

OK
★

Preliminary Project Title: An Analysis of Emissions from Electronic Devices

Mentor: Ming Chow

Abstract:

When an electrical current goes through a wire, it causes an electromagnetic field around that wire. This means that any electronic device is broadcasting the signals going through it. In the early 1960's agents from the NSA tried to exploit this electric property and attempted to eavesdrop on communications. Through Van Eck phreaking, it became possible to recover the image from a CRT monitor from a distance. The high voltage and frequencies used in CRT monitors made it "easy" to recover the signal. However, it was showed in 2004 that signals from conventional displays can also be recovered. Signals from electronic keyboards have also captured. However eavesdropping on electromagnetic emissions does not only extend to monitors and keyboards; every electronic device can be listened to by tuning in to the correct frequency. Today, ultra-cheap software defined radios (SDR) (radios that can tune to a very wide frequency spectrum ☺ and output the raw signal to software for analysis) can be used to listen to various signals from electronic devices. Mellissa Elliot from Veracode conducted a presentation at Defcon this summer where she discussed how she discusses using an SDR to tap into various communications. The fact that a \$10 radio can be purchased to tap into potentially very private communications is astounding and deserves more research into.

Holy ~~sxxx~~.....
Points off for
misspelling her
name. What a
shame...

OK

Privacy on the Web: How Anonymous is Tor?

Michael Silverblatt
Tufts University

Mentor: Ming Chow
Tufts University

Abstract

Tor is a popular service for browsing the web without sharing one's identity that works by routing one's encrypted traffic through a series of nodes throughout the world in such a way that it is impossible to trace from start to finish. It is an invaluable tool for people such as journalists or peace and human rights workers who may not have unfiltered access to the internet. However, it remains controversial due to the inevitable use of the service for illegal activities, not limited to arms trafficking, illegal drug trade, and even murder-for-hire. In the wake of the NSA's crackdown on users of ".onion" sites like the "Silk Road", which are only accessible through the Tor service, questions have arisen regarding just how anonymous Tor browsing really is. Initial investigation has led some to believe that the service itself was never compromised and that the users' identities were revealed due to an exploit of the Firefox browser included with the software. Recently released NSA documents leaked by Edward Snowden seem to back these claims, as they admit the near impossibility of compromising a significant portion of users due to the vastness of the network. This paper looks to explore the way Tor protects the anonymity of its users, the legality of such a service, the ways in which the NSA was able to identify certain Tor users, as well as the future security of the Tor service.

OK
★

Computer Network Security
Final Project Abstract
Jacob Schmitz

For my final project I intend to research several security vulnerabilities in Apache Hadoop. I spent the summer working at Cloudera working very closely with HDFS, MapReduce, and HBase and in the process I was exposed to several gaping security issues in the Hadoop infrastructure. Some of these vulnerabilities include lacks of authentication on reading AND writing to HBase tables, as well as susceptibilities to Man in the Middle attacks from a Jobtracker node during a MapReduce job (this is especially dangerous because the culprit now has access to everything stored on the cluster's HDFS, including raw HBase data and many other things). I'm currently trying to figure out whom at Cloudera I want to be my mentor for the project, but I'm basically deciding between Alan Jackoway and Adam Warrington.

OK
★

Adam Zakaria
Comp 116

Abstract: Android Rootkits

A rootkit is software designed to give a user “root” priveleges by subverting an operating system. Rootkits are particularly insidious because they are often kernel-based, making it almost impossible for malware detection programs within an operating system to combat them. Windows and linux based rootkits are well-documented topics, but documentation on rootkits for Android, the popular mobile operating system based on a modified linux kernel, is relatively sparse. Given the increasing ubiquity of mobile computing, and the increasing market share of Android, development of malware for the platform has become very popular, and will continue to grow. It is thus imperative that preventive measures are disseminated throughout both the developer and end-user communities. My paper will explore methods of implementing Android rootkits, what can be done by an attacker once a rookit is sucessfully deployed, and how we should address the inevitable proliferation of Android rootkits and mobile malware in general.

still a
big
problem

James Downer
October 17, 2013
Introduction to Computer Security

NICE
Yes

Recent research by Trend Micro has illustrated a number of vulnerabilities of Automatic Identification Systems (AIS). AIS a method of communication between ships, run over radio frequencies. It is used to show ship's position, speed, heading, closest proximate approach (used for navigational purposes to communicate passage), status (under sail, motor, or anchored), and potential issues (such as man overboard or weather or not the ship is around). Radar is a useful alternative, but lacks much of the information offered by AIS, is dramatically more expensive, and has a much shorter range. AIS has stood as the standard used in the marine industry for location and information of ships around the world. It's vulnerabilities to fraud have dramatic potential consequences for abuse.

As piracy has grown to be a larger issue in the Indian Ocean, these exploits have the real potential of being used by pirates. In areas of treacherous navigation combined with malicious intent, these exploits could be deadly. Using these exploits, pirates have the potential to defraud the radio signals used to report on ship's location to ensnare ships through false distress signals, fake reporting of ships location to divert a ship into a trap all for a relatively low cost. My project will explore the ease of a variety of false reports demonstrated by Trend Micro in their recent research including creation of fake vessels, false man overboard reports.

These exploits have extreme real world consequences for the safety of the shipping industry and I will therefore explore potential alternatives to counter exploits and their shortcomings.

