Cybersecurity in Montana

Dr. Brent Kirkpatrick[*]

June 25, 2016

Intrepid Net Computing

www.intrepidnetcomputing.com

[*] bbkirk@intrepidnetcomputing.com

Abstract

Using publicly available data, Intrepid Net Computing has evaluated cybersecurity in the state of Montana. We use `buttressIT`$^{\mathrm{TM}}$ a proprietary audit methodology based on data science and artificial intelligence.

This report outlines the cyberinfrastructure currently in use in the state of Montana. We assess the cybersecurity vulnerabilities of the services offered by a number of Internet Service Providers. We reveal the activities and IP addresses of the most prominent hackers in the state of Montana. We suggest solutions to these security problems.

1 Introduction

Hacking harms our whole economy, from small business to big business and from the technology industry to the health 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.

In a world where data theft is popular, the best measures are preventative, rather than restorative. By employing state-of-the-art security measures, companies can spare themselves the outrageous cost of recovering from data theft. The cost of implementing these security measures is minuscule when compared with the 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 household 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 how prepared Montana is to face cybersecurity challenges. Five shields indicates optimal preparedness and zero shields indicates critical problems.

2 Physical Infrastructure

The physical infrastructure of the Internet in Montana is unknown. Dozens of companies contribute to creating and maintaining the existing infrastructure which consists of fiber-optic cables, telephone cables, coax cables, dedicated high-speed cables, satellite connections, and cell towers. Since no single entity is responsible for the entire infrastructure, nobody knows the layout of the network. Each company knows the layout of their portion of the network, but this information is not communicated between companies or with the government.

Discovering the layout of the physical infrastructure in Montana is a scientific problem. 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 biology, these methods are used to reconstruct the tree of life [2] or the network of life [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 in Montana. Figure 1 shows our estimate of the layout of the Internet infrastructure. The darker edges indicate the 'Internet backbone' which consists of dedicated high-speed, high-bandwidth data lines that were installed in the late nineties and early part of this century. The backbone was created to connect key computational infrastructure in the United States that includes universities, supercomputer centers, and government laboratories.

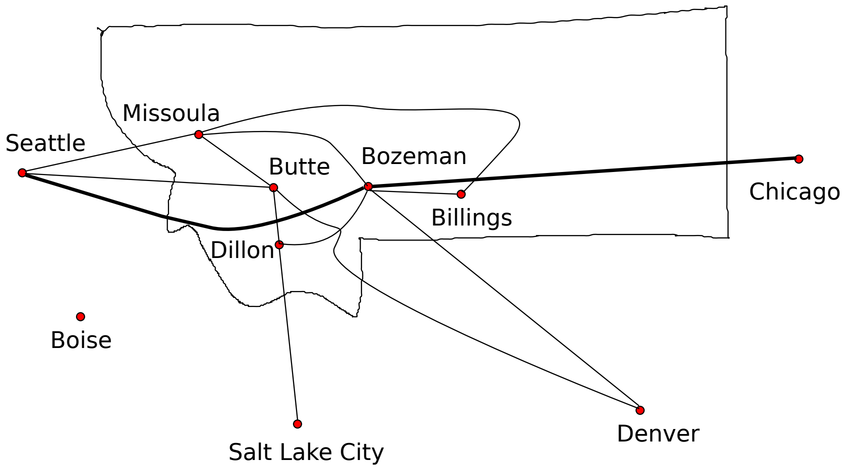

Figure 1: **Layout of the Internet.** This is an estimate of the layout of the Internet infrastructure in Montana. While there may be some incorrect lines in this figure, this estimated layout is largely accurate. Darker edges show dedicated high-speed lines.

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

■■■■□

Bozeman, in particular, is directly on the Internet backbone and has an incredibly fast connection with the rest of the country. Missoula and Butte are connected to the backbone through Bozeman, through Salt Lake City, through Seattle, or through Denver. It is no surprise that most of the high-tech industry in Montana is located in Bozeman.

The average speed of consumer Internet service in Montana is slower than the rest of the country, as fiber-optics have not been installed in residential neighborhoods. Cell-coverage is worse than in the rest of the nation, and satellite remains one of the few options in the most rural portions of the state.

In terms of reliability, the physical infrastructure in Montana is quite reliable. There are occasional outages that vary in frequency based on whether the service area is rural. The primary threats to service reliability are weather-related outages.

In terms of security, the physical infrastructure is very secure from physical hacking. Although it is not the fastest, Montana has a safe infrastructure. The state has relatively little crime and good physical security. There is relatively little hacking in the state, and the cybersecurity is correspondingly good.

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) servers act like highway signs.

