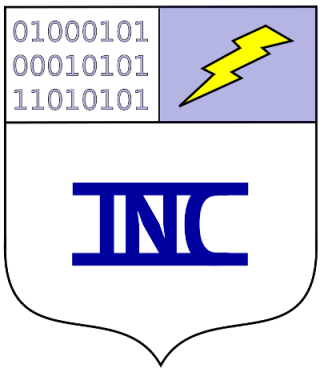
Cybersecurity in Salt Lake City

Dr. Brent Kirkpatrick*

November 30, 2016

Intrepid Net Computing



www.intrepidnetcomputing.com

*bbkirk@intrepidnetcomputing.com

Abstract

Using the buttressIT^{TM} audit methodology, Intrepid Net Computing has evaluated the cybersecurity of Internet Service Providers the Salt Lake City region. Our audit methodology is a statistical epidemiology and experimental science method that relies on public data to examine broad indicators of the health of computer networks.

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.

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 is able to efficiently map your network infrastructure. Please contact us for pricing.

buttressIT^{TM} Rating

Salt Lake 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 seems very reliable.

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

3 Software Infrastructure

The software infrastructure in Salt Lake is **completely compromised**. Due to extensive intrusions in the Internet infrastructure in the metro area, Intrepid Net Computing was unable to complete the buttressIT^{TM} audit which typically requires surveying 5-10 locations. During our buttressIT^{TM} survey, our data-collection platform was hacked in several days.

Intrepid Net Computing uses `buttressIT`^{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`^{TM} Rating

There is extensive hacking in the Salt Lake area relative to other survey sites. Many servers appear to be rogue. Intrepid has witnessed hacking in real-time in the city. There is little effort by systems administrators to adopt DNSSEC, and this informs our rating.

More recently installed or configured Internet service tend 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.

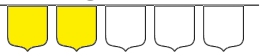
4 Internet Service Providers

We were able to evaluate four ISPs. Only one ISP used DNSSEC, Comcast Business. Most ISPs have failed to secure their infrastructure, and some failed to hide the IP addresses of their DNS servers.

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

`buttressIT`^{TM} Ratings

Following the `buttressIT`^{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
AT&T	Business	
Comcast		
Integra		
Level3		

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 extensive hacking in the Salt Lake City metro area. The tech industry in the Salt Lake area is either under attack from outsiders or has dissatisfied computer users locally.

The buttressIT^{TM} evidence suggests that computers in Salt Lake have been exposed to tainted updates for Windows, Adobe, Ubuntu, and CentOS software. During our audit, many 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 Salt Lake will cost-effectively improve computer security, preventing data theft and fraud.

buttressIT^{TM} Rating

Intrepid Net Computing uses the buttressIT^{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 Salt Lake 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^{TM} audit is highly suggestive that the following IP addresses belong to rogue update servers. Very likely any operating system that uses one of these IP addresses to get updates will be completely compromised.

IP Address	ISP of Server	Server Location	Updates	Affected ISP DNS
212.69.166.138		Europe	CentOS	Level3, Comcast, Integra
64.131.83.114		Wash. D.C.	CentOS	Level3
85.236.43.108		Europe	CentOS	Level3, Comcast, Integra
65.182.107.60			CentOS	AT&T
204.15.73.245			CentOS	AT&T, Comcast, Integra
198.15.72.18			CentOS	Comcast
91.189.88.152		Europe	Ubuntu	Level3, Comcast, Integra
91.189.88.162		Europe	Ubuntu	Level3, Comcast, Integra
91.189.88.149			Ubuntu	Level3, Comcast, Integra
91.189.88.161			Ubuntu	Level3, Comcast, Integra
5.153.231.35		Europe	Debian	Level3, Comcast, Integra
8.8.178.110	Level3	Salt Lake	FreeBSD	Level3, Comcast, Integra
129.128.5.194		Alberta	OpenBSD	Level3, Comcast
64.86.132.152		Texas	Adobe	Level3
64.86.132.138		Texas	Adobe	Level3
65.55.50.189			Windows	Level3, Comcast, Integra

6 Solutions

The principle goal of cybersecurity is prevention. In this case, the city would benefit from a concerted push

1. to identify new worms,
2. to remove rogue/zombie servers from the Internet infrastructure, and
3. 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.

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: InfraGard.

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.