Noah Daniels
may be
interested
in this

↑
why?
ugh

yes

TUFTS UNIVERSITY

COMPUTER SCIENCE

INTRODUCTION TO COMPUTER SECURITY

The Questionable Anonymity of Tor

Author:

Aaron WISHNICK

Mentor:

Ming CHOW

October 17, 2013

ugh

The Malware Epidemic Convon

Yes

As smartphone popularity continues to increase, so does the threat to mobile privacy and security. Mobile malware presents a unique challenge; as the mobile community and connectivity of the general public reaches an all time high, applications and operating systems must be designed in a security conscious way. Education on the dangers and potential risks of mobile malware is paramount to successful defense and prevention. Here we discuss general trends in mobile malware, the different kinds, and several security good practices to ensure the integrity of smartphone data. In this increasingly mobile world, the importance of taking this security risk seriously cannot be understated.

ugh

Security & the Cloud

McShane

Revise
broad,
known,
too general

Abstract

I am writing this term paper for Computer Science 116 – Introduction to Computer Security. The purpose of this paper is to uncover and present the security risks and potential vulnerabilities that may arise as more companies move to cloud-driven Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS) models. As a secondary focus, I would like to convince the reader that although cloud processing and storage can offer many benefits, it may not be suitable for some applications because of the security vulnerabilities that it may introduce.

The scope of my research includes (1) some general background information about the three major cloud service models, (2) research on the popular perception that cloud service models are more secure than traditional IT models, (3) research on the security vulnerabilities that may be introduced with a cloud service model, and (4) some scenarios in which a cloud service model may not be suitable from a security standpoint to implement in an organization.

Note: This abstract is incomplete as I have not yet completed my research. As I continue to work on my paper I will update my abstract with a brief overview of my findings and the significant contributions that my research has to offer to the field of security.

Not an abstract

vgh

An Analysis of Mobile Malware Detection Techniques

Yes

Abstract

A. Dinesh

Day by day the number of smartphone users is increasing rapidly, along with Smartphone usage mobile malware attacks are also growing. Malware is malicious software used to disrupt, gather information, or gain access to a computer system or mobile device. Malware developers make use of third-party application to inject malicious content into smartphone and compromise phone security. Malware detectors are the primary tools to fight against these malwares. The success of malware detectors are based on techniques it uses. The primary objective of this report is to focus on various malware detection techniques along with their strengths and limitations and help users assess the risk imposed by malware.

Revise

World War v3.0.0.1 The Current State of Cyber Warfare

SAMUEL DANIEL
samuel.daniel@tufts.edu
October 17, 2013

Abstract

The Internet is undeniably one of the most important technological and social innovations in modern human history. As undersea cables and satellites ferry more and more Internet traffic, the world becomes exponentially more dependent on the Internet for communication and commerce. Utilities systems, communication networks, supply chains, and more have all become "connected". Only recently has the Internet's potential as a platform for disruptive actions been recognized. Pervasive connectivity means that a cyber attack could have consequences on a modern society comparable to the detonation of a nuclear weapon. This paper will examine the history of cyber warfare, the current state of cyber weapons and defenses, as well as the potential consequences of a cyber attack

Too broad

✓
Focus on
current &
future
states

WAY too broad
Revise

Dennis Chen

Mobile Security

As technology becomes more portable and society puts more trust/data in their phones, the problem of security in mobile devices arises. With more people using their mobile phones for work and their private life, the amount of sensitive information that is stored on them is also increasing. Since these smartphones are relatively new to technology, users are unaware of many attacks and weaknesses that phones have. Some basic attacks involve Bluetooth, wi-fi networks, text messages and even web browser attacks. This doesn't even include physical attacks in which stolen devices can be broken into. Most people are aware of malware designed for Windows, but with the growing use of phones, there has also been a growth in mobile malware. There are ways to prevent and guard against this behavior but it also requires attention from the users themselves. Similar to computers, phones need something similar to antivirus and firewalls. Just because a phone is with a user in their bag or pocket, does not mean they are safe from attacks near by. Security awareness is a big key in the prevention in of vulnerabilities as well as simple security measures that can be implemented.

Yes

Denis Richard – dricha09
Comp116 – Prof. Ming Chow
Preliminary Paper Abstract

Abstract

At DEFCON 16, Anton Kapela and Alex Pilosov demonstrated a technique that allowed them to stealthily steal Internet traffic along the lines of a MITM attack. This attack utilizes an inherent feature of the Border Gateway Protocol (BGP), fooling routers into redirecting traffic to an eavesdropper's network. Because it does not exploit a bug in the protocol, but exploits the natural way BGP works, such attacks are hard to detect and would require an overhaul of the protocol to prevent them. Secure GBP (S-BGP) is the name of such a potential overhaul and is designed to verify an ASE's authenticity through a hierarchical process of authentication by the succeeding "hops" in a route's path. This paper outlines the inherent flaw of BGP and analyzes the problems faced by the implementation of a revised S-BGP protocol.

Is this
still a
problem
today?

What will be
your demo?

Paper title?

Yes

Nicholas Andre
Security Abstract
iClass RFID Vulnerabilities

The iClass RFID access systems are widely deployed and look, at first glance, like a fantastic way to manage access control to corporate and university buildings. When compared with common keys, lost cards can be deactivated instantly, temporary access or time-based access can be given without supplying additional physical access devices or collecting them afterwards, and an entire student body's access can be removed instantly without changing the locks. However, there are vulnerabilities latent within both RFID products in general and also the iClass system itself which severely threaten the overall security of the system. This paper will analyze the poor security practices used by iClass in the development of the product and how they affect the current usability and exploitability of these systems. In addition, the paper will analyze how this particular system frames the broader implications of organizations using closed source access or encryption systems with six figure price tags without the full understanding of (or ability to understand) the capabilities, weaknesses, and exploits of a given system, especially a system that we trust with the safety of our buildings and the student body.