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

If the software infrastructure is insecure, then traffic on the Internet may not reach its destination, it may get routed to a different destination than the user had in mine, 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 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 relatively little security in the software infrastructure in Montana. The state is relies on the good intentions of its users to maintain security. This strategy back-fires when sophisticated hackers from other parts of the country target known vulnerabilities in the software infrastructure. On the other hand, there seem to be few hackers in residence in the state, so this approach may be appropriate.

More recently installed or configured Internet access has better software security. Some businesses, such as Starbucks, rely on successful software companies to provide their Internet, and this service can come with good 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 falling behind on security upgrades and training.

Secure Public WiFi Hotspots

A number of Montana businesses are progressively secure, and some of these businesses offer public WiFi hotspots. If you are traveling in Montana or working away from home, please use one of these secured networks for sensitive Internet transactions.

Town	Business	Location
Dillon	Sweetwater Coffee	E Bannack St
Bozeman	Starbucks	19th Ave
	First Security Bank	E Main St.
Missoula	Starbucks	Brooks St.
Butte	Starbucks	Harrison Ave.

4 Internet Service Providers

The two largest providers of business and residential Internet are CenturyLink and Charter. Additionally, there are a number of other companies and providers that buy bandwidth from the infrastructure owners. Each of these companies also has multiple service offerings.

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
Charter	Residential	🟨⬜⬜⬜⬜
Charter	Business	🟨🟨🟨⬜⬜
CenturyLink	Residential	🟨🟨⬜⬜⬜
CenturyLink	Business	🟨🟨⬜⬜⬜
Google	By Contract	🟨🟨🟨🟨⬜
Blackfoot Communication	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. This is true in Montana and most states.

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

5 Hackers

There appear to be hackers operating with impunity in Montana. The buttressIT$^{\text{TM}}$ evidence suggests that every computer in Montana may have been exposed to tainted Adobe and Windows updates. The buttressIT$^{\text{TM}}$ audit also locates several suspicious servers near Bozeman that are rogue servers if they deliver tainted software updates.

One of the largest risks, today, is DNS poisoning. Most ISPs software infrastructures are very vulnerable to these attacks. To poison the DNS, the hacker inserts the information of their own server into the DNS domain directory and creates a fraudulent server. This is analogous to a vandal changing a destination on a freeway sign at an interchange. That vandalism causes a similar kind of chaos as poisoned DNS entries on the Internet.

Suppose that you are interested in updating your computer's Adobe software. When you hit the update button, your computer will ask the DNS system for the IP address of Adobe's update server and they will request the update from that server IP address. Suppose, instead, that a hacker has poisoned the DNS entry for Adobe's update server and has inserted the IP address of a server they control. Then, your computer will be directed to get the update from the hacker's server. Since updates are trusted by your operating system, the hacker will likely get complete access to your computer.

Hacker's are typically interested in adding your computer to their bot-net, which an illegal, distributed computing infrastructure for launching attacks. In some cases, hackers will want your identity or financial information. In other cases, hackers might pilfer your business files and customer financial information.

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). These rogue servers are located in state or out of state. There seem to be relatively few of these rogue servers in Montana, and the DNS servers in Montana are clean compared with other parts of the country.

There are suspicious servers that appear to be located near Bozeman, Montana. If further investigation yields more evidence of nefarious activities on these servers, they will be considered rogue servers. The evidence collected during our `buttressIT`$^{\text{TM}}$ audit of the state suggests that the following IP addresses are very suspicious and likely belong to rogue servers.

IP Address	**ISP of Server**	**Server Location**	**Updates**	**Affected ISP DNS**
69.144.75.40	Charter Communications	near Bozeman	Adobe	Charter & CenturyLink
69.144.75.19	Charter Communications	near Bozeman	Adobe	Charter & CenturyLink
69.144.75.8	Charter Communications	near Bozeman	Adobe	Charter
69.144.75.34	Charter Communications	near Bozeman	Adobe	Charter

Intrepid Net Computing has notified several effected ISPs who choose not to comment. Subsequent to our notifications, the DNS servers went through a cleaning cycle that produces temporarily better security. However, users in Montana continue to be exposed to these grave security risks, since the vulnerabilities have not been repaired.

6 Solutions

The principle goal of cybersecurity is prevention. This means keeping up with the latest security innovations, understanding the risks, and being knowledgeable computer users. Knowledgeable users can direct their online activities to more secure services. Knowledgeable users know when to perform updates and when to ask for help. Knowledgeable users also know their risk profiles and restrict their most risky activities (i.e. financial transactions) to safe Internet connections.

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 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] C. Semple and M. Steel. *Phylogenetics.* Oxford University Press, 2003.

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