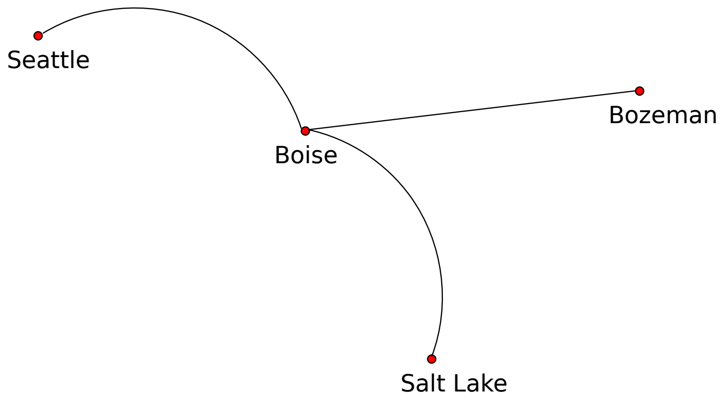

Figure 1: **Layout of the Internet.** This is an estimate of the layout of the Internet infrastructure in and near Boise. This map is not to scale and near is referring to cyber-distance, not physical distance. A more detailed network diagram could be inferred.

`buttressIT`™ Rating

🛡🛡🛡🛡🛡

Boise has a thriving tech industry and robust network infrastructure. The speed of Internet service is not part of our rating.

In terms of reliability, the physical infrastructure in Boise is very reliable. There are occasional outages with the primary threats being due to weather.

In terms of security, the physical infrastructure is fairly secure from physical hacking. Only physical hacking is included in the rating for this section. Relative to other parts of the country, there is very little software hacking in the city, which we discuss next.

3 Software Infrastructure

Crucial elements of the Internet infrastructure involve software that routes data through the physical network. Similar to freeway interchanges and cars, there are computers on the Internet, called routers, that help data choose the proper path through the Internet network. The data packets are like cars on the freeway, each with its own destination. The routers are interchanges, and the domain name service (DNS) acts like highway signs.

If the software infrastructure functions properly, then traffic on the Internet is reliable. This means that when you, as a user, connect to the Internet, your traffic will reach the destination that you intend. In other words, when you communicate with a server, it will be the server that you think it is.

If the software infrastructure is unreliable, then traffic on the Internet may not reach its destination; it may get routed to a different destination than the user had in mind, or it may not be authentic. For example, suppose that you want to visit your bank's web-site to do a financial transaction. The first step of the process is for your web-browser to use the DNS system to look up the IP address of your bank's web server. After that, your web browser creates a connection with the bank's server and an exchange of information occurs. If the DNS system gives a fraudulent response, then you might actually connect with a hacker's server that is masquerading as your bank. If the traffic is fraudulent, a hacker might be able to inject incorrect information into the transaction. Any of these possibilities can result in data and identity theft.

Intrepid Net Computing uses `buttressIT`$^{\text{TM}}$ a proprietary audit technology to asses the quality of the software infrastructure. Our approach examines the routers and DNS servers to determine whether they are hacked. We also look at the generation of DNS technology that is installed a local network.

`buttressIT`$^{\text{TM}}$ Rating

🟨□□□□

There is good security in the software infrastructure in Boise, likely due to the efforts of the thriving tech industry. The city appears to prevent hacking at a social level, though the good-will of a community with technology expertise. This strategy works well locally. However, there appear to be sophisticated hackers targeting the city from afar.

The good news is that since most of the hacking is remote, the city of Boise can easily clean-up existing computer security issues with concerted local upgrades to the DNS infrastructure.

More recently installed or configured Internet service tends to have better software security. Some businesses, such as Starbucks, rely on successful software companies to provide their Internet, and this service can come with better-than-average security.

Organizations that have their own IT departments have the opportunity to set their own security standards. These include universities, hospitals, and banks. However, many of these organizations are having difficulties prioritizing upgrades and consequently are falling behind on the most crucial upgrades.

Secure Public WiFi Hotspots

Intrepid Net Computing was unable to find progressive security. We looked for proper implementation of DNSSEC in public WiFi sub-networks, and were unable to find such a hotspot. We did not do a full survey of hotspot options, and we remark that Starbucks locations often have DNSSEC.

4 Internet Service Providers

The two largest providers of business and residential Internet are CenturyLink and Integra. Additionally, there are a number of other companies and providers that own infrastructure or buy bandwidth from the infrastructure owners.

`buttressIT`$^{\text{TM}}$ Ratings

Following the `buttressIT`$^{\text{TM}}$ audit method, we rate each of the major service providers for security. We rate based on physical and software infrastructure security. The speed of the connection does not factor into this score.

Provider	**Product**	**Rating**
T Mobile	Business	🟨□□□□
CenturyLink	Business	🟨□□□□
Integra	Business	□□□□□
Qwest	Business	□□□□□

Generally, business service that has been installed and configured recently tends to be more secure than older business service that has not been maintained. Residential service tends to have worse security than business service. Generally, the ISPs are not keeping pace with security upgrades.

Some organizations run their own sub-network infrastructure and manage their own security. These organizations can guarantee that upgrades happen and that state-of-the-art security is installed. This has a higher up-front installation cost, but can yield the best results for security.

5 Hackers

There appears to be relatively little hacking in the Boise metro area. A thriving tech industry seems to keep technology experts happily and productively employed.