Revised

Security Final Abstract

Nathaniel Tenczar

October 17, 2013

With the rise of mobile devices to a prominent position in today's technology market, two major platforms arose: the Android and iOS mobile operating systems. While both have a substantial user base, Android devices currently command 80% of the mobile device market as of the second quarter of 2013. With such a large number of devices running the platform, there is a heightened imperative for developers to provide a secure experience via the operating system and the applications that the OS runs. Unfortunately, this has proven to be a challenge due to the fragmentation of Android versions across a plethora of different devices.

This paper explores the security features built into the Android operating system such as application sandboxing, and user permissions, and their basis in Android's UNIX roots. In addition, the paper highlights application based exploits and demonstrates security problems that developers may run into, with the goal of illuminating best practices for Android development.

Title?

Two directions here

Android OS

Android
dev

kezhi Wu

yes

GPS Spoofing for smart phone

Abstract

Nowadays GPS technology has an important role in people's life. Nearly all Smart phones now have GPS location functions meanwhile more and more applications are using/ basing on GPS on it. Apps like facebook checks location when posting status, "Momo" which is a GPS location based social networking software pairs people near each other to chat. However, many has ignored the safety issue behind using GPS services. On smart phones, location can be easily spoofed with applications/plugins and there are free apps that does that in the open market (store for android and Cydia for iphone). I am going to look into GPS spoofing on a smart phone basis, try to understand and actually do it. This paper will mainly discuss about different ways to achieve GPS spoofing and some legal ramification of using GPS spoofing to mask one's location info.

Nicholas Davis

Abstract— In this paper I present an analysis of RFID systems and the secure implementations. I will test the integrity of the cryptographic implementation, and well as hardware and software functionality and security. I will present my findings in the form of example code and design instructions. This analysis will cover the entire RFID stack from high-level software, to embedded hardware.

cmom man

Title?

Is
this
another
RFID
paper?

yes
★

When Analytics Cross the Line

Author: Alison Tai

alictai@gmail.com

Mentor: Ming Chow

Abstract

Data mining is the process of gathering large volumes of information from a particular source and analyzing it to predict performance. As technology moves towards analyzing everything within its grasp, data mining becomes more and more interesting tool for looking at trends over time. Data mining can be a powerful tool in predicting future trends and guiding decisions. As the price of information dramatically rises, though, data mining becomes more and more of a security and privacy violation. This paper will take a look at the value of information, the history and current status of data mining tools, and their consequent security and privacy implications.

Revise

Diogenes Nunez
Comp 116 - Abstract

Attacks on web applications can occur at any moment, from any place in the world. Some are so prevalent and dangerous, they are on the Open Web Application Security Project (OWASP)'s Top 10. Despite this, there are more than a few applications that do not prevent them. Developers can choose to repair their applications. However, this can be considered "infeasible". In some cases, the code is difficult to maintain to the point that "repair" means "build from scratch". In others, one can deem a vulnerability as "not harmful" and ignore it. This can lead to a more harmful attack in the future.

Web application firewalls (WAFs) are another choice open to these developers. With these, malicious requests can be dropped before they inflict damage. Examples include ModSecurity, part of the OWASP WAF Project, and NAXSI for the Nginx. In this report, we look at these WAFs and how they can not only prevent attacks, but possibly point developers towards where repairs should be made.

I'm not
sure what
you are
trying
to
accomplish.
This
seems all
over
the place.

Yes
★
we discuss

Abstract - c116 final project

Dave Mancinelli*

E-mail:

Abstract

Public WiFi hotspots have become ubiquitous in coffee shops, airports, and other commercial venues where consumers have come to expect internet connectivity for their laptops, smart phones, and tablets. The traffic on public networks is largely unencrypted, but public WiFi users, many of whom are unaware of the associated risks, continue to log in to email accounts, Facebook, bank accounts, or any other domains containing sensitive personal information. Such an environment – wherein a large base of users sends personal data across an unprotected network – could also be a hotspot for nefarious hacker activities. This paper examines the known hacker exploits of public WiFi networks, such as man-in-the-middle attacks, packet sniffing, and ARP spoofing; analyzes the risks of using public networks; and provides recommendations for safer public WiFi usage.

*To whom correspondence should be addressed

Hayley Weiss

Yes!
★

Overview of Cooperative Infrastructure Defense and Ant Based Cyber Defense

Today we monitor cyber defense by gathering data across an infrastructure to a single point and analyzing it centrally, which is problematic as it scales poorly. To combat this, the Pacific Northwest National Laboratory (PNNL) has been working on a method called Cooperative Infrastructure Defense (CID), which utilizes “digital ants” and “swarming intelligence” to quickly react and adapt to cyber attacks with humans supervising at the appropriate level. This paper gives an overview of the concepts behind CID and digital ants.

ves

Comp 116 Final Project Abstract
Using Automation to Combat Phishing

Kelly Gerritz
10/16/2013
Ming Chow

This paper will investigate the viability of creating automation to reduce security issues caused by Social Engineering. Specifically, to combat Phishing attempts that attempt to mimic authentic businesses in an attempt to gain access to a user's username and password. Either in the case of attempting to mimic a site like "wellsfargo.com" or capturing generic username and passwords that users might use for numerous sites.

Two hypothetical pieces of software will be compared in terms of their potential to combat Social Engineering. The first will be a web crawler, that will crawl and perform screenshots or download the front end of code of popular sites that contain sensitive information such as "google.com" or "wellsfargo.com". The software would be an addon that would compare the current site that a user is browsing and if it detects a similarity with the more well known site but a mismatch in domains would alert the user.

The second would be a honeypot crawler. It would crawl to various sites soliciting a signup for a free game or for a free cash give away and give the site a unique e-mail and password. Then it would watch the e-mail account and detect if any unapproved logins were attempted.

To examine both pieces of software two different aspects will be examined. First the success of previous implementations of similar forms of software. Secondly, how the pieces of software would themselves be implemented and examine various strengths and weaknesses of the implementation.

Yes!
★

Visual Geolocation Based Black and White Listing

Karl Cronburg*

Dept. of Computer Science, Tufts University, Medford MA 02155

Abstract

Various commercial and open-source tools are available for managing IP-based filtering of web traffic. A common open-source method is the use of static ‘tricks’ found on stackoverflow (e.g. defining Apache rewrite rules). A more involved approach is to create *iptables* rules. However, the availability of tools to interact with iptables from a high level is lacking. As such, we present a novel approach to managing iptables rules through an interactive map of the world powered by Google Maps and IP2Location.com. Our approach focuses on effectively conveying web site traffic in a way that any content-provider can understand, regardless of prior experience with tools like iptables. We discuss the effectiveness of existing black and whitelisting tools, and where our approach fits into today’s network security landscape. We conclude with a discussion of possible improvements to our approach, which should lead to increased productivity of website administrators in dealing with network attacks.

*Electronic address: karl@cs.tufts.edu

yes

Building Secure Websites With Web Application Firewalls

by

Albert Jose de Vera

Abstract

The current Internet landscape includes sophisticated attacks on websites that disrupt applications from servicing the intended audiences. Other types of attacks lead to the unauthorized access and control of the servers, thereby compromising integrity and confidentiality of data. The security community has developed solutions to mitigate these problems. This paper describes processes and products which enable website operators to secure their servers and applications from attacks. A sampling of web application firewalls (WAFs) are discussed and tested against a number of attacks as part of developing a systematic process of securing websites. Certain open source WAFs are used in a testing environment to determine their effectiveness. Commercial products may be included if vendors agree to participate in this project.

Security Final Paper Abstract

William Clarkson
william.clarkson@tufts.edu

October 17, 2013

Currently, there are widely used cryptographic algorithms which strictly regulate who can encrypt or decrypt a message, but not *when* it can be decrypted. A system to enable the encryption of messages which can only be decrypted after a certain time interval that does not depend on a trusted third party to hold keys would be valuable for many applications, including encrypting bids in online auctions, delayed payments with digital currency like Bitcoin, and ensuring secrecy of votes cast in an election. Several partial solutions to this problem have been proposed, which require a fixed amount of computation to be performed to decrypt the message, which is related to actual clock time required by the speed of the processor. I will discuss several approaches which level the playing field between faster and slower processors, as well as ways to improve the ratio of the lifetime of a timed encrypted message to the time required to initially generate the message. Finally, I will provide and explain the implementation of a simple proof-of-concept system for encrypting and decrypting time-locked messages.

Yes,
see
Ben
Hescott.
We
talked
about
this

Visual Abnormality Detection in SQL Data

MAX GOLDSTEIN¹

¹*Tufts University* Max.Goldstein@tufts.edu

ABSTRACT

SQL queries can ask incisive questions of persistent data, but only if one knows where to look. Existing visualizations of SQL typically focus on the schema graph, not the data themselves. We contribute a visualization of SQL data that integrates with the schema and types of a single table to detect abnormalities, locate frequently-accessed hotspots, and find correlations between fields. Security applications include locating tampered data (possibly the result of injection attacks), preventing sensitive data exposure, and detecting unusual (e.g. potentially fraudulent) actions. We apply the visualization to a 290-thousand song radio music library.

Keywords: Security, Visualization, SQL

Intriguing

I don't care about this.

Yes but careful

David Kalayeh

Comp. 116

17 October 2013

typed

Yes!

Final project abstract:

((

Supervisory control and data acquisition (SCADA) systems, LonWorks networking hardware, and their associated protocols are ubiquitous in industry. Many countries, including the United States and China, have codified the protocols as national standards. These systems often link with internet connected devices, and such links expose industrial control infrastructures to internet-based attacks. Furthermore, control hardware often has poor physical security. In at least one very high profile case — the Stuxnet virus attack on Iran's nuclear enrichment facility — attackers specifically targeted a SCADA system to cause catastrophic system failure. This paper compares and contrasts Ethernet-TCP-IP technology with LonWorks-SCADA technology to determine if security best practices from the former domain are applied or could be applied to enhance

Yes
★

Security in Startups

Michael B. James Mentor: Aaron Boyd
michael@michaelbjames.com aaron@nomic.com

October 17, 2013

Abstract

By devoting all of their time to making a product, startups rarely take the time to step back and review the security of their product. While creating an minimum viable product always comes first, the business costs of getting abused from a simple security hole often outweigh that amount of time spent creating a new feature. Using new technologies and full of programmers aware of SQL injections and XSS, they often overlook other gaping security holes. I will outline the forgotten parts of security in startup life, their impact, and how they are used maliciously. I will also suggest preventative measures that are not time consuming so that a startups product can maintain security throughout the development process.

Nicholas Teleky
Fall 2013
Computer Security
Final Project

Yes

Abstract:

With well over 1 billion users combined, Chrome and Firefox internet browsers are among the most popular in the world. A contributing factor to that popularity is that users have the ability to install third-party browser extensions, usually to streamline a user's experience with that browser. Unfortunately, black-hat hackers have exploited the fact that millions of these extensions are downloaded every day, and can easily build malicious extensions that can track browser usage, intercept cookie information, and even obtain logon credentials for web sites.

In this paper, I'll examine how extensions are built and what extensions can be given access to, attempts that Google and Mozilla have made to secure their browsers, and demonstrate how an individual could create an extension to hijack a Facebook or Twitter account.