The `buttressIT`$^{\text{TM}}$ evidence suggests that computers in Boise have been exposed to tainted updates for Windows, Adobe, Red Hat, CentOS software. During our audit, all of the suspicious IP addresses of possibly rogue update servers appear to be located outside of the state. This suggests that upgrades to the DNS infrastructure in Boise will cost-effectively improve computer security, preventing data theft and fraud.

`buttressIT`$^{\text{TM}}$ Rating

■□□□□

Intrepid Net Computing uses the `buttressIT`$^{\text{TM}}$ audit method to detect DNS poisoning and identify servers that are either administrated by hackers or are zombie servers (legitimate servers that have been taken over by hackers). There seem to be a number of these rogue servers targeting computers in the Boise area through poisoning to the local DNS infrastructure. However, since the poisoned IP entries appear to refer to zombie servers located at some distance, the damage to the city's computer security seems largely limited to the DNS infrastructure.

The evidence collected during our `buttressIT`$^{\text{TM}}$ audit is highly suggestive that the following IP addresses belong to rogue update servers.

IP Address	ISP of Server	Server Location	Updates	Affected ISP DNS
216.176.179.218	Wowrack.com	Seattle Area	CentOS	CenturyLink, Integra, Qwest
23.7.52.243	Akamai	?	Adobe	T Mobile, Integra, Qwest
23.15.20.176	Akamai	?	Windows	T Mobile, Integra, Qwest
173.222.212.251	Akamai	?	Red Hat	T Mobile, Integra, Qwest
104.126.133.158	Akamai	?	Red Hat	Integra, Qwest
66.109.26.212	Galaxyvisions	Atlanta Area	CentOS	CenturyLink, T Mobile, Integra, Qwest
23.208.218.146	Akamai	?	Adobe	CenturyLink, Integra, Qwest
104.103.72.35	Akamai	?	Adobe	Integra, Qwest
104.103.72.19	Akamai	?	Adobe	Integra, Qwest

6 Solutions

The principle goal of cybersecurity is prevention. In this case, the city of Boise would benefit from a concerted push to upgrade DNS servers to DNSSEC technologies. Prior to DNSSEC upgrades, the existing DNS servers need to have their caches regularly cleaned-out to remove poisoned entries that are probably being entered by some automated hacking methods. Improvements to DNS server firewall technologies might also address these DNS poisoning attacks, however these improvements are not yet implemented. Additionally, firewalls can be used to block the suspicious IP addresses released in this report.

Intrepid Net Computing strongly recommends that the city of Boise immediately roll-out DNSSEC upgrades. DNSSEC technologies are already implemented, tested, and debugged. DNSSEC is very easy to roll-out for caching DNS servers. DNSSEC upgrades to authoritative servers are absolutely crucial, even though such upgrades may disrupt some IT content-delivery network services.

Organizations that are responsible for Internet infrastructure need to be especially vigilant of risks and upgrades. Every ISP and web-hosting service needs to introduce DNSSEC as soon as possible. Using old versions of DNS remains one of the most significant security risks for the entire Internet.

Cooperation between multiple organizations is increasingly necessary to catch hackers and stop their activities. A single hacker might serve fraudulent updates for several software vendors by using one ISP to deliver traffic to their fraudulent server while attacking the DNS system of multiple ISPs. Since hackers use multiple technologies and attack multiple infrastructures to spoof many users, we must cooperate to stop their hacking.

Government aid is increasingly available from the FBI and the DHS. The FBI investigates cybercrime and the DHS works to prevent and track cybercrime. The DHS provides audit teams through the NCCIC's NCATS teams (`ncats_info@hq.dhs.gov`). The DHS also provides incident response capabilities through the CyberSecurity Advisors (`cyberadvisor@hq.dhs.gov`). Both services are free of charge and offered on a first-come-first-serve basis. The DHS also tracks cyberincidents through its information sharing programs: IT-ISAC, US-CERT, and AIS. The AIS system is a real-time database of security incidents. The FBI offers an industry-government cooperation program: IfraGard.

The technology industry also provides help in the form of security audits, intrusion response teams, and targeted security for specific software. Much of the effort is aimed at providing patches and updates for specific vulnerabilities. The system-level perspective of security deserves more attention. Intrepid Net Computing offers data-centric audits, intrusion response, and breach clean-up. We also offer state-of-the-art enterprise and mobile security in packages that scale to your business needs.

Biography

Dr. Kirkpatrick has a bachelor's in computer science from Montana State University-Bozeman, a master's and a Ph.D. in computer science from the University of California, Berkeley. Dr. Kirkpatrick is an expert in deterministic and statistical computer algorithms, and his main application area is the field of computational biology, in particular genetics. Due to market pressures, Dr. Kirkpatrick has applied these skills to computer security. Intrepid Net Computing takes a data science perspective on solving challenging security problems.

References

[1] Ponemon Institute. 2016 cost of data breach study: Global analysis. *Ponemon Institute Research Report*, 2015.

[2] Dan Gusfield. *ReCombinatorics: The Algorithmics of Ancestral Recombination Graphs and Explicit Phylogenetic Networks.* The MIT Press, 2014.

[3] P. Shannon, A. Markiel, O. Ozier, N. S. Baliga, J. T. Wang, D. Ramage, N. Amin, B. Schwikowski, and T. Ideker. Cytoscape: a software environment for integrated models of biomolecular interaction networks. *Genome Research*, 13:2498–2504, November 2003.