Mentor: Ming Chow

See Black Hat
2011 presentation
as reference

Yes
Yes
Yes
William Tucker Stone

Mentor: Ming Chow

Google Glass and Wearable Technology: A New Generation of Security Concerns

Abstract:

As new technologies such as the Google Glass are developed and released to the public, so too are new security problems and privacy apprehensions that must be acknowledged and accounted for. The Google Glass is a small headband-like computer that puts a screen in front of the user's eye, allowing them to navigate the web, take pictures, and manage their various social media and communication. The device contains a wide-angle camera, retina sensor, microphone, and touch screen for device navigation. Users can easily shoot video clips or take pictures at the utterance of a command, and already there exists the ability to create custom applications for the device using Google's "Mirror-API", a web-based API that allows developers to interface with a Glass unit.

This paper examines the connotations of such abilities in the hands of everyday users, as well as the process through which your average programmer can deploy potentially insidious applications to a Google Glass unit. In addition, this piece will explore such topics as new social engineering apprehensions inherent with the release of a technology such as this and hardware vulnerabilities or exploits that have been discovered (as well as those that haven't). Already, dozens of Google Glass first-look users have found various ways to sabotage or subvert the device for other purposes, and these types of misuses must be something every user and developer of this new technology must be aware of.

Ashley Hedberg
Comp 116
10/17/2013

Yes!
★

Final Project Proposal: The “Privacy” of Private Browsing

Abstract:

Most modern web browsers have a “private browsing” mode that supposedly allows a user to surf the internet without leaving any traces on his or her machine. However, the notion of “private browsing” offers users a false sense of security, as browsing information is often left behind when a private browsing session terminates. Several researchers have already demonstrated methods of detecting this information; these include the analysis of virtual and browser memory¹ and the pagefile on Windows machines.² The existence of private browsing artifacts on a user’s machine raises many questions: how much privacy do web browser developers actually aim to provide with “private browsing” modes? Are these goals accurately conveyed to the end user? And if the user’s browsing session can be reconstructed from these artifacts, how might this be exploited by digital forensics professionals and creators of malware?

This paper seeks to answer these questions. Additionally, supporting materials seek to prove that such artifacts can be used to determine, at least in part, what a user was doing during his or her “private browsing” session—thereby rendering it not very private at all.

That's
correct

¹ Mahendrakar, A., Irving, J., and Patel, S. “Forensic Analysis of Private Browsing Mode in Popular Browsers.” Carnegie-Mellon University. <http://www.mocktest.net/paper.pdf>

² Mueller, L. “How Private is Internet Explorer’s InPrivate Browsing?...First define ‘private’.” Magnet Forensics. <http://www.magnetforensics.com/how-private-is-internet-explorers-inprivate-browsing-first-define-private/>



Hidden In Plain Sight: An Analysis of Private Browsing

Abstract

Almost every web browser available today comes with a setting for a private mode. This leads users into believing that their web activity cannot be monitored, traced or stored while under the protection of private browsing when, in fact, there are many ways that all browsing data can be seen. This article will discuss what levels of privacy these services actually do and do not provide as well as many ways to break these systems and view the activity from a machine running an incognito window, such as automatic screen capturing software, browser add-ons/extensions, sniffing and availability of browsing information at different levels of network access. This article will then discuss more advanced methods of anonymous browsing, such as IP spoofing and onion routing (Tor) as well as the benefits and downsides of these services. In conclusion, we will discuss whether or not network anonymity is a necessary service as well as the potential problems that it allows.

Author: Amadou Crookes
Mentor: Ming Chow
10/17/2013

Yes
LOL-
✱

Node.js Vulnerabilities

Node.js is a fresh take on "building fast, scalable network applications" in the form of a server-side framework. There are two main differences to Node.js from the other well-known frameworks. Node.js is written entirely in JavaScript and through JavaScript's straightforward anonymous functions the use of handling events asynchronously. With Node.js being a "new" technology, the community has uncovered several vulnerabilities.

This paper will survey the vulnerabilities that are most prevalent to Node.js and explore the techniques used to exploit those vulnerabilities. As we look at the vulnerabilities we will also see if Node.js lends itself to these vulnerabilities. While checking vulnerabilities we will look at the features under the hood of Node.js, such as JavaScript or Chrome's V8 JavaScript Engine, to ensure a proper level of security at that level. We will take about best practices to avoid creating vulnerabilities at the code level. Lastly we will look at how to exploit vulnerabilities.

You could take a
look at my
SOURCE
Boston 2013
pres

yes

Abstract

Stefan Dimitrov
Mentor: Ming Chow

October 17, 2013

The traditional software distribution channel on the iOS platform is Apple's own AppStore, which is known for its stringent app approval policies and quality control. One of the aims of Apple's approval process is to prevent malicious software from reaching its customer base. This preemptive strategy has proven to be relatively successful, but has been criticized for rejecting benign apps that replace or enhance core services. Jailbreaking has opened an alternative outlet for this niche of software offerings by letting users install apps from third party software repositories outside of Apple's regulation, however, this lack of security audit theoretically enables the unhindered distribution of potentially malicious code. Moreover, because jailbreaks exploit a security vulnerabilities within iOS in order to grant apps root privileges and unrestricted filesystem access, they effectively disable several security features in iOS. However, jailbreaking also allows the installation of third-party patches targeting those very vulnerabilities. In addition, jailbreak tweaks that improve privacy control have surfaced in response to controversial AppStore apps that misuse user information, yet pass the approval process. These subtle, but significant differences between the stock and jailbroken flavors of iOS motivate this paper in an attempt to explore the pros and cons of jailbreaking regarding security and privacy.

Mentor: Ming Chow

Student: Andrew Li

Abstract:

Recent concerns have arisen over the security of pseudorandom number generators (PRNG's). Cryptographically secure PRNGs are verified mathematically to produce a sufficiently random series of numbers. However, some PRNG's previously thought to be secure have suffered from a range of issues, including improper implementation and backdoors. These flaws become apparent when PRNG's are depended upon for cryptography or encryption.

Without a sequence of seemingly random numbers, the possibility for an attacker to subvert the software security exists. In this paper, we will explore the problems found in PRNG's and highlight recent examples of vulnerabilities and consequences. We will also demonstrate how an attacker might take advantage of such weaknesses.

Yes
✗

There was a paper just pushed out by CMU on the security of /dev/random which is used to generate secure random #s

Yes
Krzysztof Danielewicz
17 October 2013
COMP116

Final Paper: Abstract

On October 2 2013, the largest illegal online marketplace in the world was shut down by the FBI, and its founder arrested. Ross William Ulbricht, the "Dread Pirate Roberts" and founder of Silk Road, had spent 2½ years escaping the efforts of the United States Government to take down his creation, with great success. During this time, Silk Road offered the ability to solicit and purchase a staggering number of blatantly criminal substances and services within minutes, from practically anywhere in the world: it was well known as "the Amazon.com of illegal drugs." Silk Road was run through Tor, a service which offers online anonymity and security. Which brings the question: how did the FBI manage to take down a supposedly anonymous online drug empire, arrest its owner, and seize over \$3 million in Bitcoin? Will these actions by the United States Government make a significant difference in the online proliferation of illegal goods, or do the alternatives to Silk Road (already in full swing) make their efforts fruitless? And do these alternatives suffer from the same vulnerabilities that took down Ulbricht? This paper will explore the above questions and discuss the implications of this take down on illegal trade over the internet and, more generally, the anonymity and potential flaws of the Tor network as it exists today.

Paul Pemberton

10/17/2013

Comp 116

Final Project Abstract

Yes
See Black
Hat 2011
pres.

As internet browsers become more and more customizable, there is a correlated demand for browser add-ons and extensions. The top four internet browsers (Google Chrome, Mozilla Firefox, Internet Explorer, and Safari) have all developed extension modules that allow users to add customized functionalization to their browsers. These extensions also provide an easy target for malware and malicious scripting attacks. For example, it is trivial to write an extension that will act as a keylogger and sniff for passwords and other valuable information once downloaded and installed. Additionally, there is an abundance of issues regarding site checking in general. The remedies for high risk websites are the following: denial of script running, user warning, and user redirection/blockage (Faziri). For example, if a website has an expired certificate, most browsers will block the user from navigating to that site. Sometimes users override the block, which then encourages the user to override the block in the future, even for high risk websites. Current remedies to high risk websites are very restrictive to users and can encourage bad behaviors. To remedy the issues presented with both risky navigation as well as high risk script/extensions, we propose a script that is built to analyze the scripts running in a given website and look for keywords that pose a high risk threat. Then, instead of blocking or denying the user access, the script/extension will display a website risk status so that the user is constantly informed in real-time about the websites that they are visiting.

Works Cited:

Faziri. "NoScript Protects Your Firefox." *NoScript Protects Your Firefox*. Gizmo's Freware, 12 Sept. 2013. Web. 17 Oct. 2013.

Chia, Pern Hui, Yusuke Yamamoto, and N. Asokan. "Is This App Safe? A Large Scale Study on Application Permissions and Risk Signals." *World Wide Web Conference Committee* (2012): 311-21. Web. 17 Oct. 2013.

Carlini, Nicholas, Adrienne Felt, and David Wagner. "An Evaluation of the Google Chrome Extension Security Architecture." *University of California, Berkeley* (2012): 1-15. Web. 17 Oct. 2013.

Wang, Yi-Min, Roussi Roussev, Chad Verbowski, Aaron Johnson, Ming-Wei Wu, Yennun Huang, and Sy-Yen Kuo. "Gatekeeper: Monitoring Auto-Start Extensibility Points (ASEPs) for Spyware Management." *LISA XVIII* (2004): 33-47. Web. 17 Oct. 2013.

Djeri, Vladan, and Ashvin Goel. "Securing Script-Based Extensibility InWeb Browsers." *University of Toronto* (2009): 1-16. Web. 17 Oct. 2013.

Yes but...

Connor Blanck

Digital Rights Management

Abstract

As early as some of the first commercial computer games, DRM or Digital Rights Management has been in place to avoid the illicit copying and distribution of software. While earlier DRM often made use of only off-disk copy protection like CD keys, more current DRM is more likely to make use of copy protection like online activation or verification, data position measurement as seen in SecuROM, or even the requirement of a constant online connection. Growing alongside the development of DRM and copy protection was the desire to bypass these protection systems to allow for people with pirated copies to play the game. This conflict has been a center of controversy as game developers attempt to balance the integrity of their software with the intrusive nature of some DRM schemes, leading to some eschewing copy protection altogether while others attempt to use the most restrictive copy protection to avoid lost sales. This paper will examine the software used in the most popular DRM technologies today, the software "cracks" that attempt to bypass them, and the complex relationship between developer, cracker, and consumer.

Def an
interesting
topic. Perhaps
it would be
better to go
into why DRM
does not work

Final Project Abstract/Proposal: The Security Implications of HTTP 2.0
Isobel Redelmeier – 10/17/13

Yes
to
we
discussed

Through its major role in the network model of the Internet, the HTTP protocol is essential to modern communications. HTTP 2.0, the upcoming version of the protocol currently being drafted as the sequel to HTTP 1.1, primarily aims to improve the protocol's performance. However, the security of HTTP is crucial to the security of the Internet, including the privacy of its many users – individuals as well as corporations, governments, and other significant parties – and the confidentiality of the data they store and share. Already there are numerous known vulnerabilities in the Internet model and the HTTP protocol especially, most of which involve attackers acquiring or changing data which is meant to be restricted. Will HTTP 2.0 help to limit any of the existing weaknesses, or will the focus on performance lead to the exposure or exacerbation of security issues?

This paper will use analysis of the actual working draft of the HTTP 2.0 specification and the discussion surrounding its creation, as well as various literature regarding the security of HTTP 1.0 and 1.1, to examine the potential security effects of HTTP 2.0. In particular, I plan to focus on how the increased connection lifespan and multi-connectivity introduced by HTTP 2.0 may compromise encryption and certificate authenticity.

Security Paper Final
Sam Purcell

Yes
✱
oh dear--~

Abstract

It's a fact that database technologies are constantly being improved and created. Unfortunately, new technologies tend to be designed from the ground up with little to no security built in. Developers who are used to established systems for which there is a substantial amount of built-in security are simply clueless when it comes to securing their data. What's more, these technologies are so new that there is a dearth of developers experienced in correctly implementing the technology – businesses must often learn hard lessons when deploying applications with these technologies. NoSQL databases are a prime example of this type of emerging technology. This paper seeks to analyze NoSQL database vulnerabilities and their causes, and to provide a comprehensive list of attacks and examples of attacks. Specifically, this paper will discuss MongoDB as an example of a NoSQL database, and focus on its vulnerabilities in the context of a schema-less storage system. The security merits and demerits of such a system will be discussed and the reasoning behind using NoSQL versus a traditional relational system will be elucidated. Finally, techniques that developers can use to secure applications built upon NoSQL will be presented.

Final Project Abstract
Comp 116 - Computer Security
Chris Piraino

Peer-to-Peer Protocol Vulnerability:
The Sybil Attack

Yes
Is this
still
a
problem?

Peer-to-Peer networks are a big part of internet traffic, and are only increasing in size and number. P2P networks are utilized by file-sharing services, distributed systems, botnets, streaming services, and many other applications. P2P networks have some obvious security vulnerabilities, most notably how to ensure that malicious nodes do not collude within the network. This paper will examine this type of attack, called a 'Sybil attack', in regards to the penetration and protection of a P2P network. A P2P network's vulnerability to this attack is dependent upon the strength of a P2P protocol's reputation system, namely the ease with which a new node can be created and how trusting existing nodes are. Many P2P protocols exist, but for our purposes we will limit trials to the Kademlia P2P algorithm and its implementations.

The goal is to provide a proof-of-concept Sybil attack against a Kademlia peer-to-peer network that successfully infiltrates the network. The paper will then analyze how the attack penetrated the network as well as ideas for added protection, specifically adding in an implementation of trusted nodes to the protocol.

Abstract



Advisor: Ming
Hao Wan

The last decade has witnessed a significant improvement of mobility of Wifi-enabled devices, including tablet computers and smart phones dominated by Android and iOS operating systems. What accompanies the aforementioned trend is the popularity of public hotspots offered by merchandises aiming to attract customers or collect statistics on their patrons. This act of “free-riding” on public hotspots exposes mobile device users to potential privacy and security risks, for their private data could be exposed to hackers or business owners through various attacks, especially Man-in-the-middle attack.

This paper explore of how mobile platforms use mobile cryptography techniques such as Secure Sockets Layer to reduce the risks of mobile attacks. We will also focus on potential attacks that bypass the security layer and steal personal information such as login credentials, credit card information and MAC addresses.

Ayal Pierce
Final Project Abstract
10/18/2013

Abstract: RFID Hacking and Social Engineering

Radio Frequency Identification (RFID) technology is everywhere; in credit cards, badges, gas stations, Tufts student IDs, and is growing in popularity. A prevalent use of this seemingly magical tool is simplifying access control to buildings, or even logging on to computer systems. However, there are many security pitfalls to the budding technology. As Ari Jules said, "The world of RFID is like the internet in its early stages," referencing the lack of security features built into the technology.¹ Numerous RFID readers are susceptible to simple brute-force attack and RFID tags or cards are easily cloned or read, by simple proximity between attacker and victim. While RFID technology is relatively cheap, encrypting the readers and cards often increase the price twenty-fold. In addition to the technology itself, using RFID technology often makes the client a target of social engineering manipulations.

This research paper will focus on the various RFID hacks from readily available and cheap emulators to social engineering access to the physical RFID key. The paper will then delve into the various methods RFID companies use to protect their clients. It will pose cheap and efficient ways to make RFID technology more secure, as well as give advice to the plethora of RFID users on how to keep their data safe. The paper will also use Tufts University as a case study and will attempt to find security holes in the widespread RFID use on campus.

Project: Physical, cheap, RFID Emulator (Reader/Writer) (the goal will be to build an RFID emulator to read a card and simulate permissions on that card) .

Mentor: Ming Chow

Note: I contacted Dr. Stein of Columbia University and he said that his area of expertise is not RFID technology, but will be happy to provide insight on any algorithmic problems I may run into.

Yes but
this
sounds
like
another
RFID
hacking
paper

↓
this would
be
very
special

¹ <http://www.wired.com/wired/archive/14.05/rfid.html>

>

Dolan
REB Yes

Nathan Tarrh
COMP116
Final Paper Abstract
10/17/13

For my final project, I propose a study of RFID weakness related to Tufts campus, focusing on either a) Tufts IDs or b) Charlie Cards. I propose researching and designing low-cost RFID readers (sniffers based on open-source tools (most likely arduino). Since prior work ~~has been done on the~~ weaknesses of Charlie Cards (Anderson, Ryan, Chiesa, McVeety) it will be more straight-forward to either replicate their work or prove that their exploits have been fixed. Since RFID stealing and cloning is more dangerous and less legally defensible, I do not intend on exploring those options, but rather focusing on weakness in current implementations (see Francis Brown's presentation at Black Hat 2013 for more information about long-range sniffers).

I plan on Ming Chow being my mentor for this project.

Not an
abstract✓
This
would
be
great

George Aquila
10/17/2013
Comp 115 - Abstract for Final Paper

Revise
Too
broad

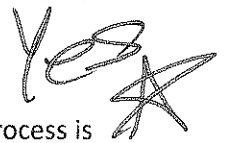
Topic – Cyberwarfare and Security:

My final paper topic will focus on the rising prominence of cyberwarfare and cybersecurity in international relations, both with regards to how it is used by countries like the United States to undermine its potential enemies, as well as how it is used by more stand alone groups to carry out political or ideological attacks. The paper will explore the nature of cyberwarfare on an international level, its potential as an actual weapon as war, and to what extent it will affect the growth of general computer systems security in other contexts. It will highlight specific examples of how cyberwarfare has been used, such as in the case of the Stuxnet worm (exploring the technical specifics of what made it such a unique and devastating attack) and the recent incursions by the Syrian Electronic Army in targeting the United States Armed Forces websites.

Although the exact nature of the supporting material is still uncertain, it will most likely use some form of proof-of-concept to demonstrate the way that a cyber-warfare attack may target a system with a specific political goal both including classical (DoS, delivery tampering, information gathering) and warfare-specific objectives of cracking (Power grid attacks, sabotage).


✓
This is
a good
focus
area

Password Cracking with Distributed John the Ripper Processes
Abstract



Password Cracking can be an incredibly complicated process. A very common tool for this process is John the Ripper (JtR). JtR is free and Open Source, and is largely distributed in compilable source code form. It uses three main modes of attack: single, wordlist, and incremental. The Single and Wordlist attacks compute hashes for supplied password lists and check those hashes against the hashes in the password files. Incremental is a brute force attack, and this is where things get complicated. Brute forcing passwords of under 5 characters is a pretty trivial process. However, as the password length grows, the complexity of brute forcing those passwords grows exponentially. This paper will deal with detecting accessible network computers on a *nix based network and distributing JtR processes across those computers in an attempt to speed up the incremental attack. The distributed processes will all check passwords of different lengths (so that machine A will check passwords of length 5, machine B passwords of length 6, etc.). This project will not deal with parallelizing JtR processes on a single machine. The main deliverables of this project will be a script to detect available and accessible machines on a *nix based network, and automatically distribute JtR processes amongst those machines. It will also look in to alternatives to JtR.

Jon Dutko
October 17, 2013
Comp. 116
M. Chow

kes


A Technical History of Trans-Pacific Cyberwarfare

Abstract

Network privacy and security concerns have come into the purview of American domestic politics recently, most notably in reaction to the NSA's data mining surveillance program, PRISM. Public awareness of the government's domestic relationship with the internet has never been higher. Less ubiquitously well-understood, however, is American foreign policy on the networked, global stage. This paper explores a technical, close-to-the-grain approach to the historic context and present state of American information security and surveillance in an increasingly global world. How the United States government approaches cyberwarfare is then contrasted to the Chinese approach, which influences a similarly large portion of the internet. The currently raging "cyber war"¹ between the two superpowers is discussed. Finally, the effects of international "cyber" conflict on personal privacy and security are made clear. Code deliverables can include examples of attacks and methods of defending oneself in an era in which cyberwarfare is beginning to express civilian collateral damage.

¹ "Intelligence Chairman: U.S. Fighting Cyber War 'Every Day'" *PJ Media*, July 29, 2013

Revise

Eli Kohlenberg

Comp 116 Final Project Abstract

October 17, 2013

It is well known that huge amounts of data exist about everyone who uses the internet. Much of that data is collected by Google and similar companies and sold to others. But much of it is just completely public. Private investigators and journalists have been known to connect screen names to real names purely through legitimate investigative techniques. If that process takes time and directed effort, then we can feel pretty safe; most of us don't expect anyone to spend that much time investigating us. However, it could be possible to do this investigation programmatically.

For my final project I would like to study how these investigations are accomplished, how they can be prevented, and what tools currently exist for assisting the investigator. Then I will examine different software methods that could be used to make them more efficient and easier, and implement such a program.

↓
Maltego

Im not so high on
this, as Ive worked
on this since ~~2008~~ 2007
& tools are rather
well known now

Comp 116

Final Project Abstract

Paul Nixon

Yes

For this project I plan to build a True Random Number Generator using an Arduino's Analog Read capability on a disconnected pin. This was a project which I had previously done with a partner in undergrad, but the Arduino code has since been lost, and there was no paper produced (only a PowerPoint). One part which was not previously done was to generate keys using the random data, which would be cryptographically useful. My goal for this project would be to create release-quality code that anyone could load onto an Arduino and a connected Linux PC, in order to generate their own cryptographic keys. I would appreciate if you could my mentor for this project.

Not an
abstract
but great
idea

Abstract

With the recent events regarding the National Security Agency(NSA), the question of internet anonymity has been on everyones' minds. And for those who prefer to remain under the radar, like Ross Ulbricht of the Silk Road, there was always one place to turn, The Onion Router. Commonly referred to as Tor, the tagline of this service is "Anonymity Online". A report was recently released, however, stating that the NSA was able to crack 90 percent of Tor keys. So the question remains, is there any way to be completely anonymous on the internet?